PRÊT POUR LES PAIEMENTS[MC]

Guide d'utilisation à l'intention du commerçant

Moneris[MC]

PRÊT POUR LES PAIEMENTS

(05/16)

Moneris[MC]

PRÊT POUR LES PAIEMENTS

Pour obtenir de l'aide ou de plus amples renseignements :

Site Web : moneris.com

Sans frais : 1 866 319-7450

Inscrivez votre ID de commerçant Moneris[MD] ici :

_____

Table des matières

À propos de Moneris

Travailler avec Moneris vous permettra de rester à jour dans le monde en constante évolution du paiement. En tant que l'un des plus importants acquéreurs de transactions de paiement en Amérique du Nord, nous sommes à l'avant-garde domaine du paiement. Nous adoptons le changement pour que votre entreprise soit prête pour demain, dès aujourd'hui.

Des terminaux en magasin aux plateformes de point de vente mobiles et de commerce électronique, l'innovation est à l'avant-garde de nos solutions de paiement. De plus, nos solutions sont soutenues par une technologie fiable et sécuritaire afin d'assurer une expérience positive pour tous vos clients.

Notre mission est de rester à l'affût du changement. La vôtre est de satisfaire vos clients. Vous avez déjà choisi d'être préparé pour ce que l'avenir vous réserve.

› Bienvenue dans une nouvelle ère où vous serez **PRÊT POUR LES PAIEMENTS**.

Voici ce que vous offre Moneris :

FIABLE – La **fiabilité à 99,9 % du système*** de Moneris vous permet d'offrir une excellente expérience client.

EN LIGNE – Nos **solutions de commerce électronique** complètes et éprouvées aident à assurer une expérience fluide d'achat en ligne pour vos clients, en tout temps.

PRATIQUE – Nos **solutions d'entreprises intégrées** vous permettent de tout faire en même temps : brancher un terminal de point de vente, faire vos rapports, gérer la relation que vous avez avec vos clients et effectuer des ventes en ligne.

MOBILE – Nos **solutions de paiement mobiles** vous permettent d'atteindre votre plein potentiel, des terminaux sans fil aux applications de traitement des transactions qui transforment n'importe quel téléphone intelligent en un appareil de point de vente.

SÉCURITAIRE – Les transactions sont protégées par les **normes de sécurité les plus strictes du domaine**, ce qui permet de prévenir la fraude.

TECHNOLOGIQUE – Les transactions ne sont qu'une partie du portrait : nous sommes constamment à la recherche d'**outils novateurs pour les entreprises** qui vous permettront d'atteindre votre plein potentiel, aujourd'hui et demain.

*Le service de Moneris est disponible seulement si la plateforme de traitement du système serveur de Moneris est opérationnelle. La disponibilité du service est évaluée par Moneris chaque trimestre et est assujettie à certaines exclusions telles que déterminées par Moneris.

Traitement des transactions

Voici ce que vous devez savoir pour traiter les transactions des clients.

Exigences générales pour le traitement des transactions

Identification et responsabilités du commerçant

À tout moment, vous devez vous assurer de faire savoir au titulaire de carte que vous êtes le commerçant, et ce, de façon évidente et sans équivoque, afin que le titulaire de carte puisse facilement vous distinguer, vous, le commerçant, des tierces parties, comme les fournisseurs de produits ou de services.

Vous devez faire en sorte que le titulaire de carte comprenne que vous êtes responsable de la transaction, y compris de la livraison des produits (qu'ils soient physiques ou numériques) ou de la prestation des services sujets à la transaction, ainsi que du service à la clientèle et de la résolution des réclamations, conformément aux modalités applicables à la transaction.

Transactions valides

Vous devez seulement traiter des transactions entre vous et le véritable titulaire de carte. Vous ne devez pas traiter de transactions que vous savez ou devriez savoir frauduleuses, ou non autorisées par le titulaire de carte, et vous ne devez pas participer à une transaction frauduleuse autorisée par le titulaire de carte. Vous êtes tenu responsable des actions de vos employés, de vos agents, de vos représentants et de toute autre personne traitant des transactions.

Discrimination

Vous n'adopterez aucune pratique d'acceptation qui fait preuve de discrimination à l'égard d'une carte en faveur d'une autre, ni n'en dissuaderez l'utilisation.

Procédures adéquates de traitement des transactions

TRANSACTION PAR CARTE À PUCE

Une carte à puce est une carte de débit ou de crédit dotée d'un circuit intégré que le titulaire doit insérer dans le lecteur de cartes d'un terminal de point de vente (PDV). Il est difficile de copier ou d'altérer une carte à puce puisque les cartes de ce type traitent les données de façon sécuritaire.

La technologie des cartes à puce aide à :

- réduire les débits compensatoires;
- réduire la fraude;
- simplifier les opérations des magasins.

Son fonctionnement

Une transaction effectuée à l'aide d'une carte à puce et d'un terminal de PDV prenant en charge les cartes à puce est simple : plutôt que de glisser la carte et de

Ce qu'il faut savoir au sujet des transactions par cartes à puce

- Lorsqu'on vous présente une carte à puce, ne la glissez pas en premier. Insérez-la simplement dans le lecteur de cartes à puce, puis suivez les invites.
- Une carte à puce doit demeurer dans le terminal de PDV pour la durée de la transaction. Ne retirez pas la carte tant que le terminal ne vous invite pas à le faire. Si vous retirez la carte avant que la transaction ne soit terminée, la transaction sera annulée.

signer un reçu, le titulaire de carte insère sa carte dans le terminal de PDV et saisit manuellement son numéro d'identification personnel (NIP) à l'aide du clavier.

Laissez la carte dans le lecteur de cartes pour la durée de la transaction.

1. Commencez la transaction d'achat.
2. Vérifiez si la carte est dotée d'une puce.
3. Insérez la carte dans le lecteur lorsque vous êtes invité à le faire. La carte doit être insérée avec la puce vers le haut.
4. Suivez les invites.
5. Attendez que le message « Retirez la carte » s'affiche, puis retirez la carte.

La transaction est maintenant terminée.

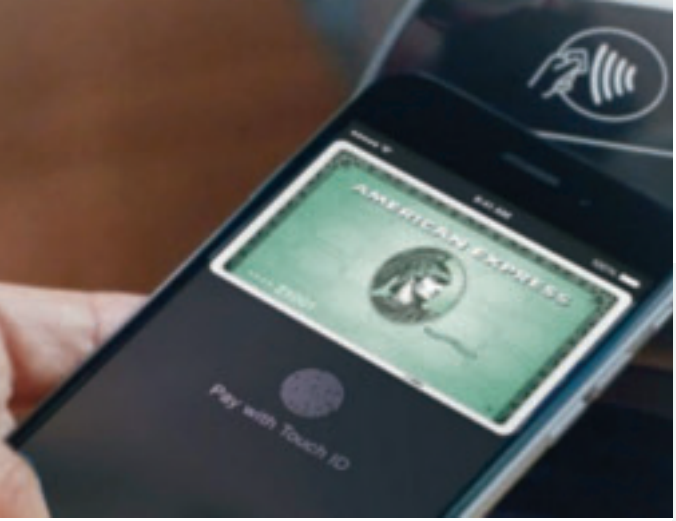
Remarque : *Certains clients possèdent une carte à puce et à signature ne nécessitant pas de NIP. Votre terminal reconnaîtra la carte et vous invitera à suivre le processus de traitement de la transaction approprié.*

Remarque : *La mention « VÉRIFIÉE PAR NIP » n'apparaît pas sur les reçus des transactions effectuées avec une carte UnionPay; la signature du titulaire de carte est requise pour toutes les transactions, y compris celles vérifiées par NIP. Vous pourriez ne pas être protégé contre les débits compensatoires si vous n'obtenez pas la signature du titulaire de carte.*

Ce qu'il faut savoir au sujet des transactions par cartes à puce ...suite

- Nous vous recommandons de ne pas effectuer manuellement une transaction par carte à puce sur votre terminal. Les transactions saisies manuellement pourraient ne pas être protégées contre les débits compensatoires, même si vous obtenez une empreinte, une autorisation et une signature.

  Remarque : *Les saisies manuelles ne sont pas autorisées pour les transactions effectuées par UnionPay, sauf dans un établissement hôtelier ou un service de location de voitures pour traiter une transaction de préautorisation pour la réservation d'une chambre d'hôtel ou d'une voiture de location.*
- Comme pratique exemplaire, nous vous recommandons d'encercler la mention « VÉRIFIÉE PAR NIP » apparaissant au bas du reçu.



TRANSACTION SANS CONTACT

Les transactions sans contact sont conçues pour accélérer le traitement des transactions et pour simplifier le processus de paiement pour vous et pour vos clients.

Son fonctionnement

Au lieu de glisser ou d'insérer la carte, le client présente sa carte au terminal prenant en charge les transactions sans contact.

Comme la technologie sans contact est en constante évolution, plus d'appareils de paiement connaissent une popularité grandissante (les téléphones mobiles, les téléphones intelligents ou les porte-clés, par exemple). Ces appareils fonctionnent de la même façon que les cartes, c'est-à-dire que le titulaire de carte présente l'appareil de paiement sans contact au terminal.

Ce qu'il faut savoir au sujet des transactions sans contact

- Pour accepter les transactions sans contact, vous devez posséder un terminal ou un système logiciel prenant en charge ce type de transaction, ou un lecteur sans contact certifié.
- Aucun NIP ou signature n'est requis pour les transactions d'une valeur inférieure au montant spécifié (consultez la section *Programmes sans contact* à la page 36).
- Vous n'êtes pas tenu de remettre un reçu de transaction au titulaire de carte, à moins que ce dernier n'en fasse la demande ou que la valeur de la transaction soit supérieure à la limite établie.
- Vous devez tout de même conserver une copie du reçu dans vos dossiers au cas où une réclamation serait effectuée.

TRANSACTION PAR GLISSEMENT DE LA CARTE

Voici ce que vous devez faire lorsqu'un client présente une carte à bande magnétique.

Ce qu'il faut faire

- Avant de glisser la carte, assurez-vous que la bande magnétique fait face au lecteur.
- Glissez toujours la carte une seule fois dans la direction indiquée par la flèche sur le lecteur.
- Ne glissez jamais une carte dans le sens inverse ou avec un certain angle, car cela peut fausser la lecture de la bande magnétique.
- Si le message « Appeler » ou « Appeler Centre » s'affiche sur votre terminal de PDV, appelez le centre d'autorisation de Moneris au **1 866 802-2637**.
- Si vous suspectez une activité frauduleuse ou si vous avez des questions relatives à l'autorisation des transactions, demandez une autorisation de code 10 (consultez la section *Procédure code 10* à la page 17).
- Si le Centre d'autorisation exige que vous reteniez une carte, ne le faites que par des moyens pacifiques et raisonnables. Ne vous mettez jamais en danger.

TRANSACTION SAISIE MANUELLEMENT

Il est parfois possible que la carte à puce ou la carte à bande magnétique du client ne fonctionne pas. La puce ou la bande magnétique d'une carte ne peut généralement pas être lue dans les cas suivants :

- le lecteur de cartes à puce ou le lecteur de bandes magnétiques est brisé ou sale;
- le lecteur est obstrué, ce qui empêche la carte d'être insérée ou glissée correctement;
- la carte n'a pas été insérée ou glissée correctement;
- la puce ou la bande magnétique de la carte est endommagée.

Si vous traitez vos transactions à l'aide d'un terminal de PDV, votre seuil de transaction est de zéro; vous devez donc obtenir un numéro d'autorisation pour chaque transaction saisie manuellement.

Remarque : *UnionPay n'autorise pas les transactions saisies manuellement, à moins qu'il ne s'agisse d'une transaction de préautorisation pour la réservation d'une chambre d'hôtel ou d'un véhicule de location.*

Ce qu'il faut faire

Remarque : *Il est important de se souvenir qu'une autorisation ne signifie pas que le vrai titulaire de carte effectue l'achat ou qu'une carte authentique est utilisée. Une autorisation signifie seulement que les fonds sont disponibles et que la carte n'est pas bloquée. Pour aider à détecter et à prévenir la fraude, une combinaison d'outils et de contrôles devrait être ajoutée au processus d'autorisation.*

- La puce et la bande magnétique sont des composants de sécurité importants d'une carte. De ce fait, la saisie manuelle est appropriée seulement dans les cas où la puce ou la bande magnétique d'une carte ne peuvent être lues.
- Lorsqu'une carte à puce ou une carte à bande magnétique ne peut être lue, une facture manuelle doit être créée et elle doit comporter les éléments suivants :
  - la date;
  - une empreinte de la carte;
  - les détails de la transaction;
  - la valeur totale de la transaction, y compris les taxes et les autres frais;
  - la signature du titulaire de carte;
  - le numéro d'autorisation;

Remarque importante au sujet des transactions saisies mensuellement

Nous vous recommandons de ne pas saisir de transactions manuellement sur votre appareil. Les transactions saisies manuellement peuvent ne pas être protégées contre les débits compensatoires, et ce, même si vous obtenez une empreinte de la carte, une autorisation et une signature.

Remarque : *UnionPay n'autorise pas les transactions saisies manuellement, à moins qu'il ne s'agisse d'une transaction de préautorisation pour la réservation d'une chambre d'hôtel ou d'un véhicule de location.*

Il n'est pas recommandé de saisir des transactions manuellement pour les raisons suivantes :

- Cette méthode augmente les risques de fraude et/ou de contrefaçon.
- Cette méthode peut augmenter vos frais, car

- le nom et le numéro du commerçant;
- n'inscrivez pas la mention « annulée » ou « copie » sur le dessus de la facture manuelle.

- Sur le terminal de PDV, vous devez :
  - saisir manuellement le numéro de la carte;
  - saisir le montant exact et une date d'expiration valide;
  - vérifier que l'autorisation est acceptée.
- Sur le reçu du terminal de PDV, vous devez :
  - imprimer la mention « TIRAGE D'ESSAI » sur la ligne de signature;
  - noter le numéro de référence préimprimé apparaissant sur la facture manuelle.

Étapes pour minimiser la saisie manuelle

- Vérifiez régulièrement le lecteur de cartes à puce et le lecteur de bandes magnétiques du terminal de PDV pour vous assurer qu'ils fonctionnent correctement.
- Nettoyez périodiquement vos lecteurs à l'aide de la carte de nettoyage de lecteur fournie avec votre terminal de PDV. Pour commander des cartes de nettoyage ou d'autres fournitures pour votre entreprise auprès de Moneris, visitez notre site Web **magasin.moneris.com** ou appelez le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**.
- Placez les lecteurs de façon à faciliter l'insertion ou le glissement de la carte, en plus de veiller à ce que tout obstacle soit retiré.
- Empêchez votre personnel de déposer près des terminaux des articles pouvant salir ou endommager l'équipement de PDV, particulièrement de la nourriture et des boissons.

Remarque importante au sujet des transactions saisies manuellement ...suite

votre taux d'escompte de commerçant est calculé en fonction de votre capacité à lire et à transmettre les données des bandes magnétiques à partir de votre terminal de PDV.

- Cette méthode est moins efficace, car les transactions prennent plus de temps à compléter et sont propices aux erreurs.
- Cette méthode peut vous faire perdre des ventes, car le taux d'autorisations refusées est plus élevé pour les transactions saisies manuellement.

Si une transaction est saisie manuellement, vous devez obtenir une empreinte de la carte sur une facture. Si, par la suite, la transaction est contestée, l'empreinte prouve que la carte était présente et peut vous protéger contre certains débits compensatoires.

Ces transactions doivent être autorisées, et le numéro d'autorisation doit apparaître sur la facture.

- Ne placez pas les lecteurs près de tout équipement désactivant les dispositifs antivol magnétiques fixés à la marchandise.

Aider à réduire la fraude pour les transactions effectuées sans puce

Souvenez-vous, si une carte à puce ne peut être lue, vous pouvez réduire les risques de fraude en suivant les procédures adéquates suivantes :

- Recherchez l'hologramme, le numéro d'identification de la banque imprimé sur la carte, le symbole incrusté unique et la boîte de signature.
- Vérifiez la date d'expiration de la carte.
- Si vous êtes convaincu de la validité de la carte, suivez la procédure d'autorisation adéquate.
- Demandez au titulaire de carte de signer la facture bien en vue.
- Comparez la signature sur la carte et la signature sur la facture pour vous assurer qu'elles correspondent.

Remarque importante au sujet des transactions saisies manuellement ...suite

Si les transactions saisies manuellement représentent plus d'un pour cent des transactions totales traitées par caissier ou par terminal, essayez d'en déterminer la raison.

Procédures lors des temps d'arrêt

Si le système tombe en panne, suivez les procédures suivantes pour traiter des transactions par cartes de crédit :

Remarque : *Ces procédures ne s'appliquent pas aux transactions UnionPay, car il est impossible d'accepter des cartes UnionPay lorsque le système est en panne.*

- Prenez une empreinte de la carte.
- Appelez le centre d'autorisation de Moneris au **1 866 802-2637** pour obtenir une autorisation vocale, puis notez le numéro d'autorisation sur la facture manuelle.
- Demandez au titulaire de carte de signer la copie avec l'empreinte de carte.
- Une fois le système/service de nouveau en fonction, saisissez la transaction sur votre terminal de PDV en ligne à l'aide du numéro d'autorisation reçu.

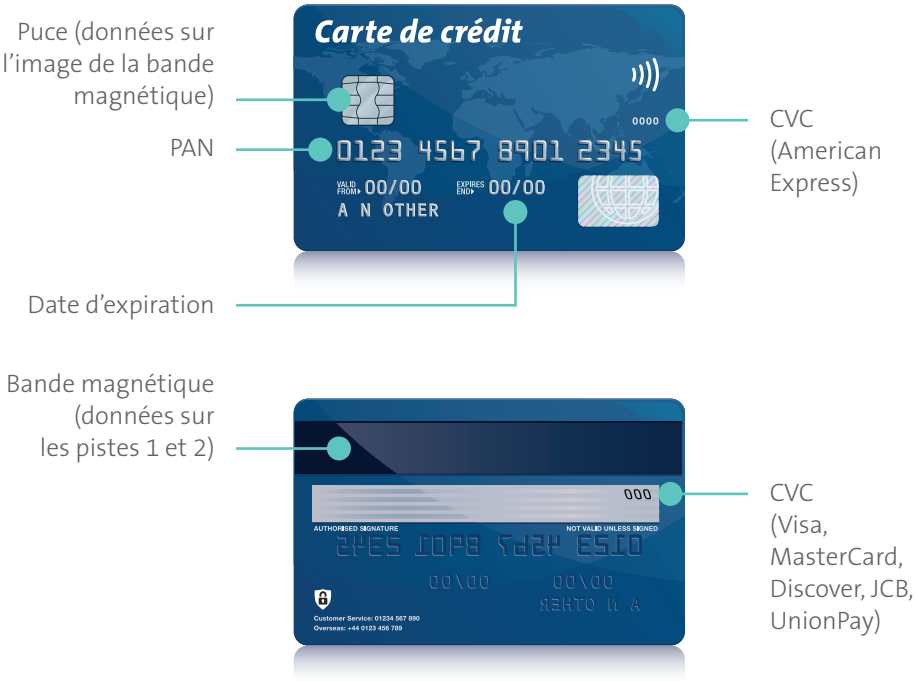
Assurez-vous que tous les renseignements sont clairement inscrits sur votre facture manuelle. (Consultez la section *Transaction saisie manuellement* à la page 10.)

Protéger votre entreprise contre la fraude

La fraude peut s'avérer un danger pour votre entreprise; découvrez les pratiques exemplaires que vous pouvez utiliser pour vous aider à vous en protéger.

Reconnaître les caractéristiques de sécurité

Les types de données d'une carte de paiement



Comportement suspect du client

La détection de la fraude par carte de crédit peut être classée en deux catégories. Les cartes de crédit légitimes perdues ou volées où l'utilisateur n'est pas le titulaire de carte autorisé forment la première catégorie. La deuxième catégorie est formée des cartes de crédit contrefaites, lorsqu'une carte est créée illégalement afin de ressembler à une carte légitime et de fonctionner de la même façon que ces dernières. Notre expérience nous a démontré que les fraudeurs de cartes de crédit peuvent présenter une ou plusieurs des caractéristiques suivantes :

Cartes de crédit perdues ou volées

- **Achats sans discernement**
  - Le client a pris des articles au hasard et semble nerveux ou pressé.
  - Le client peut effectuer un achat au moment de la fermeture du magasin.
  - Dans un magasin de vêtements, le client peut avoir choisi des articles sans se soucier de la taille, de la couleur, du style ou du prix, et possiblement sans les avoir essayés.
  - Lorsque le client achète des articles électroniques onéreux, il est possible qu'il ne pose aucune question au sujet des spécifications techniques ou des garanties.
  - Le client peut demander une livraison immédiate des gros articles et ne pas demander d'aide.
- **La carte**
  - Le titulaire de carte peut retirer la carte de ses poches au lieu de la retirer d'un portefeuille ou d'un sac à main.
  - Le titulaire de carte peut signer la facture d'une façon réfléchie et/ou qui ne semble pas naturelle.
  - La signature sur la carte et celle sur la facture ne correspondent peut-être pas.
  - Le nom sur la carte est féminin, mais la personne l'utilisant est un homme, ou vice versa.
  - Le titulaire de carte peut porter des articles coûteux au solde d'une carte nouvellement émise.

Cartes contrefaites

- **Assurance**
  - Le titulaire de carte peut ressembler à une personne qui achète des articles onéreux. Il peut être bien vêtu et confiant.
  - Le titulaire de carte est certain que son achat sera approuvé, car il participe à la production de ces cartes de haute qualité.
  - Le titulaire de carte peut passer beaucoup de temps à regarder, puis venir chercher l'article la journée suivante.
- **Retour au magasin pour d'autres achats**
  - Le titulaire de carte peut revenir au magasin avec des amis, qui auront aussi des cartes contrefaites, en affirmant que les articles et les prix sont intéressants.

Remarque : *Toutes ces caractéristiques peuvent être présentes lors d'une transaction légitime, au même titre que leur absence ne signifie pas que la transaction est légitime. Le bon sens est le meilleur guide. Si vous ou votre personnel avez des doutes, donnez-vous, et non au titulaire de carte, le bénéfice du doute. Appelez le centre d'autorisation pour obtenir une autorisation de code 10 (consultez la* Procédure code 10 *ci-dessous) lorsque vous pensez que la carte utilisée pour la transaction est frauduleuse ou suspecte.*

Marche à suivre en cas de cartes perdues, volées ou oubliées

Procédure code 10

Le code 10 est un code universel qui permet aux commerçants d'avertir un centre d'autorisation qu'il suspecte une transaction frauduleuse sans alerter l'individu présentant la carte pour le paiement.

Même lorsque les procédures adéquates sont suivies (p. ex., une carte est glissée, et une signature correspondant à celle sur la carte est obtenue sur la facture), il n'y a aucune garantie que la transaction est légitime. Si vous suspectez une fraude, demandez une autorisation de code 10.

Les transactions sont légitimes dans la plupart des cas, mais vous devez savoir quoi faire si vous devez demander une autorisation de code 10 :

- Appelez le Centre d'autorisation de Moneris au **1 866 802-2637** et suivez les instructions pour un code 10.
- Identifiez l'appel comme étant un code 10.
- Conservez la carte entre vos mains lors du processus d'autorisation. Restez calme ainsi que désinvolte et courtois avec le titulaire de carte.
- Votre appel peut être transféré. Ne raccrochez pas.
- On vous posera une série de questions à répondre par oui ou non pour vérifier l'authenticité de la carte.
- Suivez les instructions qu'on vous donnera au téléphone.
- N'essayez pas d'appréhender ou de retenir le titulaire de carte.
- Une récompense peut être accordée pour le retour d'une carte perdue, volée ou contrefaite.

  Remarque : *Les récompenses sont à la discrétion de l'émetteur de cartes.*

Si vous suspectez une transaction ou un titulaire de carte, appelez le Centre d'autorisation de Moneris. Les procédures code 10 ont été créées pour votre protection.

Retour des cartes oubliées

Si une carte est oubliée dans votre magasin :

- Remettez la carte au titulaire de carte s'il la réclame dans un délai de 24 heures et qu'il présente une pièce d'identité 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 suivante :
  Solutions Moneris
  À l'attention de : Récompenses destinées au commerçant
  C.P. 219 Stn D
  Toronto, ON M6P 3J8

Assurez-vous d'inclure les renseignements ci-dessous lors du retour de la carte :

- nom du magasin;
- adresse;
- nom de la personne qui a conservé la carte;
- numéro de téléphone.

Écrémage présumé

L'écrémage des données est le transfert des données électroniques de la bande magnétique d'une carte à une autre, dans un but frauduleux, au moyen d'un lecteur de cartes. Les stations-service et les restaurants sont souvent la cible des fraudeurs puisque les employés travaillent seuls pendant de longues périodes.

Son fonctionnement

Des technologies de plus en plus sophistiquées permettent de transférer les données contenues dans la bande magnétique des cartes de débit et de crédit à l'aide d'un terminal de PDV factice ou trafiqué.

Il existe aussi des appareils d'écrémage portatifs qui transfèrent les données de la bande magnétique d'une carte. Ces appareils sont souvent cachés sous les comptoirs et ils peuvent fonctionner pendant de longues périodes, car ils ont une capacité de stockage importante.

Outre les données contenues dans la bande magnétique d'une carte, les fraudeurs doivent aussi obtenir le NIP du titulaire de carte. Ils peuvent généralement procéder de deux façons :

- **En épiant le NIP** saisi par-dessus l'épaule du titulaire de carte. Un employé ou un complice passe « par hasard » derrière le titulaire de carte au moment où celui-ci saisit son NIP dans le clavier NIP.
- **En utilisant une minicaméra pour capter le NIP**. La caméra est placée dans un trou au plafond ou sur une tablette au-dessus du comptoir et du clavier NIP. Pour que ce type d'équipement soit utile, le clavier NIP doit être fixé dans une position précise sur le comptoir afin que la lentille de la caméra puisse capter les chiffres saisis par le titulaire de carte.

Aider les titulaires de carte à protéger leur NIP

- Les titulaires de cartes doivent pouvoir saisir leur numéro d'identification personnel (NIP) sans qu'il ne soit vu par quelqu'un d'autre.
- Assurez-vous que le terminal de PDV est installé de façon à ce que le titulaire de carte puisse facilement cacher son NIP avec son corps, ou installez des écrans d'intimité sur votre appareil de PDV si le clavier NIP est fixe ou fixé à un socle.
- Autorisez le titulaire de carte à tenir le clavier NIP jusqu'à ce que la transaction soit autorisée ou refusée.
- Remettez toujours au titulaire de carte une copie du reçu de transaction ainsi que sa carte.

Commande postale/téléphonique et fraude de commerce électronique

Beaucoup de mesures de sécurité servant à protéger les commerces de détail traditionnels contre la fraude ne sont pas applicables aux environnements où la carte n'est pas présente au moment de la transaction, y compris les commandes postales, téléphoniques et en ligne. Ces transactions ne requièrent pas un contact en personne ou la présence d'une carte, alors un certain anonymat est lié à la transaction.

Tous les commerçants traitant des commandes postales, téléphoniques et en ligne doivent obtenir une autorisation pour ce type de transactions.

Si les fonds sont disponibles et que la carte n'a pas été déclarée perdue ou volée, la transaction sera probablement autorisée par l'émetteur de la carte.

Remarque : *Il est important de se souvenir qu'une autorisation ne signifie pas que le vrai titulaire de carte effectue l'achat ou qu'une carte authentique est utilisée. Une autorisation signifie seulement que les fonds sont disponibles et que la carte n'est pas bloquée.*

Pratiques exemplaires pour prévenir la fraude électronique

- Autorisez toutes les transactions, peu importe leur montant.
- Mettez en place les outils de prévention de la fraude applicables (consultez la section *Exigences en matière de sécurité pour protéger votre réseau* à la page 53).
- Facturez seulement les articles ayant été expédiés.
- Créditez le compte du titulaire de carte immédiatement s'il a retourné la marchandise ou s'il conteste le montant facturé.
- Autant que possible, expédiez la marchandise par un service de messagerie demandant une signature comme preuve de livraison.
- Conservez un registre détaillé de tous les bons de commande, bordereaux de marchandise, reçus de livraison et renseignements comme les adresses, numéros de téléphone, signatures, factures pertinentes et adresses courriel.
- Développez et maintenez une base de données ou des fichiers sur l'historique de compte des titulaires de carte pour suivre les habitudes d'achat et comparer les ventes individuelles pour détecter des signes de fraude.
- Faites le suivi des comptes de carte de crédit à « problèmes » (c.-à-d. les comptes pour lesquels des débits compensatoires ont été effectués) et vérifiez que les commandes futures n'utilisent pas ces comptes.
- Faites le suivi des adresses IP.
- Contrôlez de façon adéquate les employés ayant accès à la base de données des titulaires de carte et aux numéros de compte.
- Respectez les normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS) pour garantir la sécurité de vos systèmes. (Consultez la section *Normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS)* à la page 46.)

SI VOUS SUSPECTEZ UNE FRAUDE

Si une transaction vous semble suspecte ou si les circonstances d'une transaction sont douteuses :

- Demandez au titulaire de carte de fournir des renseignements supplémentaires comme :
  - les numéros de téléphone pour le joindre en journée et en soirée, lesquels peuvent être vérifiés à l'aide de l'assistance-annuaire ou du **canada411.ca**;
  - le nom de la banque présent sur le dessus de sa carte.
- Vous pouvez lui demander un nom et une adresse de vérification. (Consultez la section *Service de vérification de l'adresse (SVA)* à la page 56.)

Remarque : *Si le doute persiste, ne traitez pas la transaction.*

› Pour obtenir de plus amples renseignements au sujet de la protection de votre entreprise contre la fraude, visitez la page **moneris.com/fraude**.

Débits compensatoires

Un débit compensatoire se produit lorsque le crédit ou le paiement d'une transaction ayant été autorisée est annulé.

Il peut résulter d'une contestation du titulaire de carte ou d'un non-respect des procédures adéquates d'acceptation ou d'autorisation. Ces rectifications sont faites directement dans votre compte, et un avis de rectification ainsi qu'un rapport sommaire du débit compensatoire vous sont envoyés par télécopieur, par la poste ou en ligne par l'entremise du centre de messagerie sécuritaire de Marchand Direct[MD].

Dans certains cas, les débits compensatoires peuvent être annulés si vous fournissez la documentation nécessaire dans les délais établis dans votre convention d'affiliation. Si vous recevez un avis de rectification de débit compensatoire, nous vous recommandons d'y répondre immédiatement.

L'avis de rectification est accompagné d'instructions précises sur ce qu'il vous faut fournir afin de contester le débit compensatoire. Si vous avez besoin d'assistance ou souhaitez obtenir plus de renseignements au sujet d'un débit compensatoire, appelez le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**.

CODES DE RAISON DE DÉBIT COMPENSATOIRE

Consultez la page **moneris.com/fr-ca/chargeback** pour obtenir une liste des codes de raison de débit compensatoire pour lesquels votre compte pourrait être ajusté.

Demandes de récupération

Il peut arriver que l'émetteur de cartes vous demande de fournir une copie de la facture ou du relevé de transaction d'une vente conclue dans votre établissement. Ces requêtes émanent généralement des titulaires de carte souhaitant vérifier des frais ou voulant obtenir des précisions au sujet des montants prélevés dans leur compte de carte de débit ou de crédit. Elles peuvent également provenir d'autres institutions financières émettrices de cartes voulant régler une fraude ou un litige.

En tant que commerçant acceptant les paiements par carte, vous devez conserver une copie de tous les reçus de vente et de transaction, et toutes les factures pour une certaine période à compter de la date de la transaction, en plus de devoir répondre à la demande dans le délai indiqué dans votre convention d'affiliation. Cette période varie en fonction de chaque marque de cartes : 13 mois pour Visa[MD], MasterCard[MD] et UnionPay, 18 mois pour Discover[MD] et 24 mois pour American Express[MD].

Répondre aux demandes de récupération

Si vous recevez une demande de récupération de la part de Moneris, vous devez y répondre dans les délais établis dans votre convention d'affiliation en envoyant une copie lisible du document utilisé pour facturer la transaction au compte du titulaire de carte. Les factures manuelles, les reçus de transaction du terminal de PDV, les factures, les références, les ententes de location de véhicule, les bons de

Envoyez les documents à Moneris par télécopieur ou par la poste :

1. **Par télécopieur :**
   - **Pour les demandes de récupération :**
     416 231-9329 (local) ou
     1 866 596-1116 (sans frais)
   - **Pour les demandes de débit compensatoire :**
     416 734-1561 (local) ou
     1 866 354-3797 (sans frais)

   Conservez votre confirmation de télécopie comme preuve que vous avez rempli la demande de récupération ou de débit compensatoire.

2. **Par la poste :**
   Solutions Moneris
   C.P. 410 Station A
   Toronto, Ontario M5W 1C2

Les délais sont primordiaux! Le défaut d'envoyer une copie des renseignements demandés dans les délais impartis établis dans votre convention d'affiliation pourrait entraîner un débit compensatoire irréversible. Pour être certain de recevoir les demandes de récupération et les avis de débit compensatoire, assurez-vous que l'adresse postale ainsi que les numéros de téléphone et de télécopieur de votre emplacement sont à jour.

Assurez-vous d'envoyer tous les documents requis à Moneris en réponse aux codes de raison de débit compensatoire applicables.

Le document doit inclure les renseignements suivants (et tout autre document demandé) :

- numéro de carte tronqué;
- numéro d'autorisation;
- nom du titulaire de carte;
- signature du titulaire de carte (au besoin);
- nom du commerçant;
- emplacement du commerçant;
- date de la transaction;
- montant de la transaction.

Veuillez aussi inclure la demande de récupération originale avec le document.

Remarque : *Si vous recevez une demande de récupération pour un article que vous avez déjà remboursé, veuillez joindre tous les documents relatifs à ce remboursement à la documentation devant être envoyée à Moneris.*

Conseils utiles au sujet des demandes de débit compensatoire et de récupération

- Pour éviter que le titulaire de carte soit perplexe au sujet de la transaction, assurez-vous que vos dépôts sont effectués tous les jours.
- Pour éviter toute confusion quant à la description du commerce sur le relevé du titulaire de carte, assurez-vous que le nom de l'entreprise imprimé sur les factures correspond au nom affiché sur votre magasin. Pour les transactions en ligne, assurez-vous que le nom de l'entreprise apparaissant sur le reçu correspond aux renseignements présents sur votre site Web.
- Si vous découvrez qu'une transaction a été dupliquée, créditez immédiatement le compte du titulaire de carte.
- Si on vous demande de fournir une facture pour une carte n'ayant pu être insérée ou glissée dans votre terminal de PDV, assurez-vous de fournir la facture manuelle pour confirmer qu'une empreinte de la carte a été prise et que la carte était présente dans votre établissement au moment de la vente.
- Pour éviter un éventuel débit compensatoire irréversible dans votre compte, assurez-vous de respecter à la lettre les délais impartis pour les demandes de récupération et d'envoyer vos réponses le plus rapidement possible.
- Répondez à toutes les demandes de récupération, même si elles semblent dupliquées.
- Répondez toujours aux demandes de récupération et de débit compensatoire en envoyant des copies lisibles des documents d'information.

MARCHAND DIRECT

La documentation peut être consultée en ligne par l'entremise du centre de messagerie sécuritaire de Marchand Direct. Si vous n'êtes présentement pas inscrit à Marchand Direct, visitez la page **moneris.com/marchanddirect** ou appelez le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**.

Pour obtenir de l'aide au sujet des demandes de récupération ou de débit compensatoire, ou si vous désirez les recevoir par télécopieur ou par Marchand Direct, appelez le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**.

Normes importantes

- Assurez-vous que toutes les transactions avec carte présente sont autorisées au moyen de votre terminal de PDV; si la carte est insérée ou glissée, un NIP doit être saisi ou une signature doit être obtenue comme méthode de vérification.
- Pour les ventes avec carte présente, si la carte ne peut être insérée ou glissée dans le PDV, une empreinte manuelle doit être prise à l'aide d'une imprimante à carte. Assurez-vous que la transaction est autorisée et que le reçu est signé.

  Remarque : *UnionPay n'autorise pas les transactions saisies manuellement, à moins qu'il ne s'agisse d'une transaction de préautorisation pour la réservation d'une chambre d'hôtel ou d'un véhicule de location.*
- Obtenez l'autorisation requise (avec le montant total de la transaction ainsi qu'une date d'expiration valide) pour toutes les transactions, et ce, le jour de la transaction.
- Ne traitez pas de transaction dont l'autorisation a été refusée. Demandez au client de payer d'une autre façon.
- Assurez-vous que toutes les cartes acceptées comprennent le logo et les caractéristiques de sécurité.
- Pour les cartes de crédit Visa, Discover et American Express, une différence de 20 % par rapport au montant autorisé est permise dans les restaurants pour l'ajout du pourboire. Par conséquent, le montant actuel (ou final) ne doit pas dépasser le montant autorisé de plus de 20 %.

- Pour les cartes de crédit UnionPay, une différence de 15 % par rapport au montant autorisé est permise dans les restaurants pour l'ajout du pourboire. Par conséquent, le montant actuel (ou final) ne doit pas dépasser le montant autorisé de plus de 15 %.
- Assurez-vous que les caractéristiques et les descriptions des biens et des services pour les transactions avec carte absente sont détaillées, précises et non trompeuses.
- Assurez-vous que toute la marchandise expédiée a été reçue et signée par le titulaire de carte. Autant que possible, obtenez une empreinte de la carte au moment de la livraison. Demandez au titulaire de carte de signer la facture d'expédition.
- Assurez-vous que toute la marchandise expédiée répond au besoin pour lequel elle a été vendue, et assurez-vous qu'elle est livrée dans un état satisfaisant.
- Assurez-vous que vos politiques de retour, de remboursement et d'annulation sont clairement indiquées au moment de la transaction. Le défaut d'afficher vos politiques de remboursement ou de retour peut entraîner un litige si votre client retourne la marchandise.
- Si le titulaire de carte demande d'annuler une transaction récurrente facturée périodiquement (mensuellement, trimestriellement ou annuellement), vous devriez annuler la transaction, comme demandé par le titulaire de carte, conformément à votre entente avec le client.
- Pour les transactions dont la marchandise est expédiée ultérieurement, le client ne devrait être facturé qu'au moment de l'expédition de la marchandise.
- Demandez au titulaire de carte de signer une entente ou un contrat pour tout service à être fourni ou pour toute marchandise à être expédiée.
- Assurez-vous que tous les services sont fournis dans les délais impartis. Les services payés d'une autre façon ne devraient pas être portés à la carte du titulaire de carte.
- Évitez de traiter une transaction unique plus d'une fois; rapprochez vos dépôts quotidiens pour vous assurer que les transactions sont traitées correctement. Si vous remarquez qu'une transaction a été traitée deux fois, nous vous recommandons de créditer le compte du titulaire de carte immédiatement et d'avertir le titulaire de carte que la transaction en double a été remboursée afin d'éviter un débit compensatoire.

- Assurez-vous que tous les dépôts électroniques (ventes et remboursements) sont virés via votre terminal de PDV au cours des trois jours ouvrables suivant la date de la transaction.
- Assurez-vous que tous les remboursements sont enregistrés comme crédit/remboursement dans votre terminal de PDV, et non pas comme vente.
- Si la marchandise doit être expédiée, vous pouvez obtenir une autorisation pour une commande postale, téléphonique ou en ligne dans les sept jours civils suivant la date de la transaction. Pour ce type de transaction, la date de la transaction correspond à la date où la marchandise est expédiée.

Programmes des marques de cartes

Les marques de cartes surveillent les taux de fraude et de débit compensatoire pour les commerçants acceptant leurs cartes.

Remarque : *Les règles de Visa, de MasterCard, de Discover et d'American Express sont disponibles publiquement sur les sites :*

- **visa.ca/marchand**
- **mastercard.com/ca/merchant/fr/**
- **discovernetwork.com/merchants/services**
- **americanexpress.ca/optblueguide**

Programmes de gestion du risque

Les marques de cartes surveillent les niveaux de fraude et de débit compensatoire de tous les commerçants acceptant leurs cartes. Les taux de débit compensatoire et de fraude de ces commerçants doivent rester sous le seuil établi et, chaque fois que des fraudes ou des débits compensatoires excessifs sont découverts, les commerçants doivent prendre des mesures correctives.

Les mesures correctives qu'un commerçant doit entreprendre dépendent de certains facteurs comprenant, mais sans s'y limiter, le type de commerçant, le volume de ventes du commerçant et son emplacement. Les commerçants doivent souvent former davantage leur personnel en ce qui concerne les procédures d'acceptation des cartes. Il est aussi possible qu'ils doivent élaborer un plan détaillé pour réduire les débits compensatoires et les fraudes.

En tant que commerçant, vous pouvez faire partie de quelques-uns des programmes de marques de cartes suivants :

Remarque : *Chacun des programmes de surveillance de Visa, de MasterCard, de Discover, d'UnionPay et d'American Express listé est sujet à différents frais ou amendes et à différentes structures d'évaluation. Ces programmes sont occasionnellement sujets à changement, et ces changements peuvent comprendre une modification des critères et des seuils.*

Programmes Visa

Programme de rendement antifraude à l'intention des marchands (PRAFM) – Ce programme comprend les seuils de rendement antifraude pour les commerçants ainsi qu'un cadre de conformité pour assurer la résolution des fraudes en temps opportun afin de réduire adéquatement les niveaux de fraude.

Le programme comporte deux volets : un premier volet qui correspond au rendement antifraude du marché local, et un deuxième volet qui correspond au rendement antifraude interrégional et transfrontalier. Le volet concernant la fraude dans les marchés locaux mesure les activités de fraude et de vente à l'échelle nationale et identifie les commerçants ne respectant pas les seuils de rendement de Visa Canada. Les commerçants ont un délai précis pour résoudre leur problème de rendement, après quoi une amende peut être donnée.

Le volet concernant la fraude interrégionale et transfrontalière mesure les activités de fraude et de vente entre les régions Visa et identifie les commerçants ne respectant pas les seuils de rendement de Visa Canada. Ce volet comporte deux méthodes de mesure de rendement :

- **Seuil minimal de rendement antifraude :** Ce seuil est conçu pour assurer la résolution rapide des problèmes survenant régulièrement en raison du non-respect des mesures de contrôle et d'acceptation des cartes interrégionales et transfrontalières.
- **Seuil de rendement antifraude excessif :** Ce seuil met en œuvre des actions immédiates contre les commerçants présentant un risque de fraude interrégionale élevé pour l'émetteur de cartes en fonction du seuil de norme de rendement établi par Visa. Les commerçants ont un délai établi pour résoudre ces problèmes de rendement, après quoi des débits compensatoires et des amendes peuvent être imposés.

Programme mondial de contrôle des débits compensatoires des commerçants (PMCDCC) – Visa surveille les transactions internationales pour identifier les commerçants qui génèrent un nombre excessif de débits compensatoires (en lien avec les transactions par cartes internationales). Les commerçants ont un délai établi pour résoudre ces problèmes de rendement, après quoi des débits compensatoires et des amendes peuvent être imposés.

Programmes MasterCard

Programme mondial de vérification des commerçants (PMVC) – Le programme mondial de vérification des commerçants (PMVC) est un programme de gestion et de surveillance de la fraude qui détecte les commerçants ayant un niveau de fraude mensuel inacceptable en fonction des critères du programme. Les commerçants ont un délai établi pour résoudre ces problèmes de rendement, après quoi des débits compensatoires et des amendes peuvent être imposés.

Programme de débits compensatoires excessifs (PDCE) – Le programme de débits compensatoires excessifs (PDCE) est conçu pour surveiller de façon continue le rendement des débits compensatoires des commerçants et de déterminer rapidement si un commerçant a dépassé, ou s'apprête à dépasser, le seuil mensuel de débits compensatoires. Le ratio débits compensatoires/transactions correspond au nombre de débits compensatoires d'un commerçant dans un mois donné divisé par le nombre de transactions traitées à l'aide d'une carte MasterCard au cours du mois précédent.

Programmes UnionPay

« High-Risk Merchant Monitoring Program (HMMP) » – Le programme *High-Risk Merchant Monitoring Program (HMMP)* est un programme de gestion et de surveillance de la fraude qui détecte les commerçants ayant un niveau de fraude mensuel inacceptable en fonction des critères du programme. Les commerçants ont un délai établi pour résoudre ces problèmes de rendement, après quoi des débits compensatoires et des amendes peuvent être imposés.

« Merchant Chargeback Monitoring Program (MCMP) » – Le programme *Merchant Chargeback Monitoring Program (MCMP)* mesure le nombre de débits compensatoires liés aux ventes d'un commerçant. Le programme surveille le nombre de débits compensatoires pour s'assurer que le ratio débits compensatoires/transactions n'est pas excessif. Les commerçants ont un délai établi pour résoudre ces problèmes de rendement, après quoi des débits compensatoires et des amendes peuvent être imposés.

Programme Discover

Le programme de débits compensatoires excessifs de Discover est conçu pour surveiller les statistiques sur les débits compensatoires et les remboursements ainsi que pour s'assurer que le coefficient mensuel de débits compensatoires d'un commerçant par rapport à son nombre de transactions n'est pas excessif.

Programme American Express

Le programme American Express surveille les débits compensatoires disproportionnés ainsi que la fraude liée au rendement.

> Pour de plus amples renseignements au sujet des programmes de gestion du risque, y compris les seuils de conformité et les amendes possibles pour le non-respect de ces seuils, consultez la page **moneris.com/fraude**.

Autres programmes

Programme NSR de Discover (aucune signature requise)

Les transactions Discover d'un montant égal ou inférieur à 50,00 $ CA (taxes et pouboires inclus) sont admissibles au programme NSR de Discover. Afin de permettre un service encore plus rapide, ce programme permet aux commerçants de traiter des transactions Discover sans devoir obtenir une signature sur le reçu ou remettre un reçu aux clients. Les commerçants doivent toutefois remettre un reçu au client s'il le désire.

Pour être admissible au programme NSR de Discover, une transaction doit posséder les caractéristiques suivantes :

- La transaction est identifiée correctement, et le montant total de cette transaction est égal ou inférieur à 50,00 $ (taxes et pourboires inclus).
- La carte est glissée et la transaction est autorisée.
- La carte était présente lors de la transaction.
- La transaction est traitée à l'aide d'une carte à bande magnétique; les transactions traitées à l'aide de cartes à puce ne sont pas admissibles.

Programme sans signature/sans NIP d'American Express

Le programme sans signature/sans NIP d'American Express permet aux commerçants de ne pas exiger de NIP ou la signature du titulaire de carte sur le reçu de transaction. Le seuil établi pour qu'une transaction soit admissible au programme sans signature/sans NIP d'American Express est de 50,00 $ CA ou moins (taxes et pourboire inclus). Le commerçant n'est pas obligé de remettre un reçu au titulaire de carte conformément au programme sans signature/sans NIP d'American Express, à moins que le titulaire de carte en fasse la demande.

Pour qu'une transaction soit admissible au programme sans signature/sans NIP d'American Express, elle doit répondre aux critères suivants :

- Le montant de la transaction doit être égal ou inférieur à 50,00 $ CA (taxes et pourboire inclus).
- La transaction doit être autorisée.
- La carte doit être présente au moment de la transaction.

Si la transaction ne respecte pas ces trois critères d'admissibilité, le programme sans signature/sans NIP d'Amex ne s'applique pas.

Programmes sans contact

Les transactions sans contact dont le montant est inférieur à la limite établie (consultez le tableau ci-dessous pour plus de détails) ne nécessitent pas de NIP ou de signature.

Pour activer ces programmes, vous devez posséder un lecteur sans contact et un terminal de point de vente certifié prenant en charge les transactions sans contact ou un système logiciel certifié. Seules les transactions traitées par l'entremise d'un lecteur sans contact certifié sont admissibles à ces programmes.

Programme sans contact	Le programme sans contact s'applique aux transactions dont le montant est inférieur ou égal à :	Marche à suivre pour les transactions dont le montant dépasse la limite établie :
Visa payWave	100,00 $ CA (taxes et pourboires inclus)	Obtenez la signature du titulaire de carte pour les transactions de plus de 100,00 $ CA.
MasterCard TAPEZ ET PARTEZ[MC]	100,00 $ CA (taxes et pourboires inclus)	Les transactions de plus de 100,00 $ doivent être payées d'une autre façon. Demandez au titulaire de carte d'insérer ou de glisser sa carte. Si le lecteur sans contact est utilisé pour des transactions de plus de 100 $ CA, la protection contre les débits compensatoires ne s'appliquera plus et vous serez responsable du montant total de la transaction.
Flash *Interac*	100,00 $ CA (taxes et pourboires inclus)	Les transactions de plus 100,00 $ doivent être payées d'une autre façon. Demandez au titulaire de carte d'insérer sa carte.
Discover ZIP	50,00 $ CA (taxes et pourboires inclus)	Obtenez la signature du titulaire de carte pour les transactions de plus de 50,00 $ CA.
American Express	100,00 $ CA (taxes et pourboires inclus)	Obtenez la signature du titulaire de carte pour les transactions de plus de 100,00 $ CA.

> Pour de plus amples renseignements au sujet des programmes sans contact, consultez la page **moneris.com/quickservice**.

Normes d'acceptation des cartes

Les commerçants souhaitant traiter des transactions par cartes doivent respecter les normes suivantes :

Troncature du numéro de compte primaire (PAN) (masquage de carte)

Le numéro de compte primaire (PAN) apparaît sur les reçus de transaction générés automatiquement et il doit être masqué.

Copie du titulaire de carte – Tous les chiffres du PAN, à l'exception des quatre derniers, doivent être cachés ou supprimés et, si applicable, la date d'expiration de la carte ne doit pas apparaître sur le reçu de transaction du titulaire de carte.

Remarque : Interac *indique qu'une version abrégée du PAN peut être utilisée si elle indique précisément la carte utilisée au cours de la transaction.*

Copie du commerçant – Seuls les six (6) premiers chiffres du PAN ainsi que les quatre (4) derniers peuvent figurer sur le reçu de transaction du commerçant, et les chiffres restants doivent être cachés et la date d'expiration doit être supprimée. Les marques de cartes exigent que les chiffres cachés soient remplacés par des caractères de remplissage n'étant ni des espaces blancs, ni des caractères numériques comme « x », « * » ou « # ».

Cartes prépayées

Les cartes prépayées de Visa, de MasterCard, de Discover, d'UnionPay et d'American Express sont des cartes de paiement comportant un montant prédéfini pouvant être utilisées dans n'importe quel commerce acceptant les paiements par cartes de crédit.

Pour traiter une transaction par carte prépayée :

- Demandez au titulaire de carte quel montant vous devez déduire de la carte.
- Traitez la transaction de la même façon qu'une transaction par carte de crédit : glissez la carte, saisissez le montant et obtenez une autorisation en ligne.
- Demandez au titulaire de carte de signer le reçu, puis vérifiez que cette signature correspond à celle de la carte.
- Une carte prépayée ne peut être traitée qu'à l'aide d'un terminal de PDV pouvant obtenir immédiatement une autorisation en ligne.

Frais supplémentaires et de commodité

Vous ne devez pas ajouter de frais supplémentaires ou de commodité à n'importe quelle transaction, à moins que les règles de la marque de cartes vous le permettent.

Interdiction d'établir un montant minimal ou maximal de transaction

Il vous est interdit d'établir un montant minimal ou maximal pour l'acceptation d'une carte valide présentée adéquatement.

Transactions interdites

Une transaction interdite signifie :

- une transaction effectuée par le commerçant ou à la suite d'une activité interdite ou illégale;
- une transaction indiquée par Moneris comme étant interdite;
- toute transaction pour laquelle vous n'avez pas d'autorisation de traitement.

Vous ne devez pas soumettre des transactions aux fins de paiement d'interchange comprenant, mais sans s'y limiter, toute transaction qui :

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

Transactions illégales ou qui nuisent à l'image de la marque de cartes

Vous ne devez pas accepter un paiement par carte pour toute transaction illégale ou qui, à la seule discrétion des marques de cartes, pourrait porter atteinte à la réputation de ces marques.

Les marques de cartes considèrent toutes les activités suivantes comme non-respect de cette règle :

- La vente ou l'offre de vente d'un produit ou d'un service n'étant pas totalement conformes à la loi qui s'applique à l'acquéreur de transactions, à l'émetteur de cartes, au commerçant, au titulaire de carte ou aux marques de cartes.
- La vente d'un produit ou d'un service comprenant une image, mais sans s'y limiter, qui est offensive ou qui manque de valeur artistique sérieuse (par exemple, mais sans s'y limiter, des images de comportements sexuels non consensuels, l'exploitation sexuelle d'un mineur, la mutilation non consensuelle d'une personne ou d'une partie du corps d'une personne, et la bestialité) ou tout autre matériel qu'une marque de cartes considère comme inacceptable à la vente relativement à son image de marque.

Virement des fonds

Vous devez présenter les registres d'une transaction valide dans un délai maximal de trois jours ouvrés après la date de la transaction.

Vente ou échange d'information

Il vous est interdit de vendre, d'acheter, de fournir, d'échanger ou de dévoiler de quelque façon que ce soit un numéro de carte, une transaction ou tout renseignement au sujet du titulaire de cartes à toute entité autre que votre acquéreur de transactions, les marques de carte ou en réponse à une demande valide du gouvernement. Ces interdictions s'appliquent aux empreintes de carte, aux reçus de transaction, aux copies au carbone, aux listes postales, aux enregistrements, aux dossiers des bases de données et à tout autre média créé ou obtenu à la suite d'une transaction.

Vous ne devez pas demander ou utiliser le numéro de carte ou les renseignements personnels d'un titulaire de carte à des fins que vous reconnaissez, ou devriez reconnaître, comme frauduleuses ou non conformes aux normes de la marque de cartes, ou à toute fin non autorisée par le titulaire de carte.

Factures et dépôts multiples – transactions différées

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

Vous n'avez pas le droit de traiter des transactions de vente pour lesquelles seule une partie du montant est incluse sur la facture, à l'exception des cas suivants :

- le solde dû est payé par le titulaire de carte au moment de la transaction de vente par une autre méthode de paiement, soit en argent comptant ou par chèque, ou les deux; ou
- le titulaire de carte demande deux factures si la totalité ou une partie de la marchandise ou des services sera fournie ultérieurement. Si tel est le cas, deux factures seront créées; un dépôt peut être effectué pour une facture, et le paiement du solde sera effectué à la complétion de la seconde facture (la seconde facture est conditionnelle à la livraison de la marchandise ou au rendement des services identifiés). Les deux factures doivent être autorisées.

Vous devrez inscrire « dépôt » ou « solde » sur les factures, au besoin. La facture portant la mention « solde » ne sera pas présentée tant que la marchandise n'est pas livrée ou que le service n'est pas complété.

Exigences relatives à l'autorisation

L'autorisation représente une étape cruciale au processus d'acceptation d'une carte.

- 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 est expirée, vous ne devez pas traiter cette transaction.
- Si vous traitez une transaction portant sur les voyages et le divertissement, assurez-vous de respecter les modalités d'autorisation si vous voulez être en mesure de traiter des autorisations différentielles.

- Respecter ce manuel d'utilisateur et cette section n'exclut pas la possibilité de débits compensatoires en vertu de votre convention d'affiliation. En cas de doute, que votre transaction ait été autorisée ou non, vous demeurez responsable d'une transaction comprenant, mais sans s'y limiter, les éléments suivants :
  - le titulaire de carte est présent, mais n'a pas sa carte;
  - le titulaire de carte ne signe pas la facture;
  - la signature semble non autorisée ou ne correspond pas à celle de la carte; ou
  - la carte est expirée.

Retours de marchandise, crédits et redressements

Votre politique de retour relative aux biens et aux services payés par carte de crédit doit être équitable, sauf si autrement interdit par la loi. Cette politique doit au moins être équivalente à la politique de retour relative aux biens et aux services payés d'une autre façon, à moins de divulgation complète de la politique au moment de la transaction et sous réserve que la facture comporte un avis évident à cet effet avant de compléter la transaction.

- Le défaut d'afficher votre politique de remboursement ou de retour peut entraîner un litige si le client retourne la marchandise.
- Un affichage adéquat n'inclut pas une déclaration annulant le droit d'un titulaire de carte de contester la transaction avec son émetteur de carte.
- Les remboursements peuvent seulement être effectués sur la carte utilisée lors de l'achat initial.

Conversion de devises

Moneris offre deux services de conversion de devises : la conversion de devises dynamique (CDD), qui permet aux commerçants de traiter des transactions dont la carte est présente (transaction en personne), et ce, dans la devise du titulaire de carte, et la conversion de prix, qui permet aux commerçants de traiter des transactions en plusieurs devises lorsque la carte est absente (en ligne, par exemple). Si vous offrez, ou nous demandez d'offrir, la conversion de devises dynamique ou un autre service de conversion de devises, vous devez :

- Aviser les titulaires de carte que le service de conversion de devises est facultatif.
- Vous assurer que le titulaire de carte est la seule autre partie à accepter ou à refuser d'utiliser le service de conversion de devises.
- Ne pas avoir d'exigence supplémentaire pour les titulaires de carte afin que la transaction soit traitée dans sa devise.
- Ne pas utiliser de langage ou de procédure obligeant le titulaire de carte à choisir les services de conversion de devises par défaut.
- Ne pas faussement présenter, de façon explicite ou implicite, les services de conversion de devises comme étant offerts par les marques de cartes.
- Répondre à toutes les exigences relatives aux reçus que nous demandons ou que les marques de cartes demandent de temps à autre.
- Répondre à toutes les autres exigences relatives aux services de conversion de devises dont nous pouvons vous faire part de temps à autre, ou requises dans les règles et réglementations des marques de cartes.

Transactions périodiques

Si vous décidez d'accepter les transactions périodiques pour l'achat de biens ou de services livrés ou rendus périodiquement (mensuellement, trimestriellement ou annuellement par exemple), le titulaire de carte devra rédiger et vous remettre une demande écrite pour que de tels biens ou services soient facturés à son compte. La demande écrite doit minimalement spécifier la fréquence des transactions facturées au compte du titulaire de carte, les frais périodiques et la durée pour laquelle cette permission est accordée.

Dans le cas du renouvellement d'une transaction périodique, le titulaire de carte doit rédiger et vous remettre une autre demande écrite pour que les biens ou services continuent d'être facturés à son compte. Une transaction périodique peut comprendre le paiement de frais périodiques comme une prime d'assurance, un abonnement, une cotisation, des droits de scolarité ou des frais de service.

Sauf stipulation contraire du présent manuel, une transaction périodique ne peut comprendre un paiement partiel effectué pour l'achat de biens ou de services en une transaction unique, ni ne peut servir pour le paiement ponctuel de biens. L'autorisation écrite du titulaire de carte doit être conservée pour la durée de la transaction périodique et fournie à la demande de Moneris ou des marques de cartes.

Il est interdit de traiter une transaction périodique initiale ou ultérieure après avoir reçu un avis d'annulation de la part du titulaire de carte ou de celle de Moneris, ou après avoir été avisé de ne pas accepter la carte.

Veuillez indiquer lisiblement la mention « transaction périodique » sur la ligne de signature d'une facture pour une transaction périodique.

Équipement perdu ou volé

En cas d'équipement perdu ou volé, veuillez communiquer immédiatement avec le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**. Au besoin, un agent de service prendra des dispositions pour remplacer l'équipement de PDV manquant.

Remarque : *Les commerçants de Moneris sont responsables d'assurer la sécurité de tout équipement loué en leur possession. Veuillez consulter les modalités de votre convention d'affiliation pour obtenir de plus amples renseignements.*

Normes de sécurité de l'industrie du paiement

Le *Payment Card Industry Security Standards Council* (PCI SSC) est responsable du développement et de l'évolution continue des normes de sécurité concernant la protection des données du compte des titulaires de cartes. Le PCI SSC gère présentement les normes de sécurité suivantes :

- la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS);
- la norme PCI des transactions à NIP (PTS);
- la norme de sécurité des données des applications de paiement (PA-DSS).

Le PCI SSC est aussi responsable de la formation et de la qualification des évaluateurs et des fournisseurs de sécurité qui s'assurent que les commerçants et les fournisseurs de services respectent ces normes. Le PCI SSC n'a pas à s'assurer de la mise en application de ces normes, cela relève entièrement des marques de cartes.

> Pour de plus amples renseignements au sujet du PCI SSC, veuillez consulter la page **pcisecuritystandards.org**.

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

La norme PCI DSS est une norme de sécurité à plusieurs volets comprenant les exigences en matière de gestion de la sécurité, les politiques, les procédures, l'architecture du 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 relatives aux comptes des titulaires de carte.

Voici les exigences principales de la norme PCI DSS que vous devez respecter :

- Créer et maintenir un réseau sécuritaire
  - Installer un pare-feu et contrôler sa configuration pour protéger les titulaires de carte.
  - Ne pas utiliser les mots de passe et les autres paramètres de sécurité par défaut pour votre système.
- Protéger les données des titulaires de carte
  - Protéger les données des titulaires de carte enregistrées.
  - Chiffrer la transmission des données des titulaires de carte sur les réseaux ouverts et publics.
- Maintenir un programme de gestion de la vulnérabilité
  - Utiliser un antivirus et le mettre à jour régulièrement.
  - Développer et maintenir des systèmes et des applications sécuritaires.
- Mettre en place des mesures de contrôle d'accès rigoureuses
  - N'autoriser l'accès aux données des titulaires de carte qu'aux personnes ayant vraiment besoin de les consulter.
  - Assigner 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 les réseaux régulièrement
  - Surveiller et tester tous les accès aux ressources du réseau et aux données du titulaire de carte.
  - Tester régulièrement la sécurité et les processus du système.
- Maintenir une politique de sécurité de l'information
  - Maintenir une politique en matière de sécurité de l'information.

› La norme PCI DSS complète ainsi que de la documentation connexe sont disponibles sur le site **pcisecuritystandards.org**.

Stockage des données des titulaires de carte

Le tableau suivant illustre les données des titulaires de carte fréquemment utilisées ainsi que les données d'authentification sensibles. Il indique aussi s'il est permis ou non de stocker chaque élément et si chaque élément de données doit être protégé.

Instructions relatives aux données des titulaires de carte

		Données	Stockage permis	Rendre illisible les données stockées selon la règle 3.4
Données du compte	**Données du titulaire de carte**	Numéro de compte primaire (PAN)	✓	✓
		Nom du titulaire de carte	✓	X
		Code de service	✓	X
		Date d'expiration	✓	X
	Données d'authentification sensibles[1]	Données complètes de la bande magnétique[2]	X	Stockage non permis selon la règle 3.2
		CAV2/CVC2/ CVV2/CID	X	Stockage non permis selon la règle 3.2
		NIP/Blocage du NIP	X	Stockage non permis selon la règle 3.2

[1] Les données d'authentification sensibles ne doivent pas être stockées à la suite d'une autorisation (même si elles sont chiffrées).
[2] L'ensemble des données stockées sur la bande magnétique, données équivalentes sur la puce ou à un autre endroit.

Fournisseurs de services

Un fournisseur de services est un organisme qui stocke, traite ou transmet les données des titulaires de carte au nom des commerçants ou des fournisseurs de services. Tous les fournisseurs de services doivent respecter la norme PCI DSS. De plus, tous les fournisseurs de services doivent confirmer leur conformité à la norme PCI DSS. Il incombe au commerçant de s'assurer que son fournisseur de services utilisé pour stocker, traiter ou transmettre les données des titulaires de carte respecte la norme PCI DSS.

Programmes de conformité des marques de cartes

Chaque marque de cartes a élaboré son propre programme de conformité pour s'assurer que les commerçants et les fournisseurs de services respectent la norme PCI DSS.

Chaque programme possède des exigences de validation spécifiques devant être respectées pour que la marque de cartes reconnaisse la certification à la norme PCI DSS. Tous les commerçants et fournisseurs de services stockant, traitant ou transmettant des données des titulaires de carte doivent respecter la norme PCI DSS.

Pour obtenir de plus amples renseignements au sujet des programmes de conformité des marques de cartes, consultez les pages suivantes :

Programme de sécurité de l'information concernant les comptes de Visa Canada (Visa Canada Account Information Security Program (AIS))	**visa.ca/ais**
Programme de détection des données MasterCard (MasterCard Site Data Protection Program (SDP))	**mastercard.com/sdp**
Programme DISC (sécurité de l'information et conformité) (Discover Information Security & Compliance (DISC) Program)	**discovernetwork.com/disc**

Brèches de sécurité

La compromission des données d'un compte correspond à (est définie par) l'accès par un individu non autorisé, qu'il s'agisse d'un employé mécontent, d'un compétiteur malveillant ou d'un pirate malavisé, aux renseignements relatifs au compte d'un titulaire de carte. Les brèches de sécurité peuvent être causées par une brèche du système résultant d'une attaque électronique des systèmes électroniques ou de communication. Elles peuvent aussi être causées par une brèche physique où un individu s'est introduit par effraction pour voler des documents papier, des appareils de traitement des transactions ou des ordinateurs contenant des données des titulaires de carte.

Les entreprises qui soupçonnent ou confirment une brèche de sécurité doivent prendre des mesures rapidement pour prévenir l'exposition supplémentaire des données des titulaires de carte :

- Contenez et limitez immédiatement l'exposition des données.
- Avisez immédiatement toutes les parties nécessaires, y compris Moneris.
- Fournissez à Moneris une description détaillée des événements ainsi qu'une liste de tous les numéros de carte ayant pu être compromis.
- Élaborez un plan de redressement pour répondre aux problèmes de sécurité ayant causé la brèche de sécurité.

> Si vous soupçonnez que les données ont été compromises, ou si vous le confirmez, communiquez immédiatement avec le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**.

Si un commerçant est victime d'une brèche de sécurité entraînant la compromission des données des titulaires de carte, il risque de :

- devoir assumer le coût d'une enquête judiciaire;
- recevoir une évaluation de non-conformité;
- devoir assumer les coûts engagés par les émetteurs de cartes, comme la surveillance des cartes, la réémission d'une carte et les pertes liées à la fraude;
- devoir assumer les coûts de validation de la conformité à la norme PCI DSS; et
- devoir cesser le service de traitement des transactions par cartes.

Norme de sécurité des données des applications de paiement (PA-DSS)

La norme PA-DSS est une norme de sécurité s'appliquant aux applications de paiement développées par les fournisseurs de logiciels et vendues, distribuées ou mises sous licence aux commerçants. L'objectif de la norme PA-DSS est d'aider les fournisseurs de logiciels à développer des applications de paiement sécuritaires qui n'enregistrent pas les données sensibles et qui aident les commerçants à respecter la norme PCI DSS. Tous les commerçants utilisant une application de paiement doivent s'assurer que l'application respecte les exigences de la norme PA-DSS.

En utilisant une application de paiement conforme à la norme PA-DSS, vous aider à réduire les risques de compromissions des données, à prévenir le stockage de données interdit et à respecter la norme PCI DSS.

> Pour obtenir de plus amples renseignements au sujet des mandats et des délais de la norme PA-DSS, consultez la page **moneris.com/pci**.

> Vous trouverez de plus amples renseignements au sujet de la norme PA-DSS, ainsi qu'une liste des applications validées, sur le site Web **pcisecuritystandards.org**.

Commerce électronique

Voici certains éléments à savoir si vous gérez un commerce en ligne.

Développer votre site Web de commerçant

Vous devez vous assurer que l'identité de votre entreprise est clairement affichée sur votre site Web à tout moment afin que le titulaire de carte puisse différencier votre entreprise des autres parties, comme les fournisseurs de produits ou de services au commerçant.

Votre site Web doit comporter tous les éléments suivants :

- Le nom de votre entreprise doit clairement être affiché.
- Le nom d'entreprise affiché sur votre site Web doit correspondre de façon évidente au nom de votre entreprise et au nom apparaissant sur le relevé du titulaire de carte.
- Le nom de votre entreprise doit être affiché aussi clairement que les autres renseignements sur votre site, autres que les images des produits ou des services offerts.
- Les marques de cartes doivent être affichées en couleur pour indiquer l'acceptation des cartes de crédit et de débit.
- Une description complète des biens ou des services offerts doit être affichée.
- Les renseignements concernant l'entreprise et les coordonnées du service à la clientèle doivent comprendre :
  - une adresse courriel;
  - un numéro de téléphone;
  - l'adresse de l'établissement permanent du commerçant.
- Les conditions d'utilisation, notamment les restrictions d'exportation (au besoin) ou toute restriction légale, doivent être clairement affichées lors du passage à la caisse virtuel.

- Les politiques de retour ou de remboursement détaillant les options de retour ou de remboursement doivent être affichées avant que le client achète un produit ou un service.
- La devise utilisée (p. ex., dollars américains, dollars canadiens) doit être affichée.
- Un bouton « cliquer pour accepter » sur lequel le titulaire de carte doit cliquer ou une action affirmative semblable que le titulaire doit effectuer lors de la complétion d'une commande en ligne.
- Un reçu imprimable doit s'afficher une fois que le titulaire de carte confirme l'achat.
- La politique d'expédition doit être affichée.
- Le pays dans lequel se situe le commerçant doit être affiché lorsque les options de paiements sont présentées au titulaire de carte.
- La politique de confidentialité doit être affichée.
- Les capacités et la politique de sécurité relatives à la transmission des données lors d'un paiement par carte doivent être affichées.

Le reçu de votre commerce électronique doit comporter tous les renseignements suivants :

- nom du commerçant;
- adresse courriel du commerçant;
- montant de la transaction (ou du crédit), affiché en argent;
- date de la transaction (ou date de préparation du crédit);
- numéro d'identification de transaction unique;
- nom de l'acheteur;
- code d'autorisation;
- type de transaction (achat ou crédit);
- description de la marchandise ou des services;
- politique de retour et de remboursement (si restreinte).

Exigences en matière de sécurité pour protéger votre réseau

Vous et votre fournisseur de services devez respecter la norme minimale en matière de chiffrement pour la collecte et la transmission des données des titulaires de carte. Vous devez obtenir une autorisation pour chaque transaction électronique. Vous ne pouvez pas refuser de compléter une transaction électronique sous prétexte que le titulaire de carte ne possède pas de certificat numérique ou d'autres protocoles de sécurité.

Vérifié par Visa (VpV)

Vérifié par Visa est un service mondial d'authentification en ligne permettant de sécuriser le magasinage électronique à la fois pour les commerçants Visa et les titulaires de carte.

VpV offre à votre entreprise une protection supplémentaire contre les transactions frauduleuses et les débits compensatoires pour les ventes électroniques, tout en permettant aux titulaires de carte de magasiner en ligne avec confiance, ce qui peut transformer les clients potentiels en acheteurs.

> Pour participer au programme VpV, appelez-nous au **1 866 666-3747**. Pour de plus amples renseignements au sujet de VpV, visitez la page **visa.ca**.

MasterCard SecureCode[MD]

MasterCard SecureCode est une solution électronique qui permet à vos clients de s'identifier à leur émetteur de cartes à l'aide d'un mot de passe personnel unique en plus de vous indiquer s'il s'agit d'un véritable acheteur.

Un SecureCode est un code privé connu uniquement par le titulaire de carte et son institution financière; ce code permet d'améliorer la sécurité du compte MasterCard du titulaire en le protégeant contre l'utilisation non autorisée de sa carte lorsqu'il achète en ligne sur le site Web des commerçants participants.

> Pour participer au programme SecureCode, appelez-nous au **1 866 666-3747**. Pour de plus amples renseignements au sujet du MasterCard SecureCode, visitez la page **mastercard.ca**.

Code de vérification de la carte (CVC)

Le code de vérification de la carte (CVC) est une exigence de sécurité des cartes de crédit. Il s'agit d'un code à 3 chiffres qui se trouve à l'endos des cartes Visa, MasterCard, Discover et UnionPay. Il est imprimé à la fin de la boîte de signature, ou dans une boîte blanche située à côté de la boîte de signature. Pour les cartes American Express, il s'agit d'un code à 4 chiffres situé à l'avant de la carte. (Consultez la section *Reconnaître les caractéristiques de sécurité* à la page 15.)

Après avoir soumis une demande d'autorisation pour valider l'information d'une carte (numéro de compte, date d'expiration et CVC), le commerçant reçoit une réponse lui indiquant si le CVC correspond ou non, lui permettant ainsi de prendre les mesures appropriées. Peu importe la réponse de la vérification du CVC reçue, le commerçant ne devrait pas compléter la transaction si l'émetteur de la carte n'approuve pas la demande d'autorisation.

Le CVC permet aux commerçants traitant des transactions en ligne ou par téléphone de vérifier si le titulaire de carte a en sa possession une carte véritable. Les émetteurs de cartes Visa offrent une vérification du CVC en temps réel pour vous permettre de vérifier si la personne effectuant l'achat a bel et bien la carte en main.

Si le commerçant soumet une demande d'authentification du CVC et que l'émetteur de la carte ne participe pas à la validation, le commerçant ne sera pas tenu responsable de toute transaction potentiellement frauduleuse. Si l'acheteur fournit seulement le numéro à 16 chiffres de sa carte de crédit ainsi que la date d'expiration, cela signifie qu'il n'est probablement pas en possession de la carte et que la transaction est potentiellement frauduleuse.

> Pour obtenir plus de renseignements au sujet des outils de prévention de la fraude électronique, consultez la page **moneris.com/outilsfraude** ou appelez-nous au **1 866 666-3747**.

Service de vérification de l'adresse (SVA)

Le SVA vérifie en temps réel l'adresse de facturation d'un titulaire de carte et fournit au commerçant un code de résultat distinct du code de réponse d'autorisation, ce qui permet au commerçant de prendre une décision informée au sujet de l'évaluation du risque et de déterminer s'il continue de traiter la transaction ou non.

Le SVA assure que la personne qui effectue l'achat avec sa carte est la même personne qui reçoit le relevé de carte mensuel. En faisant correspondre l'adresse de facturation du dossier à l'adresse de facturation fournie par le titulaire de carte à l'émetteur de la carte, les commerçants et les émetteurs travaillent ensemble pour s'assurer que les cartes perdues ou volées ne sont pas utilisées pour acheter des biens ou des services dans un environnement de carte non présente.

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

Remarque : *Il est interdit de stocker les CVC une fois que l'autorisation a été obtenue pour la transaction. (Consultez la section* Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) *à la page 46.)*

Foire aux questions

Voici une liste des questions les plus souvent posées par les commerçants, ainsi que les réponses correspondantes.

Traitement des transactions

Q. Puis-je imposer des frais à un titulaire de carte pour l'utilisation de sa carte Visa, MasterCard, American Express, Discover, UnionPay ou débit *Interac*?

R. Non. Vous n'avez pas le droit de facturer des frais supplémentaires pour l'utilisation d'une carte. Peu importe le type de produits vendus, facturer des frais supplémentaires à un titulaire de carte pour traiter une transaction à l'aide d'une carte va à l'encontre de votre convention d'affiliation. Vous ne pouvez pas non plus imposer un montant d'achat minimal ou maximal lorsque le paiement est effectué à l'aide d'une carte. (Consultez les sections à la page 38.)

Q. Si un titulaire de carte me dit qu'il n'a pas sa carte avec lui, mais qu'il aimerait faire un achat, puis-je effectuer la transaction à l'aide du numéro de carte et de la date d'expiration?

R. Non. Ne complétez jamais une transaction en personne si la carte est absente. Vous devez pouvoir glisser, insérer ou présenter la carte et obtenir la signature du titulaire de carte.

Q. Si un titulaire de carte me paie par chèque et que j'utilise son numéro de carte de crédit comme identification, puis-je porter un montant à sa carte de crédit si le chèque est retourné en raison de fonds insuffisants?

R. Non. Porter des frais à une carte de crédit afin de régler une dette non recouvrable va à l'encontre de votre convention d'affiliation. Nous vous suggérons de communiquer avec le titulaire de carte et de convenir d'une autre méthode de paiement.

Q. Un touriste états-unien veut faire un achat dans mon commerce. Puis-je lui facturer le montant en dollars des États-Unis et compléter la facture avec ce montant afin de faciliter la transaction pour mon client?

R. Vous pouvez le faire si vous êtes un commerçant avec le service de conversion dynamique. (Consultez la section *Conversion de devises* à la page 43.) Si vous n'offrez pas le service de conversion dynamique, vous pouvez traiter vos transactions en dollars canadiens seulement. La banque émettrice de la carte de votre client fera la conversion de devises, et le montant équivalent en dollars des États-Unis sera facturé à votre client.

Protéger votre entreprise contre la fraude

Q. Que devrais-je faire si un titulaire de carte me présente une lettre l'autorisant à utiliser la carte de quelqu'un d'autre?

R. En aucun cas une personne autre que la personne dont le nom et la signature apparaissent sur la carte n'est autorisée à utiliser une carte.

Q. Ai-je le droit de demander à un titulaire de carte de me donner des renseignements personnels, comme son numéro de téléphone ou son adresse, pour les inscrire sur la facture comme mesure de sécurité supplémentaire?

R. Ne demandez jamais à un titulaire de carte d'inscrire son numéro de téléphone ou son adresse sur la facture. Vous pouvez lui demander des renseignements seulement s'ils sont nécessaires pour compléter la transaction (comme une adresse d'expédition). Si vous croyez que la transaction pourrait être frauduleuse ou si Moneris vous demande de le faire, vous pouvez demander des renseignements d'identification supplémentaires au titulaire de carte (une carte d'identité, par exemple). Une fois que vous avez vérifié la carte et que vous êtes satisfait, vous devriez inscrire « identité vérifiée » près de la signature du titulaire de carte. En aucun cas vous ne pouvez conserver les renseignements d'identification d'un titulaire de carte.

Q. Pourquoi est-ce que le numéro de carte du titulaire est tronqué sur le reçu?

R. Pour réduire les risques d'utilisation de carte frauduleuse, seule une partie du numéro de carte du titulaire est imprimé sur le reçu de transaction et dans certains rapports. Le reste du numéro de carte est masqué (c'est-à-dire que les autres chiffres sont remplacés par des astérisques (*)). Les numéros de carte de débit et de crédit sont masqués (y compris les numéros de carte des marques privées). Le masquage des numéros de carte est aussi connu sous le nom de « masquage de numéros de carte » et « troncation du PAN ». (Consultez la section *Troncature du numéro de compte primaire (PAN) (masquage de carte)* à la page 37.)

Débits compensatoires

Q. Je viens de recevoir une demande de facture/copie de reçu/récupération. Que dois-je faire?

R. Lisez attentivement les renseignements sur la demande de facture/copie de reçu/récupération, rassemblez toute la documentation pertinente (reçus, factures, contrats, etc.) et envoyez-la par télécopieur à Moneris au numéro de télécopieur fourni. (Consultez la section *Débits compensatoires* à la page 24.)

Q. Je viens d'envoyer le reçu de transaction demandé par télécopieur. Comment puis-je savoir s'il a été reçu?

R. Conservez la confirmation imprimée par votre télécopieur ou appelez Moneris 48 heures après l'envoi du reçu pour confirmer sa réception.

Q. Combien de temps devrais-je conserver une copie de mes factures de vente et de remboursement?

R. Pour les transactions par carte de crédit, conservez une copie de vos factures de vente et de remboursement pendant une période de 13 à 24 mois, selon le programme de cartes. (Consultez la section *Demandes de récupération* à la page 25.) Pour les transactions par carte de débit, conservez une copie de vos factures de vente et de remboursement pour une période de 12 mois.

Q. J'ai parlé avec un titulaire de carte qui a ensuite reconnu une transaction que j'ai traitée avec sa carte de crédit et qui a entraîné un débit compensatoire. Comment puis-je remédier à ce débit compensatoire?

R. Conseillez au titulaire de carte de communiquer avec sa banque émettrice de carte, d'où le litige provient, pour demander à être retiré du litige, ou répondez au débit compensatoire en demandant une déclaration écrite du titulaire de carte indiquant qu'il accepte les frais portés à son compte, et envoyez le document par télécopieur à Moneris.

Q. J'ai traité une transaction avec mon terminal de PDV et j'ai reçu un code d'autorisation. Pourquoi un débit compensatoire a-t-il été effectué pour cette transaction?

R. Même si vous avez reçu un code d'autorisation, un débit compensatoire peut tout de même être effectué si le titulaire de carte conteste la transaction ou si les procédures adéquates d'acceptation des cartes n'ont pas été suivies.

Autre

Q. J'ai récemment mis à jour mon terminal de PDV. Que devrais-je faire avec mon ancien équipement?

R. Veuillez appeler le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**, et Moneris enverra un messager chercher votre équipement et vos accessoires de PDV pour vous.

Q. Mon entreprise déménage. Qui dois-je appeler pour faire part de mon changement d'adresse?

R. Si votre entreprise change de propriétaire, d'adresse, de numéro de téléphone ou de numéro de télécopieur, communiquez avec le centre d'assistance à la clientèle de Moneris.

Autres ressources

Vous avez besoin d'aide?

Vous pouvez appeler le centre d'assistance à la clientèle de Moneris sans frais et en tout temps au **1 866 319-7450**.

- Pour obtenir un code d'autorisation à l'aide de notre système automatique, appelez-nous au **1 866 802-2637**.
- Si vous désirez parler à l'un de nos représentants commerciaux, appelez-nous au **1 866 666-3747**.

Obtenir un manuel à jour

Moneris peut périodiquement mettre à jour ce guide d'utilisation sur la page **moneris.com/manuels**.

Il vous incombe d'obtenir et d'utiliser la version la plus récente de ce guide.

Faites croître votre entreprise

MARCHAND DIRECT

Accès en tout temps aux transactions quotidiennes par cartes, aux relevés mensuels, aux rapports, et plus encore.

Consultez la page **moneris.com/marchanddirect**

ACHETER ET STOCKER

Achetez commodément toutes vos fournitures d'acceptation des paiements, y compris vos rouleaux de papier, vos décalcomanies, vos signes et plus encore.

Visitez le site **magasin.moneris.com** ou appelez le centre d'assistance à la clientèle de Moneris au **1 866 319-7450**

L'AVANTAGE INTERNE

Moneris s'engage à vous tenir informé des nouveautés du marché, des nouvelles formations et des tendances de l'industrie grâce à son bulletin *Moneris Insights Hub*.

Consultez la page **moneris.com/ressources**

Liens utiles

- **moneris.com**
- **visa.ca**
- **mastercard.ca**
- **discover.com**
- **unionpay.com**
- **interac.ca**
- **americanexpress.ca**

Remarque : *Certaines des règles de Visa, de MasterCard, de Discover et d'American Express sont accessibles au public sur les pages suivantes :*

visa.ca/marchand

mastercard.com/ca/merchant/fr/

discovernetwork.com/merchants/services

americanexpress.ca/optblueguide

Notes

Moneris

PRÊT POUR LES PAIEMENTS

moneris.com

MERMAN-F (05/16)