

Guide d'utilisation à l'intention du commerçant



Solutions Moneris « Moneris » est la principale entreprise de traitement des paiements par cartes de crédit et de débit en Amérique du Nord. Dans le cas des entreprises qui acceptent des clients des paiements par carte, Moneris offre aux commerçants un « point de contact unique » VISA^{MD}, MasterCard^{MD}, American Express^{MD} et Interac^{MD}, ainsi que tous les terminaux point de vente (PDV) et solutions. Nous offrons des produits s'échelonnant du clavier NIP et des terminaux en magasin jusqu'aux solutions sans fil mobiles et le commerce électronique.



PAGES 2 – 10

Traitement des transactions

- Identification et responsabilités du commerçant pour les transactions
- Transactions valides
- Discrimination
- Éléments de base
- Pratiques de traitement exemplaires
- Cartes à puce
- Glissement d'une carte
- Transactions manuelles
- Saisie manuelle
- Étapes pour éviter la saisie manuelle
- Aidez les clients à « protéger leur nip »
- Marches à suivre en cas d'interruption



PAGES 11 – 17

Protection de votre entreprise contre la fraude

- Comment identifier les fonctions de sécurité
- Comportement suspect du client
- Marches à suivre en cas de carte perdue, volée ou oubliée
- Doute d'écrémage
- Commande postale/téléphonique et fraude de commerce électronique
- Pratiques exemplaires de prévention de la fraude électronique



PAGES 18 – 27

Débits compensatoires

- Survol
- Demandes de copies de factures
- Codes de raisons de débit compensatoire
- Pratiques exemplaires pour éviter les débits compensatoires
- Programmes de débit compensatoire excessif
- Autres programmes
- Service de paiement rapide (SPR) MasterCard
- Signature non requise (SNR) Visa



PAGES 28 – 33

Règles et réglementation à l'égard de la conformité

- Troncation du numéro de compte principal (NCP) (masquage de carte)
- Cartes prépayées
- Frais supplémentaires
- Montant de transaction minimum/maximum
- Transactions interdites
- Transactions illégales ou qui nuisent à l'image de marque
- Dépôt
- Vente ou échange d'information
- Multiple reçus de vente et de dépôt – Transactions retardées
- Exigences relatives à l'autorisation
- Conversion de devises dynamiques
- Retour de marchandise, crédits et redressements
- Transactions périodiques
- Dispositifs point de vente (PDV) perdus ou volés

PAGES 34 – 38

Norme de sécurité des données du secteur des cartes de paiement (PCI SSC)

- Norme de sécurité des données du secteur des cartes de paiement (SCP)
 - Stockage des données du titulaire de carte
 - Fournisseurs de service
 - Programmes de conformité de marques de cartes
 - Bris de sécurité
- Norme de sécurité des données des applications de paiement (AP)

PAGES 39 – 43

Commerce électronique

- Sites Web des commerçants
- Exigences en matière de sécurité et protection de votre réseau
- Vérifié par Visa
- Code sécurisé MasterCard
- Valeur de vérification de la carte (Card Verification Value - CVV2)
- Service de vérification d'adresse (SVA)
- Exigences de reçu de commerce électronique

PAGES 44 – 46

Foire aux questions

PAGE 47

Acronymes et liens utiles

Traitement des transactions

Identification et responsabilités du commerçant pour les transactions

Vous devez vous assurer d'informer de façon évidente et sans équivoque le titulaire de carte de l'identification du commerçant à tous les points de l'interaction, de sorte que le titulaire de carte puisse distinguer le commerçant de toute autre partie tierce, tel un fournisseur de produits ou de services.

Vous devez vous assurer que le titulaire de carte comprend que le commerçant est responsable pour la transaction, y compris la livraison des produits (physique ou numérique) ou l'approvisionnement pour les services qui font l'objet de la transaction, ou un service à la clientèle et la résolution du conflit, conformément aux modalités applicables à la transaction.

Transactions valides

Vous devez soumettre des transactions valides seulement entre vous et un titulaire de carte authentique. Vous ne devez pas soumettre de transactions frauduleuses (ou que vous auriez dû savoir comme étant frauduleuses) ou non autorisées par le titulaire de carte, ou autorisées par un titulaire de carte qui complotte avec le commerçant à des fins frauduleuses. Vous êtes responsables des actions de vos employés, agents, représentants et toute autre personne qui traite des transactions.



Discrimination

Vous ne devez pas participer à toute pratique qui discrimine, contre ou décourage l'utilisation d'une carte par rapport à une autre marque de carte en particulier.

Éléments de base

En suivant les bonnes marches à suivre de traitement, vous aidez à réduire les chances de fraude :

- Recherchez l'hologramme, le numéro d'identification de la banque, le symbole embossé unique et l'espace pour la signature.
- Vérifiez la date d'expiration de la carte.
- Si vous utilisez un terminal PDV pour autoriser la transaction par carte de crédit, utilisez-le pour lire l'information sur la carte en la glissant ou l'insérant (avec un NIP) dans le terminal PDV.
- Vérifiez l'affichage du terminal PDV qui présentera le numéro de compte encodé dans la bande magnétique de la carte et comparez celui-ci avec le numéro de compte embossé sur la carte.
- Si vous êtes satisfait de l'authenticité de la carte, utilisez les marches à suivre d'autorisation normales.

Pour une transaction par carte à puce, consultez la section « Comment ça fonctionne » de ce guide d'utilisation.

- S'il s'agit d'une transaction par carte avec bande magnétique, demandez au titulaire de carte de signer le reçu devant vous.
- Comparez la signature sur la carte à celle sur le reçu afin de vous assurer qu'elles sont identiques.

Pratiques de traitement exemplaires

CARTES À PUCE

Une carte à puce est une carte de paiement en plastique (débit ou crédit) dotée d'une micropuce intégrée que le titulaire insère dans un lecteur de cartes PDV ou un guichet automatique bancaire (GAB). Au lieu d'une signature, le titulaire de carte introduit son NIP pour autoriser la transaction, comme dans le cas d'une carte de débit. Puisque les cartes à puce permettent de traiter des données de façon sécuritaire, il est donc difficile de les copier ou de les modifier. La fonction NIP, qui a toujours été utilisée pour les transactions par carte de débit au Canada, procure une sécurité accrue pour le crédit et répond aussi aux préoccupations des commerçants canadiens à l'égard du coût des activités reliées à la fraude par carte.

La technologie de la puce aidera à :

- réduire les débits compensatoires
- réduire la fraude
- simplifier les activités en magasin
- augmenter la vitesse de traitement au terminal PDV



Au Canada, VISA, MasterCard et Interac se sont engagées à une transition en douceur à la technologie de carte à puce pour tous les participants du système de paiement électronique. Ces organisations travaillent ensemble pour coordonner leurs politiques techniques, les procédures et les normes.



COMMENT ÇA FONCTIONNE

Une transaction de paiement effectuée en utilisant une carte à puce avec NIP et un terminal PDV avec capacité de lecture d'une carte à puce est très simple. Plutôt que de glisser la carte et de signer un reçu, le titulaire de carte insère sa carte à puce avec NIP et introduit son NIP dans un terminal PDV doté de la capacité de lire une puce afin de vérifier l'identité.

Éléments importants à connaître au sujet des cartes à puce avec NIP

- Si vous remarquez que la carte est dotée d'une puce, demandez au titulaire de carte de l'insérer dans le terminal PDV.
- Ne vous inquiétez pas si vous ne reconnaissez pas la carte à puce de prime abord, car si la carte est glissée dans la fente, le système vous invitera à insérer la carte. Il suffit de l'insérer et de suivre le message affiché.
- Dans le cas d'une carte à puce avec NIP, le système demandera au titulaire de carte d'introduire un NIP.
- Une carte à puce doit demeurer insérée dans le terminal PDV pendant toute la transaction. Retirez la carte seulement lorsque le message affiché vous invite à le faire. Si vous retirez la carte avant que la transaction ne soit terminée, celle-ci sera annulée.
- Comme pratique exemplaire, nous vous recommandons d'examiner la partie inférieure du reçu et d'encercler le texte « VÉRIFIÉ PAR NIP ».



IMPORTANT :

Laissez la carte à puce avec NIP dans le lecteur pour la durée de la transaction.

1. Commencez la transaction.
2. Cherchez la puce sur la carte.
3. À l'invite, insérez la carte à puce avec NIP, en vous assurant que la carte est insérée recto vers le haut.
4. Suivez les instructions.
5. Attendez que le message vous invitant à retirer la carte s'affiche, puis retirez celle-ci.

La transaction est terminée!





Glissement d'une carte

- Avant de glisser la carte, assurez-vous que la bande magnétique fait face au lecteur.
- Glissez la carte une fois et dans le sens de la flèche indiquée sur le lecteur.
- Ne glissez jamais la carte dans un geste aller-retour, car ceci peut entraîner une mauvaise lecture de la bande magnétique.
- Comparez les numéros de comptes.
- Assurez-vous que les chiffres du numéro de compte sur le reçu correspondent aux quatre derniers chiffres de la carte. Si ce n'est pas le cas, communiquez avec le centre d'autorisation Moneris au **1 866 802-2637** et suivez les instructions pour obtenir une autorisation de **code 10**.
- Si le message « **Appeler** » ou « **Appeler Centre** » s'affiche, téléphonez au **1 866 802-2637** pour obtenir le numéro d'autorisation.
- Si vous pensez qu'il s'agit d'une activité frauduleuse ou si vous avez une question à l'égard de l'autorisation de la transaction, demandez pour une autorisation de code 10.
- Si le centre d'autorisation vous demande de garder la carte du client, tentez de le faire sans qu'il y ait de problème. Ne vous mettez jamais en danger.

Transactions manuelles

Si vous utilisez un terminal PDV pour traiter les transactions, votre limite de plancher est zéro et vous devez obtenir un numéro d'autorisation pour chaque transaction.

REMARQUE IMPORTANTE :

- Il est important de se rappeler qu'une autorisation ne signifie pas que le titulaire lui-même effectue l'achat ni qu'il s'agit d'une carte authentique. Une autorisation signifie seulement que le crédit est disponible et que la carte n'est pas bloquée. Pour aider à détecter et à prévenir toute fraude, on devrait ajouter au processus d'autorisation certains outils et contrôles.

- La bande magnétique est un élément actif de la sécurité de la carte, ce qui rend le traitement manuel approprié seulement dans le cas où la bande magnétique d'une carte ne peut être lue.
- **Lorsque la bande magnétique d'une carte ne peut être lue, une facture manuelle doit être remplie qui comprend les éléments suivants :**
 - Date
 - Empreinte de la carte
 - Détails de la transaction
 - Valeur totale en dollars de la transaction, y compris les taxes et autres frais
 - Signature du titulaire de carte
 - Numéro d'autorisation
 - Numéro du commerçant

Remarque : si vous utilisez normalement un terminal PDV pour traiter les transactions, une fois la facture manuelle remplie, vous devez :

- introduire manuellement la transaction, y compris le numéro d'autorisation dans votre terminal PDV; et
- écrire « copie avec preuve » sur le reçu du terminal.

CONSEIL :

Lorsque la bande magnétique d'une carte ne peut être lue, c'est habituellement parce que :

- le lecteur de bande magnétique est brisé ou sale
- le lecteur est obstrué, empêchant un glissement parfait
- l'associé aux ventes a mal glissé la carte
- la bande magnétique de la carte est endommagée.

**INFORMATION IMPORTANTE :**

C'est une bonne idée de surveiller votre taux régulièrement. Moneris offre des services de relevés et de rapports en ligne via l'outil Marchand direct. Grâce à cet outil, vous pouvez consulter vos transactions par cartes de crédit et de débit en ligne. L'information est mise à jour tous les jours, ce qui est idéal pour équilibrer et surveiller le flux de trésorerie, et vous pouvez aussi importer ces données dans des chiffriers aux fins de prévisions et d'analyse des tendances. Vous pouvez visionner une démo en ligne à l'adresse <http://www.moneris.com/mdirect/tour>; pour obtenir de plus amples renseignements, veuillez communiquer avec le centre de vente Moneris au **1 866 666-3747** (1 866 MONERIS).

**Saisie manuelle**

Dans les cas où l'autorisation en ligne est disponible, mais le lecteur de carte ne peut lire la carte, vous pouvez saisir manuellement le numéro de carte dans votre terminal PDV.

Les transactions saisies manuellement (par opposition aux cartes glissées) comportent certains désavantages, notamment :

- Un risque accru de fraude et/ou contrefaçon.
- Possibilité d'entraîner une augmentation des coûts, car votre taux d'escompte de commerçant est calculé en fonction de votre capacité de lire et de transmettre des données par bande magnétique directement du PDV.
- Cette méthode est moins efficace, car les transactions prennent plus de temps et sont susceptibles d'erreurs.
- Cette méthode peut entraîner une perte de ventes, car le taux de refus d'autorisation est plus élevé pour les transactions entrées manuellement.

Si une transaction est entrée manuellement, vous devez obtenir l'empreinte de la carte sur la facture. Si le montant est contesté ultérieurement, l'empreinte prouve que la carte était présente et aide à vous protéger contre les débits compensatoires.

Dans le cas des autorisations, la transaction doit être approuvée et le code d'approbation doit paraître sur la facture.

Si le nombre de transactions entrées manuellement par rapport au nombre total de transactions est supérieur à 1 % des ventes ou des transactions entrées par lecteur de carte, tentez de déterminer la raison.

Étapes pour éviter la saisie manuelle

- Vérifiez régulièrement le lecteur de bande magnétique du terminal PDV pour vous assurer de son bon fonctionnement.
- Nettoyez les lecteurs régulièrement avec la carte de nettoyage de lecteur offerte avec le terminal. Vous pouvez acheter ces cartes et d'autres fournitures auprès de Moneris. Visitez le site www.shopmoneris.com ou communiquez avec nous au : **1 866 319-7450**.
- Positionnez le lecteur de sorte à assurer le glissement complet de la carte en vous assurant de retirer tout objet pouvant causer une obstruction.
- Ne permettez pas au personnel de déposer des articles près du lecteur qui pourraient le salir ou l'endommager, particulièrement de la nourriture et des breuvages.
- Ne placez pas le lecteur près de tout équipement qui désactive les dispositifs antivols magnétiques fixés à la marchandise.





Aidez les clients à « protéger leur nip »

Les titulaires de cartes doivent être en mesure d'introduire leur numéro d'identification personnelle (NIP) à l'abri du regard des autres.

Assurez-vous que le terminal PDV est installé de sorte que vos clients puissent facilement cacher le clavier NIP ou que des guides de protection de la confidentialité soient installés. Si votre clavier NIP est fixe, assurez-vous que les protecteurs de confidentialité sont installés.

Laissez vos clients tenir le clavier NIP jusqu'à ce que le message final d'approbation/refus s'affiche.

Remettez toujours à votre client une copie du reçu de la transaction ainsi que sa carte.

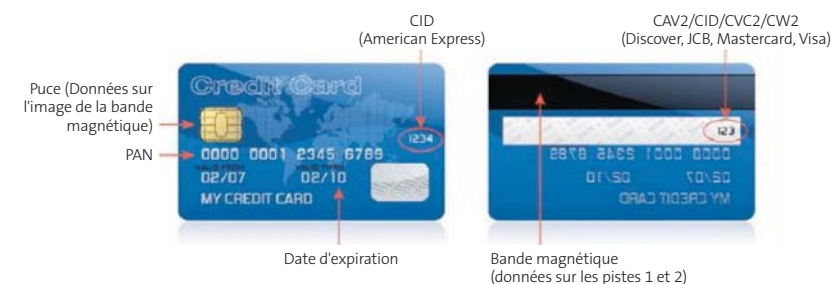
Marches à suivre en cas d'interruption

Dans le cas d'une panne du système, les marches à suivre suivantes doivent être respectées pour l'acceptation des cartes de crédit :

- Prenez une empreinte manuelle.
- Communiquez avec le Centre d'autorisation pour une autorisation verbale et inscrire le numéro d'autorisation sur la facture manuelle. Composer le **1 866 802-2637**.
- Demandez au titulaire de carte de signer la copie avec l'empreinte.
- Lorsque le service/système est rétabli, introduisez la transaction dans votre dispositif PDV en utilisant le numéro d'autorisation attribué.
- Assurez-vous que l'information est visible et parfaitement lisible sur la facture.
- Veuillez consulter la section sur les transactions manuelles du guide d'utilisation pour obtenir l'information requise sur une facture.

Protection de votre entreprise contre la fraude

Comment identifier les caractéristiques de sécurité



Comportement suspect du client

Soyez vigilant et observez vos clients.

La détection de la fraude par carte de crédit peut, de façon générale, être répartie en deux groupes. Premièrement, les cartes perdues ou volées lorsque la carte est légitime, mais il ne s'agit pas du titulaire de carte autorisé. Deuxièmement, des cartes par contrefaçon lorsque la carte a été produite de façon illégale, mais ressemble et fonctionne comme une carte authentique.

Notre expérience démontre que les fraudeurs de cartes de crédit présentent une ou plusieurs des caractéristiques suivantes :

CARTES PERDUES OU VOLÉES

Achats sans distinction

- Le client choisit des articles au hasard et peut sembler nerveux ou pressé.
- Le client peut effectuer ses achats au moment où le magasin est sur le point de fermer.
- Dans un magasin de vêtements, le client peut avoir choisi les articles sans égard à la taille, la couleur, les styles ou le prix. Il n'a peut-être pas essayé les vêtements.
- Lors d'achats d'équipement électronique coûteux, le client ne demande pas les spécifications techniques ni de l'information sur les garanties.
- Pour les gros articles, il peut demander une livraison immédiate et ne demande pas d'aide.

La carte

- Le titulaire de carte peut retirer la carte de sa poche plutôt que de son portefeuille ou sac à main.
- Le titulaire de carte peut signer le reçu de façon non naturelle ou délibérée.
- La signature sur la carte et celle sur le reçu ne correspondent pas.
- Le nom sur la carte peut être celui d'une femme, mais c'est un homme qui la présente, et vice versa.
- Le titulaire de carte peut au hasard facturer des articles dispendieux sur une carte nouvellement émise.

CARTES FRAUDULEUSES

Confiance

- Le titulaire de carte peut ressembler à une personne qui achète des articles coûteux. Il peut être bien vêtu et confiant.
- Il est confiant que son achat sera approuvé, car il participe à la production de ces cartes de haute qualité.
- Il passe beaucoup de temps à regarder et peut venir chercher l'article le jour suivant.

Retour au magasin pour d'autres articles

- Le titulaire de carte peut souvent revenir avec des amis qui détiennent aussi des cartes frauduleuses, indiquant qu'ils trouvent les articles et les prix intéressants.

REMARQUE IMPORTANTE :

- Ces caractéristiques peuvent être présentes pour une transaction légitime, au même titre que l'absence de ces caractéristiques ne garantit pas le fait qu'il s'agit d'une transaction légitime. Le bon sens est le meilleur guide.
- Si vous ou vos employés ont des doutes, donnez-vous et non le client, le bénéfice du doute. Communiquez avec le Centre d'autorisation pour obtenir une autorisation de code 10 (consultez la marche à suivre pour les cartes perdues, volées et oubliées) qui est utilisée lorsque vous soupçonnez une transaction frauduleuse.

Marches à suivre en cas de carte perdue, volée ou oubliée

Procédures code 10

- Le code 10 est un code universel qui permet aux commerçants d'alerter un centre d'autorisation d'une transaction frauduleuse possible sans alarmer la personne qui présente la carte aux fins de paiement.

PROTECTION DE VOTRE ENTREPRISE

Même lorsque les procédures adéquates sont utilisées lorsqu'une carte est glissée dans un terminal et qu'une signature correspondante est obtenue sur la facture, il n'y a aucune garantie qu'il s'agit d'une transaction légitime. En cas de doute de fraude, initiez une demande d'autorisation de code 10.

Dans la plupart des cas, les transactions sont légitimes, mais vous devez savoir quelles mesures prendre dans le cas d'une demande d'autorisation de code 10 :

- Communiquez avec le Centre d'autorisation Moneris au **1 866 802-2637** et suivez les instructions pour une demande de code 10.
- Identifiez l'appel comme une demande d'autorisation de code 10.
- Gardez la carte entre vos mains pendant le processus d'autorisation. Demeurez calme et nonchalant et courtois avec le client.
- Votre appel pourrait être transféré. Ne raccrochez pas.
- On vous posera une série de questions nécessitant une réponse oui ou non afin de vérifier l'authenticité de la carte.
- Suivez les instructions données au téléphone.
- Ne tentez pas de retenir ni d'appréhender le titulaire de carte.
- Il est possible qu'une récompense soit versée pour le retour d'une carte perdue, volée ou frauduleuse.

Si pour une raison quelconque vous mettez en doute une transaction ou le titulaire de la carte, communiquez avec le service d'autorisation de Moneris.





Cartes oubliées

Si une carte est oubliée dans votre établissement :

- Remettez la carte au client s'il la réclame dans un délai de 24 heures et présente une pièce d'identification appropriée.
- Si la carte n'est pas réclamée dans un délai de 24 heures, coupez la carte en deux et retournez-la à l'adresse indiquée ci-dessous :

Solutions Moneris

À l'attention de : Récompenses destinées au commerçant
PO Box 219 Stn D
Toronto, ON M6P 3J8

Assurez-vous d'indiquer les éléments suivants lorsque vous retournez la carte :

- Nom du magasin
- Adresse
- Nom de la personne qui a conservé la carte
- Numéro de téléphone
- À l'attention de : Récompenses destinées au commerçant

Prenez note que les récompenses sont versées à la discrétion de l'émetteur de cartes.

Doute d'écrémage

L'écrémage est le transfert des données électroniques, d'une bande magnétique à une autre en utilisant un lecteur de cartes aux fins de fraude. Les stations de service et les restaurants sont souvent des cibles d'écrémage lorsqu'un employé travaille seul pendant de longues périodes de temps souvent la nuit ou les fins de semaine.

OBTENTION DE L'INFORMATION DE LA BANDE MAGNÉTIQUE

- Il existe une technologie de plus en plus sophistiquée disponible aujourd'hui qui peut être utilisée pour l'écrémage de l'information de la bande magnétique des cartes de crédit et de débit soit via un terminal PDV altéré ou fictif.

SOYEZ VIGILANT

- Il y a maintenant des dispositifs d'écrémage portatifs qui captent des données de la bande de la carte via une ligne hôte pour les autorisations.
- Ces dispositifs ont la capacité de fonctionner pendant de longues périodes de temps et ils peuvent même avoir une très grande capacité de stockage.
- Vérifiez le dessous du comptoir qui peut être un endroit pratique pour cacher les dispositifs d'écrémage.

CARTES DE DÉBIT

Outre l'information sur la bande magnétique, les personnes qui s'adonnent à l'écrémage doivent aussi obtenir le NIP du titulaire de carte.

Habituellement, ceci s'effectue de la façon suivante :

- « Surfer le NIP », c.-à-d. se pencher sur l'épaule d'un titulaire de carte pour voir le NIP – un employé ou un complice se penche sur l'épaule du titulaire lorsque celui-ci entre son NIP sur le clavier NIP.
- L'utilisation de la lentille d'une mini caméra pour capter le NIP. L'appareil photo est placé soit dans un orifice au plafond ou sur une étagère au-dessus du comptoir et du clavier NIP. Avec ce type d'équipement, le clavier NIP doit demeurer dans une position fixe sur le comptoir afin que la lentille puisse capter les numéros saisis par le titulaire de carte.

Pour obtenir un complément d'information sur l'écrémage, visitez www.moneris.com

Commande postale/téléphonique et fraude de commerce électronique

Plusieurs des mécanismes de sauvegarde contre la fraude dans les environnements de vente au détail traditionnels ne s'appliquent pas aux environnements sans carte présente lors d'une transaction, notamment les commandes postales et téléphoniques ainsi que les commandes par commerce électronique. Ces transactions ne nécessitent pas une présence face à face ou la carte présente comme telle, alors il y a un anonymat relié à la transaction.

Tous les commerçants qui traitent des commandes postales et téléphoniques et de commerce électronique doivent obtenir l'autorisation pour la transaction.

Si les fonds sont disponibles et que la carte n'a pas été signalée comme étant perdue ou volée, il est fort probable que la transaction soit approuvée par l'émetteur de la carte.

Il est important de noter qu'une autorisation ne signifie pas que c'est le titulaire actuel de la carte qui effectue l'achat ni qu'il s'agit d'une carte légitime. Un numéro d'autorisation signifie seulement que le crédit est disponible et que la carte n'est pas retenue.

Pratiques exemplaires de prévention de la fraude électronique

- Autorisez toutes les transactions, qu'importe le montant.
- Mettez en œuvre les outils de prévention anti-fraude applicables (SVA, CVV2, VpV, Code sécurisé).
- Fracturez le titulaire de compte seulement pour les biens expédiés (pré-autorisation/saisie).
- Créditez le compte du titulaire de compte immédiatement s'il s'agit d'un retour de marchandise ou en cas de litige de la somme facturée.
- Si possible, expédiez les produits avec un service de messagerie qui obtient la signature comme preuve de livraison.



- Maintenez des dossiers détaillés de tous les bons de commande, bordereaux de marchandises, reçus de livraison et informations sur le client tels que l'adresse, numéro de téléphone, signature, factures pertinentes et adresse de courriel.
- Élaborez et maintenez une base de données des titulaires de carte ou des fichiers sur l'historique du compte pour suivre les habitudes d'achat et comparer les ventes individuelles pour des signes de fraude possible.
- Faites le suivi des adresses IP.
- Établissez et renforcez les contrôles appropriés auprès des employés qui ont accès à la base de données des clients et aux numéros de comptes.
- Suivez les normes de sécurité des données du secteur des cartes de paiement pour garantir la sécurité de votre système. (Consultez aussi la section sur la sécurité des données du secteur des cartes de paiement de ce guide d'utilisation).

EN CAS DE DOUTE DE FRAUDE

En cas de doute ou si vous trouvez que les circonstances sont douteuses, demandez au client de fournir des renseignements supplémentaires, tels que :

- son numéro de téléphone pour le joindre pendant la journée et en soirée, lequel peut être vérifié via l'assistance téléphonique ou www.canada411.ca;
- le nom de la banque au verso de sa carte ou vous pouvez aussi :
 - demander la vérification d'un nom et d'une adresse (voir Service de vérification d'adresses à la section portant sur le commerce électronique).
 - si le doute persiste, ne traitez pas la vente.





Débits compensatoires

Survol

Un débit compensatoire survient lorsqu'un crédit ou un paiement pour lequel une autorisation a été obtenue est annulé.

Il peut survenir en raison d'une contestation de la part d'un client (titulaire de carte) ou lorsque les marches à suivre appropriées d'acceptation ou d'autorisation n'ont pas été suivies. Ces débits sont traités dans votre compte bancaire de commerçant automatiquement et s'accompagnent d'un avis de débit et d'un rapport sommaire de débit compensatoire qui doit être transmis par télécopieur ou courrier.

Dans certains cas, les débits compensatoires peuvent être annulés par un crédit à votre compte de commerçant si vous fournissez la documentation appropriée dans les délais établis dans votre entente de commerçant.

Si vous recevez un avis de débit compensatoire, nous recommandons que vous preniez les mesures immédiatement.

L'avis de débit compensatoire comporte des instructions claires sur l'information que vous devez fournir afin de créditer le débit compensatoire.

Si vous avez besoin d'aide ou de l'information sur un débit compensatoire, n'hésitez pas à communiquer avec le **Centre de service à la clientèle** au **1 866 319-7450**.

Vous trouverez dans ce guide d'utilisation une liste des codes de débit compensatoire les plus courants. Les codes ont été répartis en cinq catégories et comprennent de l'information intéressante sur les pratiques exemplaires à suivre pour minimiser la possibilité de pertes financières causées par les débits compensatoires.

Prenez quelques instants pour lire cette section et vous familiariser avec les conseils importants qui peuvent vous aider à éviter les débits compensatoires.

Demandes de copies de factures

De temps à autre, votre banque peut vous demander de fournir une copie de la facture ou le registre de transaction pour une vente effectuée dans votre lieu d'affaires. Ces demandes sont généralement initiées par les titulaires de cartes qui ont besoin de vérifier ou de clarifier des frais portés à leur compte de carte de crédit ou d'autres institutions financières qui émettent des cartes de paiement afin de clarifier des situations de fraude ou de contestation.

En tant que commerçant qui accepte les cartes de paiement, vous devez conserver les copies de toutes les factures/reçus de transaction pour un minimum de 18 mois à partir de la date de la transaction et répondre à la demande dans les délais conformes à votre entente de traitement.

Si vous recevez une demande de copie de facture du service responsable des copies ou de la sécurité, répondez immédiatement en transmettant une copie lisible du document qui a été utilisé pour facturer la transaction au compte du titulaire de carte. Parmi les exemples de ces documents, nous retrouvons les factures manuelles, les reçus de transaction de terminal PDV, les factures, les références, les bons de commande, etc.

Le document doit comprendre l'information suivante :

- Date de la transaction
- Numéro de la carte
- Numéro d'autorisation
- Valeur totale de la transaction, y compris les taxes et autres frais
- Inclure la demande de facture

REMARQUE IMPORTANTE :

- si vous recevez une demande de facture pour un article et que vous avez déjà traité un remboursement, veuillez transmettre à Moneris toute la documentation applicable concernant ce remboursement.

TÉLÉCOPIEZ L'INFORMATION AUX NUMÉROS DE TÉLÉPHONE SUIVANTS SELON LE CAS :

Transactions MasterCard :
416-232-8474 (Toronto et région) ou
1 888 224-3919 (Ensemble du Canada)

Transactions Visa :
416-231-9329 (Toronto et région) ou
1 866 596-1116 (Ensemble du Canada)

Conservez votre rapport de confirmation de télécopie comme preuve de copie.

LES RÉPONSES DOIVENT ÊTRE TRANSMISES PAR COURRIER À :

Centre de résolution des débits compensatoires – comptes MasterCard
P.O. Box 1400, Station "D" Etobicoke, Ontario M9A 5B6

Centre de résolution des débits compensatoires – comptes Visa
P.O. Box 410 Station "A" Toronto, Ontario M5W 1C2

Le respect des échéanciers est essentiel! Tout manquement de fournir une copie de l'information demandée dans les délais prescrits dans votre entente de traitement pourrait entraîner des débits compensatoires irréversibles débités à votre compte bancaire. Afin de vous assurer de recevoir les demandes de factures et les avis de débits compensatoires, veuillez mettre à jour régulièrement l'information sur votre adresse postale, numéros de fax et de téléphone.

Veuillez porter une attention particulière et fournir la documentation appropriée à Moneris pour répondre aux exigences des divers codes de demande de factures.

CONSEILS UTILES POUR LES DÉBITS COMPENSATOIRES ET LES DEMANDES DE COPIES DE FACTURES

- Pour éviter toute confusion pour le titulaire de carte concernant la transaction, assurez-vous que vos dépôts sont effectués tous les jours.
- Pour éviter toute confusion à l'égard de la description du commerçant sur le relevé du titulaire de carte, assurez-vous que le nom de l'entreprise imprimé sur le reçu de caisse correspond au nom de votre magasin.
- Si vous découvrez qu'une transaction a été effectuée en double, traitez immédiatement un crédit sur le compte du titulaire de carte.



- Si on vous demande de fournir un reçu pour une carte qui n'a pas initialement été glissée dans votre terminal PDV, assurez-vous de fournir le reçu manuel pour confirmer que l'empreinte de carte a été prise et que la carte était présente dans votre établissement au moment de la vente.
- Pour éviter un débit compensatoire irréversible, assurez-vous que les délais de remise de copies et de demandes de factures sont suivis et que vos réponses sont transmises dans les délais prescrits.
- Répondez à toutes les demandes de copies même si ceci semble être fait en double.

Pour toute assistance à l'égard des demandes de copie/facture ou débit compensatoire ou si vous désirez recevoir ces documents par télécopieur, veuillez communiquer avec le service pour les commerçants au 1 866 319-7450.

Codes de raisons de débit compensatoire

CODES DE RAISONS DE DÉBIT COMPENSATOIRE MASTERCARD

N° de code	Description
01	Information sur la transaction demandée non reçue
02	Information demandée/requise illisible ou manquante
08	Autorisation demandée/requise non obtenue
12	Numéro de compte pas au dossier
31	Montant de la transaction diffère
34	Traitement en double
35	Carte non valide ou échue
37	Autorisation du titulaire de carte manquante
40	Traitement frauduleux des transactions
41	Annulation d'opérations périodiques
42	Présentation en retard
46	Code de devise de transaction valide non fourni
49	Activité du commerçant douteuse
50	Crédit inscrit comme un achat
53	Diffère de la description/défectueux
55	Article non reçu
57	Transaction téléphonique activée par carte de crédit
59	Services non rendus
60	Crédit non traité
62	Transaction par contrefaçon – fraude PDV de la bande magnétique
63	Titulaire de carte inconnu – fraude potentielle

CODES DE RAISONS DE DÉBIT COMPENSATOIRE VISA

N° de code	Description
33	Traitement en double
35	Signature manquante
38	Produits/Services non reçus par le titulaire de carte ou la personne autorisée
39	Empreinte manquante
44	Transaction dépasse la limite de plancher et non autorisée/Autorisation refusée
45	Copie non reçue dans les délais prescrits
49	Autre

Pratiques exemplaires pour éviter les débits compensatoires :

- Obtenez l'autorisation adéquate (avec le montant de la transaction, la date appropriée de validation et d'expiration) pour toutes les transactions le jour de la transaction.
- Éviter de traiter des transactions pour lesquelles les réponses « refusée » ont été reçues.
- Assurez-vous que toutes les cartes acceptées comprennent le logo et les caractéristiques de sécurité.
- Assurez-vous que tous les reçus de caisse sont lisibles et clairement imprimés avec les numéros de cartes ou glissés ou insérés dans votre terminal électronique.
- Un écart de 20 pourcent est permis pour les restaurants aux fins des pourboires seulement. Le montant réel (ou final) ne doit pas dépasser 20 % du montant autorisé.
- Assurez-vous que toutes les transactions en personne sont terminées au complet avec le glissement de la carte ou l'insertion de celle-ci dans un terminal PDV ou avec une empreinte manuelle et la signature du titulaire de carte
- Assurez-vous que toutes les caractéristiques ou descriptions des biens et/ou services écrites et verbales dans le cas de transaction sans la présence de la carte sont détaillées, exactes et non trompeuses.
- Assurez-vous que les produits expédiés sont reçus et que la documentation est signée par le titulaire de carte. (Si possible, la réception de la marchandise peut-être confirmée en obtenant l'empreinte de la carte au moment de la livraison).
- Assurez-vous que tout produit expédié correspond à la description de celui-ci et est livré dans un état satisfaisant.
- Assurez-vous que tous les services sont fournis dans les délais prescrits. Les services payés d'une autre façon ne devraient pas être facturés à la carte du titulaire de carte.
- Évitez de traiter une transaction plus d'une fois; regroupez vos dépôts quotidiens pour vous assurer que les transactions sont traitées correctement. Si vous découvrez une transaction en double, nous recommandons que vous traitiez immédiatement un remboursement par crédit au compte du titulaire de carte et que vous avisiez le titulaire de carte du remboursement pour les aider à éviter un redressement.
- Assurez-vous que tous les dépôts électroniques (ventes et remboursements) sont déposés via votre terminal PDV dans les trois jours ouvrables suivant la date de la transaction.
- Assurez-vous que tous les remboursements sont introduits comme crédit/remboursement et non une vente via un terminal PDV.

Programmes de débit compensatoire excessif

Les marques de cartes ont mis de l'avant divers programmes anti-fraudes et de débit compensatoire pour les aider à surveiller les activités des détenteurs de cartes. Les programmes comprennent :

PROGRAMMES VISA

Programme de rendement anti-fraude à l'intention des marchands (PRAFM)

Ce programme comprend les seuils pour le rendement anti-fraude d'un commerçant et un cadre de travail de conformité pour s'assurer de la résolution en temps opportun afin de réduire adéquatement les niveaux de fraude.

Le programme comporte deux volets : un premier volet qui répond au rendement anti-fraude sur le marché local et un volet qui correspond au rendement anti-fraude interrégionale/outre-frontière.

Le volet anti-fraude local mesure les activités de fraude et de vente à l'échelle nationale et identifie les commerçants qui ne respectent pas les seuils de rendement de Visa Canada. Les commerçants ont une période de temps spécifique pour résoudre les problèmes de performance, sinon des amendes peuvent s'appliquer.

Le volet anti-fraude interrégional/outre-frontière mesure l'activité frauduleuse et les ventes entre les régions Visa et identifie les commerçants qui n'ont pas atteint les seuils de rendement anti-fraude de Visa Canada.

Ce volet comporte deux méthodes de mesure du rendement :

- **Seuil minimum de rendement anti-fraude.**
Ce seuil est conçu pour s'assurer de la résolution en temps opportun des problèmes qui surviennent régulièrement en raison de pratiques de contrôle de la fraude et d'acceptation interrégionale/outre-frontière qui ne respectent pas les normes.
- **Seuil de rendement anti-fraude excessif.**
Ce seuil met en œuvre des mesures immédiates contre les commerçants qui présentent un risque de fraude interrégionale élevé pour l'émetteur de carte en fonction du seuil de norme de rendement établi par Visa.

Les commerçants ont une période de temps précise pour redresser les problèmes de rendement, sinon la responsabilité pour le débit compensatoire et des amendes peuvent s'appliquer.

Programme mondial de contrôle des débits compensatoires des commerçants (PMCDCC)

VISA surveille les transactions internationales afin d'identifier les commerçants qui génèrent un nombre excessif de débits compensatoires (relativement à ces types de transactions).

Un commerçant fera partie de ce programme s'il dépasse les niveaux d'activités de rendement mensuel suivants pour des transactions internationales : 100 transactions et 2,5 % de ratio de débits compensatoires par rapport aux transactions.

Les commerçants ont une période de temps spécifique pour régler les problèmes de rendement, sinon la responsabilité de débits compensatoires et des amendes peuvent s'appliquer.

PROGRAMMES MASTERCARD

Programme mondial de vérification des commerçants (PMVC)

Le programme mondial de vérification des commerçants est un programme de gestion et de surveillance de la fraude qui identifie les commerçants qui dépassent un niveau acceptable de fraudes dans un mois donné en fonction de critères établis pour le programme.

Les commerçants ont une période de temps précise pour redresser les problèmes de performance, sinon la responsabilité à l'égard de débits compensatoires et des amendes peuvent s'appliquer.

Programme de débits compensatoires excessifs (PDCE)

Le programme de débits compensatoires excessifs (PDCE) est conçu pour surveiller étroitement de façon continue les rendements à l'égard des débits compensatoires au niveau du commerçant et à déterminer rapidement si un commerçant dépasse ou devrait dépasser les seuils mensuels de débits compensatoires.

Le « ratio débit compensatoire à transaction » (RDCT) est le nombre de débits compensatoires MasterCard reçu d'un commerçant dans un mois donné divisé par le nombre de transactions de ventes MasterCard du mois précédent. Un commerçant est considéré comme « commerçant avec débits compensatoires excessifs » (CDCE) si au cours de chaque mois sur deux mois consécutifs, le commerçant a un minimum RDCT de 1 % et a subi au moins 50 débits compensatoires au cours de chaque mois.

Cette désignation est maintenue jusqu'à ce que le RDCT du commerçant avec débits compensatoires excessifs soit inférieur à 1 % pendant deux mois consécutifs.

REMARQUE IMPORTANTE :

- Les programmes de contrôle Visa et MasterCard indiqués ci-dessus sont assujettis à des amendes ou frais et structure d'évaluation différents.
- Ces programmes sont assujettis à des changements de temps à autre en ce qui a trait aux critères de contrôle et aux seuils.

Autres programmes

SIGNATURE NON REQUISE (SNR) VISA

Cette catégorie permet aux commerçants admissibles de traiter des transactions par carte Visa inférieures ou égales à 25 \$ CA rapidement et de façon pratique; de plus, vous êtes protégé contre certains débits compensatoires pour ces transactions qui sont admissibles au programme. **Dans le programme SNR :**

- la carte peut être glissée et la transaction est autorisée;
- aucune signature du titulaire de carte n'est requise;
- le reçu du titulaire de carte est seulement fourni sur demande.

Transactions SNR admissibles

Pour être admissible au programme SNR, une transaction doit comporter les caractéristiques suivantes :

- la valeur totale de la transaction est inférieure ou égale à 25 \$ CA y compris le pourboire et les taxes;
- la transaction est effectuée dans un environnement face à face;
- la carte émettrice provient du Canada;
- les données du compte de carte sont captées électroniquement;
- autorisation complète;
- la transaction est effectuée par un commerçant qui est doté d'un code de catégorie de commerçant spécifique (CCC).
Pour obtenir une liste des CCC approuvés, visitez www.visa.ca.

Toute transaction qui ne répond pas aux critères ci-dessus n'est pas admissible comme transaction SNR. Les transactions qui sont saisies manuellement ou effectuées dans des terminaux autonomes ne sont pas des transactions SNR et sont assujettis aux exigences des règlements d'exploitation de carte Visa.

Pour obtenir de plus amples renseignements sur le programme SNR, visitez : <http://visa.ca>

SERVICE DE PAIEMENT RAPIDE (SPR) MASTERCARD

Une transaction SPR s'effectue de la même façon qu'une transaction MasterCard standard, sauf plus rapidement, car vous n'avez pas besoin de demander la signature du client pour les transactions dont le montant est égal ou inférieur à 50 \$ CA. Il vous suffit de glisser la carte MasterCard et de la remettre au titulaire de carte. Aucune signature ni reçu n'est requis. Toutefois, si le client demande un reçu, vous devez lui en fournir un. **Pour les transactions SPR identifiées adéquatement égales ou inférieures à 50 \$ CA :**

- l'obtention de la signature du titulaire de carte est réservée à la discrétion du commerçant;
- fournir un reçu est à la discrétion du commerçant; toutefois, le commerçant doit fournir un reçu à la demande du titulaire de carte;
- la transaction doit être effectuée dans un environnement face à face.

Pour obtenir un complément d'information sur le programme SPR/PayPass et pour obtenir une liste des codes de catégorie de commerçant admissibles à ce programme et les limites de protection de débit compensatoire correspondantes, visitez : <http://www.mastercard.com>

Règles et réglementation à l'égard de la conformité

■ Troncation du numéro de compte principal (NCP) (masquage de carte)

Le numéro de compte principal (NCP) paraît sur les reçus de transactions électroniques. Chaque marque de carte a ses exigences spécifiques sur la façon de masquer le NCP.

Visa exige qu'au moins quatre chiffres du NCP soient déguisés ou supprimés sur la copie du reçu du titulaire de carte.

MasterCard exige que tous les chiffres, sauf les quatre derniers du NCP soient déguisés ou supprimés sur la copie du titulaire de carte.

Interac indique qu'une version abrégée du NCP peut être utilisée sous réserve qu'elle soit suffisante pour identifier la carte spécifique utilisée pour effectuer la transaction.

Les marques de cartes nécessitent que la portion masquée du NCP soit remplacée par des caractères qui sont ni des espaces ni des caractères numériques tels « x », « * », or « # ».

■ Cartes prépayées

Les cartes Visa et MasterCard prépayées sont des cartes de paiement comportant un montant préétabli de fonds à utiliser dans tout établissement d'un commerçant qui accepte des cartes de crédit pour effectuer les achats.

Traitement d'une transaction par carte prépayée :

- Demandez au titulaire de carte le montant à déduire.
- Suivez la même procédure que dans le cas d'une transaction par carte de crédit – glissez la carte, indiquez le montant et obtenez une autorisation en ligne.
- Demandez au client de signer le reçu et vérifiez la signature par rapport à celle sur la carte.
- Si la valeur de l'achat est supérieure au solde de la carte prépayée, la transaction sera refusée. Le titulaire de carte peut diviser la transaction entre la carte prépayée et une autre méthode de paiement si votre entreprise et/ou processus d'acceptation de paiement le permet.
- Une carte prépayée peut être utilisée seulement pour des terminaux électroniques qui peuvent obtenir une autorisation en ligne immédiatement.

Pour obtenir un complément d'information sur les cartes prépayées, visitez : www.moneris.com

<http://www.mastercard.com>

<http://visa.ca>



■ Frais supplémentaires

Vous ne devez pas ajouter des frais supplémentaires à toute transaction.

■ Montant de transaction minimum/maximum

Vous n'avez pas le droit de fixer un montant de transaction minimum ou maximum pour l'acceptation d'une carte valide présentée adéquatement.

■ Transactions interdites

Une transaction interdite signifie une transaction effectuée par un commerçant ou à la suite d'une activité illégale ou interdite. Moneris vous informe de temps à autre sur les transactions interdites ou toute autre transaction que vous n'avez pas l'autorisation de traiter.

Un commerçant ne doit pas soumettre aux fins de paiement d'interchange, y compris et sans s'y limiter toute transaction qui :

- représente le refinancement ou le transfert d'une obligation existante du titulaire de carte considéré comme irrécouvrable; ou
- survient à la suite du refus d'acceptation d'un chèque personnel du titulaire de carte; ou
- survient de l'acceptation d'une carte au terminal qui dispense d'un certificat provisoire.

■ Transactions illégales ou qui nuisent à l'image de marque

Vous ne devez pas accepter le paiement par carte pour toute transaction illégale ou qui, à la discrétion des associations de cartes, pourrait endommager l'achalandage des associations de cartes ou refléter négativement sur l'image de marque.

Les associations de cartes considèrent les activités suivantes comme étant en violation de cette règle :

- La vente ou l'offre de vendre un produit ou un service autrement qu'en pleine conformité avec la loi qui s'applique à l'acquéreur, l'émetteur, le commerçant, le titulaire de carte, les cartes ou les associations de cartes.
- La vente d'un produit ou d'un service, y compris, mais s'y limiter, toute image, qui est offensive ou manque de valeur artistique sérieuse (par exemple, mais sans s'y limiter, des images d'un comportement sexuel non consensuel, exploitation sexuelle d'un mineur, mutilation non consensuelle d'une personne ou d'une partie du corps et la bestialité), ou tout autre matériel que l'association de cartes considère inacceptable à la vente en relation avec son image de marque.

■ Dépôt

Vous devez présenter des enregistrements d'une transaction valide au plus tard trois jours (horaire des banques) après la date de la transaction.

■ Vente ou échange d'information

Vous ne pouvez pas vendre, acheter, fournir ou échanger ni dévoiler de quelque façon que ce soit le numéro de compte de la carte, la transaction ou l'information personnelle d'un titulaire de carte à toute personne, sauf son acquéreur, les associations de cartes, ou en réponse à une demande officielle provenant du gouvernement. Cette interdiction s'applique aux empreintes de cartes, aux reçus de transactions, aux copies conformes, aux listes d'envoi, aux bandes, aux fichiers de base de données et tout autre média créé ou obtenu à la suite d'une transaction.

Vous ne devez pas demander ni utiliser le numéro de compte de carte ou l'information personnelle du titulaire de carte dans tout but qui est connu ou qui aurait dû être connu comme étant une action frauduleuse ou en violation des normes de l'association des cartes pour toutes fins que le titulaire de carte n'a pas autorisées.

■ Multiple reçus de vente et de dépôt – Transactions retardées

Vous devez inclure tous les achats de biens et de services dans une seule transaction de vente (y compris les taxes applicables), en un montant total sur une facture de vente unique.

Vous n'avez pas l'autorisation de traiter les transactions de vente si seulement une partie du montant est inclus sur la facture, sauf dans les cas suivants :

- le solde du montant dû est payé par le titulaire de carte au moment de la transaction de vente soit en espèces, par chèque ou les deux; ou
- le titulaire de carte demande deux factures si une partie ou la totalité des biens ou des services seront fournies à une date ultérieure. Si tel est le cas, il y aura deux factures, un dépôt peut être fait pour une facture et le paiement du solde est effectué via une seconde facture (la seconde facture est conditionnelle à la livraison des biens et/ou de la performance des services identifiés). L'autorisation est requise pour les deux factures.
- vous indiquerez sur la facture les mots « dépôt » ou « solde », au besoin. La facture libellée « solde » ne devrait pas être présentée jusqu'à ce que les biens soient livrés ou le service fourni.

■ Exigences relatives à l'autorisation

- L'autorisation doit être obtenue à la date de la transaction.
- Si l'autorisation est refusée ou si la carte n'est pas valide ou si elle est expirée, vous ne pouvez compléter la transaction.
- Votre conformité à ce guide d'utilisation et à cette section n'exclut pas les débits compensatoires en vertu de l'entente. En cas de doute, qu'importe ou non si vous avez obtenu un code d'autorisation pour la transaction, vous demeurez responsable d'une transaction, y compris, mais sans s'y limiter, les éléments suivants :
 - (i) le titulaire de carte est présent, mais n'a pas sa carte;
 - (ii) le titulaire de carte ne signe pas la facture;
 - (iii) la signature semble non autorisée ou différente de la signature sur la carte; ou
 - (iv) la carte est expirée.

■ Conversion de devises dynamiques

Si vous offrez ou vous nous demandez de fournir la possibilité d'effectuer la conversion de devises dynamique ou tout autre service de conversion de devises, vous devez :

- nous aviser avant d'offrir de tels services aux titulaires de cartes;
- informer les titulaires de cartes que le service de conversion est optionnel;
- ne pas imposer d'exigences additionnelles aux titulaires de cartes pour traiter la transaction dans la devise locale;
- ne pas utiliser d'informations ou des procédures qui feraient en sorte que le titulaire de carte choisirait les services de conversion par défaut;
- ne pas mal représenter, soit explicitement ou implicitement, que les services de conversion sont fournis par l'association de cartes;
- vous conformer à toutes les exigences pour le reçu de la transaction requis par Moneris ou l'Association de cartes de temps à autre;
- vous conformer aux autres exigences concernant les services de conversion demandées par Solutions Moneris de temps à autres ou fournies dans le cadre des règles et de la réglementation de l'Association de cartes.

■ Retour de marchandise, crédits et redressements

Dans le cas de biens et services payés par carte, vous devez suivre une politique juste de remboursement, sauf si autrement interdit par une loi applicable. Les politiques qui seront au moins égales à de telles politiques relativement aux clients qui font le paiement en devises ou par chèque, sauf si entièrement dévoilées au moment de la transaction au titulaire de carte et sous réserve que la facture comprend un avis apparent à cet effet avant de compléter la transaction.

■ Autres remarques pour les remboursements :

- L'information adéquate ne comprend pas un énoncé qui renonce au droit du titulaire de carte de contester une transaction avec son émetteur.
- Les remboursements peuvent être faits seulement sur la carte qui a été utilisée pour l'achat original des biens ou des services.

■ Transactions périodiques

Si vous convenez d'accepter des transactions périodiques du titulaire de carte pour l'achat de biens ou de services qui sont livrés ou effectués régulièrement, le titulaire de carte doit remplir et vous remettre une demande écrite pour de tels biens ou services qui seront imputés à son compte. La demande écrite doit au moins préciser la fréquence des montants de la transaction au compte du titulaire, les frais récurrents et la durée pendant laquelle la permission est accordée.

Si une transaction périodique est renouvelée, le titulaire de carte doit remplir et vous remettre une demande écrite pour continuer la facturation à son compte de tels biens ou services. Une transaction périodique peut inclure le paiement de frais périodiques tels que les primes d'assurance, des abonnements, des frais d'adhésion, des frais de scolarité ou des frais pour services publics.

Sauf tel que précisé dans ce guide d'utilisation, une transaction périodique ne peut inclure des paiements partiels effectués pour des biens ou des services achetés dans une seule transaction et ne peuvent être utilisés pour le paiement périodique de biens. L'autorisation écrite du titulaire doit être conservée pendant la durée des frais périodiques et fournie à la demande de Solutions Moneris ou des marques de cartes.

Vous ne devez pas compléter une transaction périodique initiale ou subséquente après avoir reçu un avis d'annulation du titulaire de carte ou de Solutions Moneris ou encore après avoir reçu une réponse de ne pas accepter la carte. Vous devez indiquer lisiblement sur la ligne de signature de la facture pour les transactions périodiques, les mots « transaction périodique ».

■ Dispositifs perdus ou volés

En cas d'équipement perdu ou volé, communiquez immédiatement avec Solutions Moneris au **1 866 319-7450**. S'il y a lieu, un représentant prendra des dispositions pour remplacer le dispositif manquant. Prenez note que les clients de Moneris sont responsables de la sécurité et de la sauvegarde de tout équipement loué en leur possession. Veuillez consulter les modalités de votre entente de commerçant pour obtenir de plus amples renseignements.

Normes de sécurité des données du secteur des cartes de paiement

Le PCI Security Standards Council (PCI SSC) est responsable de l'élaboration et de l'évolution continue des normes de sécurité régissant la protection des données du compte du titulaire de carte. L'organisme PCI SSC gère présentement les normes de sécurité suivantes :

- La norme de sécurité des données du secteur des cartes de paiement (SCP)
- Le programme des dispositifs d'entrée du NIP du SCP
- La norme de sécurité des données destinée aux applications de paiement du SCP

L'organisme PCI SSC est aussi responsable de la formation et de l'admissibilité d'évaluateurs et de fournisseurs spécialisés en sécurité qui évaluent la conformité du commerçant et du fournisseur de services par rapport à ces normes. L'organisme n'est pas responsable de renforcer la conformité à ces normes mais ceci relève de la responsabilité des marques de cartes.

Pour obtenir un complément d'information sur l'organisme PCI SSC, veuillez visiter www.pcisecuritystandards.org.



Norme de sécurité des données du secteur des cartes de paiement (SCP)

La norme de sécurité des données du SCP est une norme de sécurité comportant plusieurs volets qui comprennent les exigences en matière de gestion de la sécurité, des politiques, des procédures, l'architecture réseau, la conception logicielle et d'autres mesures de protection essentielles. Cette norme complète est conçue pour aider les organismes à protéger de façon proactive les données du compte du client.

Voici les douze principales exigences de la norme de sécurité des données du SCP qui doivent être suivies :

Établir et maintenir un réseau sécuritaire

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

Protéger les données des titulaires de carte

- Protéger les données conservées.
- Chiffrer la transmission des données des titulaires de carte et de l'information de nature délicate par le biais des réseaux publics.

Maintenir un programme de gestion de la vulnérabilité

- Utiliser et mettre régulièrement à jour un logiciel d'anti-virus
- Développer et maintenir des systèmes et des applications sécuritaires.

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

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

Surveiller et tester régulièrement les réseaux

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

Maintenir une politique de sécurité de l'information

- Maintenir une politique en matière de sécurité de l'information

L'information sur la norme de sécurité des données du SCP ainsi que la documentation connexe sont disponibles à l'adresse <https://www.pcisecuritystandards.org>.

Stockage des données du titulaire de carte

Le tableau suivant illustre les éléments utilisés régulièrement et les données d'authentification confidentielles; il indique aussi qu'il est permis ou non de mettre en mémoire chaque élément; et si chaque élément de données doit être protégé.

Lignes directrices des éléments de données du titulaire de carte

	Éléments de données	Stockage permis	Protection requise	Exigences de la norme de sécurité des données SCP 3.4
Titulaire de carte	Numéro de compte principal	Oui	Oui	Oui
	Nom du titulaire de carte ¹	Oui	Oui ¹	Non
	Code de service ¹	Oui	Oui ¹	Non
	Date d'expiration ¹	Oui	Oui ¹	Non
Données d'authentification confidentielle ²	Bande magnétique complète ³	Non	S.O.	S.O.
	CAV2/CVC2/ CVV2/CID	Non	S.O.	S.O.
	BLOQUER NIP	Non	S.O.	S.O.

¹Ces éléments de données doivent être protégés s'ils sont mis en mémoire conjointement avec le numéro de compte principal. Cette protection doit être conforme aux exigences de la norme de sécurité des données du SCP pour la protection générale de l'environnement du titulaire de carte. De plus, d'autres lois (par exemple, celles reliées à la protection des données personnelles, la vie privée, le vol d'identité ou la sécurité des données) peuvent exiger une protection spécifique de ces données ou le dévoilement adéquat des pratiques d'une compagnie si des données personnelles du consommateur sont recueillies pendant les activités d'affaires courantes. Toutefois, cette norme ne s'applique pas si les numéros de comptes principaux ne sont pas mis en mémoire, traités ou transmis.

²Les données d'authentification confidentielles ne doivent pas être mises en mémoire à la suite d'une autorisation (même si elles sont chiffrées).

³Données complètes de la bande magnétique, images de la bande magnétique sur la puce, ou ailleurs.

Fournisseurs de services

Un fournisseur de services stocke, traite ou transmet les données du titulaire de carte au nom des commerçants ou des fournisseurs de services. Tous les fournisseurs de services doivent se conformer à la norme de sécurité des données du SCP. De plus, tous les fournisseurs de services doivent valider leur conformité à la norme de sécurité des données du SCP via les services d'un évaluateur de sécurité qualifié. Il relève de la responsabilité du commerçant de s'assurer que tout fournisseur de services utilisé pour mettre en mémoire, traiter ou transmettre les données du titulaire de carte exploite ses activités conformément à la norme à la norme de sécurité des données du SCP.

Programmes de conformité de marques de cartes

Les marques de carte ont élaboré leurs propres programmes de conformité pour s'assurer que les commerçants et fournisseurs de services sont conformes à la norme de sécurité des données du SCP. Chaque programme comporte des exigences de validation spécifiques qui doivent être suivies afin que les associations de cartes reconnaissent la certification en regard de la norme de sécurité des données du SCP. Tous les commerçants et fournisseurs de services qui mettent en mémoire, traitent ou transmettent des données sur le titulaire de carte doivent se conformer à la norme de sécurité des données du SCP.

Pour obtenir un complément d'information sur les programmes de conformité de marques de cartes, visitez :

Programme de sécurité de l'information concernant les comptes (SIC) de Visa Canada (Account Information Security Program (AIS) – www.visa.ca/ais)

Programme de protection des données MasterCard (Site Data Protection Program (SDP) – www.mastercard.com/sdp)

Bris de sécurité

La compromission des données d'un compte correspond à de l'information sur le titulaire du compte à laquelle une personne a eu accès sans autorisation, soit par un employé mécontent, un concurrent malicieux ou un pirate incontrôlé. Les bris de sécurité peuvent prendre la forme d'un bris de système ou des attaques électroniques délibérées sur les communications ou les systèmes de traitements de l'information ou il peut s'agir d'un bris physique ou du matériel papier, des dispositifs de traitements des paiements ou des systèmes informatiques contenant les données des titulaires de cartes sont physiquement volés.

Les entreprises qui soupçonnent ou confirment un bris de sécurité doivent prendre des mesures rapidement afin de prévenir l'exposition additionnelle des données du titulaire de carte :

- Contenez et limitez immédiatement l'exposition.
- Avertissez toutes les parties nécessaires immédiatement, y compris Moneris.
- Fournissez à Moneris une description détaillée des événements et une liste de tous les numéros de cartes qui peuvent avoir été touchées.
- Élaborez un plan de redressement pour répondre aux problèmes de sécurité qui ont causé le bris de sécurité.

Si vous avez subi un bris de compromission de données suspect ou confirmé, communiquez avec le centre de service à la clientèle de Moneris au 1 866 319-7450 immédiatement.



Si un commerçant subit un bris de sécurité qui entraîne la compromission des données du titulaire de carte, le commerçant peut devoir faire face aux situations suivantes :

- le coût d'une enquête légale;
- le financement de l'évaluation de non-conformité;
- les coûts engagés par les émetteurs de cartes tels que la surveillance de cartes, la réémission d'une carte et les pertes en raison d'une fraude;
- les coûts de validation de la conformité à la norme de sécurité des données du SCP;
- la cessation des services de traitement des cartes.

Norme de sécurité des données des applications de paiement (AP)

La norme de sécurité des données des applications de paiement (AP) est une nouvelle norme du secteur des cartes de paiement (SCP).

Cette norme connue auparavant sous le nom de Pratiques exemplaires PABP de Visa est une norme de sécurité applicable aux applications de paiement qui sont élaborées par les fournisseurs de logiciels et vendue, distribuée ou mise sous licence aux commerçants. L'objectif de la norme de sécurité des données – AP consiste à aider les fournisseurs de logiciels à élaborer des applications de paiement sécurisées qui ne mettent pas en mémoire des données confidentielles et aident à supporter la conformité des commerçants à la norme de sécurité des données du SCP. Tous les commerçants qui utilisent des applications de paiement de tiers doivent s'assurer que l'application respecte les exigences de la norme de sécurité des données – AP. Pour en savoir davantage sur la conformité à cette norme et le calendrier des échéances, visitez moneris.com/pci.

En utilisant une application de paiements conforme à la norme de sécurité des données – AP, vous aidez à réduire le risque de la compromission des comptes, à prévenir le stockage des données confidentielles et à appuyer votre responsabilité de conformité à la norme du secteur des cartes de paiements.

Pour obtenir un complément d'information sur la norme de sécurité des données des applications de paiements, y compris une liste des applications validées, visitez :

www.pcisecuritystandards.org

www.visa.com/pabp



Commerce électronique

Sites Web des commerçants

Vous devez vous assurer que votre site Web informe sans équivoque et de façon évidente le titulaire de carte de l'identité de votre entreprise à tous les points d'interaction de sorte que celui-ci peut distinguer votre entreprise de celle d'un tiers, tel un fournisseur de produits ou de services au commerçant.

Votre site Web doit comporter toutes les informations suivantes :

- Affichage évident du nom du commerçant.
- Identification évidente du nom du commerçant tel qu'affiché sur le site Web du commerçant et doit correspondre au nom qui paraît sur le relevé du titulaire de carte.
- Afficher le nom du commerçant aussi clairement que toute autre information décrite sur le site Web, autre que les illustrations de produits ou de services offerts pour une vente.

- Les marques de cartes doivent être affichées en couleur pour signifier l'acceptation d'une carte de crédit et/ou de débit.
- Description complète des biens ou services offerts.
- Politique de remboursement et de retour.
- Personne-ressource du service à la clientèle, y compris l'adresse courriel ou le numéro de téléphone.
- Adresse de l'établissement permanent du commerçant.
- Devise de transaction (dollar US, dollar canadien).
- Restrictions à l'égard de l'exportation (s'il y a lieu).
- Politique de livraison.
- Affichage du pays du commerçant au moment d'offrir les options de paiement au titulaire de carte.
- Politique de protection de la vie privée.
- Fonctions de sécurité et politique de transmission des détails de carte de paiement.

Exigences en matière de sécurité et protection de votre réseau

Vous et vos fournisseurs de services doivent respecter les normes de chiffrement minimales pour la collecte et la transmission des données du titulaire de carte tel que SSL (secure sockets layer) ou la sécurité 3-D. L'autorisation est requise pour chaque transaction de commerce électronique. Vous ne pouvez refuser d'effectuer une transaction électronique seulement parce que le titulaire de carte n'a pas de certificat numérique ou autre protocole sécurisé.

Vérfié par Visa (VpV)

Vérfié par Visa est le service d'authentification mondial en ligne qui rend le magasinage en ligne plus sûr pour les commerçants Visa et les titulaires de cartes.



VpV procure à votre entreprise une protection accrue contre les transactions frauduleuses et les débits compensatoires pour les ventes en ligne, tout en donnant à vos clients une confiance accrue lors du magasinage en ligne, ce qui peut aider à transformer les magasiniers en acheteurs.

Pour obtenir un complément d'information sur le service VpV, visitez : <http://visa.ca>



Code sécurisé MasterCard

Le code sécurisé MasterCard est une solution de commerce électronique mondiale qui permet à vos clients de s'authentifier à leur émetteur de cartes via l'utilisation d'un seul mot de passe personnel et vous identifie comme acheteur authentique.

Un code sécurisé est un code confidentiel, connu uniquement par le titulaire de carte et son institution financière qui améliore le compte MasterCard existant du titulaire de carte en le protégeant contre toute utilisation non autorisée de sa carte lors du magasinage en ligne chez les marchands en ligne participants.

Pour obtenir un complément d'information sur le code sécurisé, visitez :

<http://www.mastercard.com>

Valeur de vérification de la carte 2 (Card Verification Value – CVV2)

Le code à trois chiffres est une exigence de sécurité de toutes les cartes Visa. On le retrouve au verso des cartes Visa, imprimé après l'espace prévu pour la signature (consultez la section sur comment identifier les caractéristiques de sécurité dans ce guide d'utilisation) ou dans une boîte blanche à côté de l'espace prévu pour la signature (tel qu'indiqué ci-dessous). Le code de trois chiffres est une importante caractéristique de sécurité des cartes Visa qui aide les commerçants à valider l'authenticité du titulaire de carte qui effectue l'achat.

Après avoir effectué une demande d'autorisation pour valider l'information de la carte (numéro de compte, date d'expiration de la carte et code de trois chiffres), le commerçant reçoit une réponse lui indiquant si le code de trois chiffres correspond ou non, lui permettant ainsi de prendre les mesures appropriées.

Qu'importe la réponse de vérification du code de trois chiffres, si l'émetteur n'approuve pas la demande d'autorisation, le commerçant ne doit pas terminer la transaction.

Le code de trois chiffres permet au commerçant d'exploiter ses affaires dans un environnement de commande par téléphone ou en ligne afin de vérifier si le client a en sa possession la véritable carte. Les émetteurs de cartes Visa fournissent une vérification en temps réel du code de trois chiffres pour aider les commerçants à s'assurer que la personne qui effectue l'achat a bien la carte en main.

Si le commerçant effectue une demande d'authentification du code de trois chiffres et que l'émetteur ne participe pas à la validation, le commerçant est protégé de toute responsabilité en cas de transaction frauduleuse possible. Si l'acheteur peut seulement fournir au commerçant le numéro de carte de crédit de 16 chiffres et la date d'expiration, cela signifie qu'il n'a probablement pas en sa possession la carte, ce qui signale la possibilité d'une transaction frauduleuse.

Pour en savoir davantage sur les outils anti-fraude électroniques ou pour parler à un représentant de Solutions Moneris, veuillez composer le 1 866 MONERIS.

Pour obtenir un complément d'information, visitez : <http://visa.ca>

Service de vérification d'adresse (SVA)

Le service SVA vérifie l'information de facturation du titulaire de carte en temps réel et fournit au commerçant un code de résultat distinct du code de réponse d'autorisation, permettant au commerçant de prendre une décision informée sur « l'évaluation du risque » pour déterminer s'il va continuer la transaction ou non.

Le service SVA aide à s'assurer que la personne qui effectue l'achat avec sa carte Visa est la même personne qui reçoit le relevé de compte Visa mensuel.

En faisant correspondre l'adresse de facturation en dossier auprès de l'émetteur de carte Visa par rapport à l'adresse de facturation fournie par le client, les commerçants et les émetteurs de cartes travaillent ensemble pour s'assurer que toute carte Visa perdue ou volée n'est pas utilisée dans un environnement sans présence de la carte pour acheter des biens ou des services.

Si l'adresse de facturation exacte n'est pas fournie à un commerçant lors d'une commande en ligne, postale ou téléphonique, la transaction ne sera pas complétée, ce qui peut empêcher un achat frauduleux.

Remarque :

- il est interdit de mettre en mémoire des données CVV2 une fois que l'autorisation a été obtenue pour la transaction. Veuillez consulter la section portant sur les normes de sécurité du secteur des cartes de paiement.

Exigences de reçu de commerce électronique

- Nom du commerçant
- Adresse en ligne du commerçant
- Montant de la transaction (ou du crédit), indiqué dans la devise de la transaction
- Date de la transaction (ou date de préparation du crédit)
- Numéro unique d'identification de transaction
- Nom de l'acheteur
- Code d'autorisation
- Type de transaction (achat ou crédit)
- Description des biens/services
- Politique de remboursement/retour (si des conditions s'appliquent)



Foire aux questions

- Q.** Je viens de faire une mise à niveau de mon système électronique PDV. Qu'advient-il de mon ancien équipement?
- R.** Veuillez retourner vos terminaux et accessoires PDV à Solutions Moneris. Communiquez avec le service à la clientèle de Solutions Moneris au 1 866 319-7450 et nous prendrons les mesures afin qu'un messenger vienne chercher les terminaux à votre établissement.
-
- Q.** J'ai reçu cette demande de facture/copie, que dois-je faire?
- R.** Lisez attentivement l'information sur la facture/copie, demande de facture, trouvez toute la documentation pertinente (reçus, factures, contrats, etc.) et télécopiez le tout à Solutions Moneris au numéro de télécopieur fourni.
-
- Q.** Je viens de télécopier le reçu d'une transaction, comment puis-je savoir si vous l'avez bien reçu?
- R.** Conservez votre confirmation de transmission qui est imprimée par votre télécopieur ou communiquez avec Solutions Moneris 48 heures après que vous avez transmis la télécopie afin de confirmer que nous l'avons bien reçue.
-
- Q.** Puis-je facturer mes clients des frais pour l'utilisation de leur carte MasterCard/Visa ou Interac (débit)?
- R.** Non. Vous ne pouvez pas facturer de frais pour l'utilisation d'une carte. Qu'importe le type de produit que vous vendez, il va à l'encontre de votre entente de commerçant de facturer des frais au client pour un achat avec sa carte de débit ou de crédit. De plus, vous ne pouvez imposer un minimum ni une valeur maximum de transactions pour l'achat lorsque la carte est remise aux fins de paiement.
-
- Q.** Nous déménageons. Je communique avec qui pour notifier notre changement d'adresse?
- R.** Si votre entreprise change de propriétaire, d'adresse, de numéros de téléphone ou télécopieur, veuillez communiquer avec le Centre de service à la clientèle.
-
- Q.** J'ai traité une transaction via mon terminal PDV et j'ai reçu un code d'autorisation. Pourquoi ai-je subi un débit compensatoire pour cette transaction?
- R.** Nonobstant le fait que vous recevez un code d'autorisation, vous pouvez quand même subir un débit compensatoire si le titulaire de carte met en cause la transaction et si les bonnes procédures d'acceptation de carte n'ont pas été suivies.

- Q.** J'ai communiqué avec le titulaire de carte qui a reconnu qu'une transaction que j'ai traitée sur sa carte de crédit entraînait un débit compensatoire. Comment puis-je régler ce débit compensatoire?
- R.** Demandez au titulaire de carte de communiquer avec la banque émettrice de la carte, origine du litige, et de demander de retirer le litige ou de répondre à l'avis de débit compensatoire par un avis écrit du titulaire de carte qui accepte les frais à son compte et télécopiez le document à Moneris.
-
- Q.** Puis-je demander des renseignements personnels à mes clients, tels que numéro de téléphone ou adresse, et puis-je indiquer cette information sur la facture par mesure de sécurité?
- R.** Ne jamais demander à votre client d'écrire son numéro de téléphone/adresse sur le reçu. Vous pouvez demander de l'information personnelle seulement si celle-ci est nécessaire pour achever la transaction, telle qu'une adresse de livraison. Si un commerçant perçoit un risque ou si Solutions Moneris indique à ce dernier de le faire, il peut demander des coordonnées supplémentaires au client. Une fois que l'identité est revue et que le commerçant est satisfait, il faut écrire « ID vérifiée » près de la signature du client. En aucun cas, le commerçant ne doit inscrire le numéro de permis de conduire, numéro de carte d'assurance maladie, etc., du client.
-
- Q.** Pourquoi une partie du numéro de la carte du titulaire de carte est-il caché sur le reçu du client?
- R.** Pour réduire le risque d'une utilisation frauduleuse, seulement une partie du numéro de carte du titulaire de carte s'imprime sur le reçu du titulaire de carte ainsi que sur certains rapports. Les autres chiffres du numéro sont masqués, par exemple, un « * » s'imprime pour chaque chiffre restant du numéro de carte. Les numéros de cartes de débit et de crédit (y compris les numéros de cartes de marques privées) sont masqués. Le masquage de carte est aussi connu sous « masquage de numéro de carte et transaction NCP (consultez la section sur la troncation NCP de ce guide).
-
- Q.** Que dois-je faire si un client me remet une lettre l'autorisant à utiliser la carte d'une autre personne?
- R.** Seulement la personne dont le nom et la signature paraissent sur la carte est autorisée à utiliser ladite carte.
-
- Q.** Pendant combien de temps devrai-je garder des copies de mes factures/remboursements?
- R.** Les reçus de factures et de remboursements doivent être conservés 18 mois pour les transactions de cartes de crédit et 12 mois pour les transactions de cartes de débit.

- Q.** Si un client paie par chèque et utilise son numéro de carte de crédit comme identification, puis-je traiter des frais à cette carte de crédit pour le montant du chèque s'il est retourné sans fonds?
- R.** Non, il s'agit d'une violation de votre entente de commerçant de traiter des frais à une carte de crédit pour tenter de récupérer une créance irrécouvrable. Nous vous recommandons de communiquer avec le client et de prendre des dispositions pour une autre méthode de paiement.
- Q.** Si un client m'indique qu'il n'a pas sa carte, mais aimerait effectuer un achat, puis-je procéder et compléter la vente en utilisant le numéro de carte et la date d'expiration?
- R.** Non, nous recommandons de ne pas compléter de transactions face à face, sauf si la carte de crédit est présente et que vous êtes en mesure de prendre une empreinte de la carte ou de glisser celle-ci et d'obtenir la signature du client.
- Q.** Un touriste des États-Unis désire effectuer un achat dans mon magasin. Dois-je lui indiquer le prix en dollars US et compléter la vente pour ce montant pour que ce soit plus facile pour mon client?
- R.** Non, en tant que commerçant exploitant un compte de commerçant en dollars canadiens, vous pouvez seulement traiter vos transactions dans cette devise. La banque qui émet la carte de crédit de votre client fera la conversion et votre client sera facturé le montant équivalent en dollars US.

Acronymes et sites Web utiles

AP – Application de paiement
CA – Canadien
CCC – Code de catégorie de commerçant
CDCE – Commerçant à débit compensatoire excessif
CPPT – Commande postale/commande téléphonique
FNS – Fonds non suffisants
GAB – Guichet automatique bancaire
IP – Protocole Internet
MCW – MasterCard Worldwide
NIP – Numéro d'identification personnel
NCP – Numéro de compte principal
PCI SSC – Organisme Payment Card Industry Security Standards Council
PDCE – Programme de débit compensatoire excessif
PDS – Programme de données sécurisées
PDV – Point de vente
PED – Dispositif de saisie du NIP (Pin Entry Device)
PRAM – Programme de rendement anti-fraude à l'intention des marchands
PMCDCC – Programme mondial de contrôle des débits compensatoires des commerçants
PMVC – Programme mondial de vérification des commerçants
RDCT – Ratio de débit compensatoire à transaction
SCP – Secteur des cartes de paiement
SIC – Sécurité de l'information du compte
SNR – Signature non requise
SPR – Service de paiement rapide
SSL – Secure Socket Layer
SVA – Service de vérification d'adresses
VpV – Vérifié par Visa
VVC – Valeur de vérification de carte (CVV)

■ Liens utiles

www.moneris.com

www.visa.ca

www.mastercard.com

www.pcisecuritystandards.org

Les commerçants du secteur de l'hébergement/hôtel, visitez :
www.moneris.com (recherche hôtels) <http://visa.ca/en/merchant/>

Les commerçants du secteur de location des véhicules, visitez :
<http://visa.ca/en/merchant/>



Comment communiquer avec nous

Notre centre de service à la clientèle destiné aux commerçants est offert 24/7/365 pour répondre à toute question à l'égard de votre compte de commerçant. Veuillez communiquer avec nous au **1 866 319-7450** ou visitez notre site à **www.moneris.com**.

Pour obtenir un code d'autorisation en utilisant notre système automatisé, communiquez avec nous au **1 866 802-2637**.

Si vous désirez communiquer avec notre service des ventes, composez le **1 866 319-7450**.

Pour commander des fournitures et du matériel promotionnel

Vous pouvez commander certaines fournitures pour votre entreprise directement de Moneris. Visitez notre magasin virtuel à **www.shopmoneris.com** ou communiquez avec nous au **1 866 319-7450**.

Comment obtenir la plus récente version du guide

Moneris pourra de temps à autre mettre à jour ce guide d'utilisation. Vous devez vous assurer d'obtenir et de toujours utiliser la plus récente version du guide d'utilisation. Pour obtenir une copie à jour, visitez **www.moneris.com** et choisissez Téléchargement à partir du menu des guides d'utilisation destinés au commerçant.

Veuillez prendre note que vous pouvez aussi consulter les règlements publics de Visa et MasterCard aux adresses suivantes : **<http://corporate.visa.com/pd/rules/main.jsp>** et **<http://www.mastercard.com/ca/merchant/fr/getstarted/rules.html>**.



^{MD}Moneris et le logo de Solutions Moneris sont des marques déposées de Corporation Solutions Moneris.^{MD}VISA est une marque déposée de Visa Canada Inc. Corporation Solutions Moneris est un utilisateur licencié. ^{MD}MasterCard est une marque déposée de MasterCard International Incorporated. ^{MD}American Express est utilisé par Amex Bank of Canada sous licence de American Express. ^{MD}Paiement direct Interac est une marque de commerce de Interac Inc. Banque Royale du Canada est un utilisateur autorisé de la marque de commerce.