SOLUTIONS Moneris

Protection du terminal PDV

Réponses à vos questions courantes

Qu'est-ce que l'écrémage?

L'écrémage est l'enregistrement des données de compte stockées sur la bande magnétique d'une carte de crédit ou de débit à des fins frauduleuses.

Pourquoi les dispositifs point de vente (PDV) sont-ils ciblés par les voleurs?

Les terminaux PDV sont volés, altérés puis retournés aux établissements des commerçants dans le but d'écrémer ou de capturer des données de compte stockées sur la bande magnétique d'une carte de crédit ou de débit qui sont ensuite transférées à des cartes contrefaites.

Qu'est-ce qu'un terminal-leurre?

Un terminal-leurre est un dispositif qui ressemble au terminal qu'utilise un commerçant. Un leurre peut être utilisé pour remplacer un terminal volé afin de tromper un marchand. Il arrive souvent qu'un terminal-leurre n'ait pas le bon numéro de série. Une fois qu'il a altéré le dispositif, le fraudeur revient chez le commerçant pour l'installer et repart avec le terminal-leurre.

Que font les fraudeurs avec les données stockées sur la bande magnétique d'une carte de paiement?

Les données stockées sur la bande magnétique d'une carte de paiement sont transférées à des cartes contrefaites qui sont alors utilisées pour effectuer des achats non autorisés ou pour retirer des fonds des comptes bancaires du titulaire de carte.

Que fait Moneris[MD] pour contrer ces activités frauduleuses?

Moneris prend la fraude très au sérieux. Chez Moneris, nous travaillons en étroite collaboration avec les organismes d'application de la loi et nos partenaires de l'industrie, dont Interac[•], Visa[®] et MasterCard[†], afin d'informer les marchands de l'utilisation frauduleuse des cartes dans le but de réduire les pertes. En raison de notre formation de sensibilisation à la fraude, des présentations que nous offrons dans le cadre de colloques et de conférences et des pratiques exemplaires de l'industrie que nous diffusons, nous sommes des leaders de l'industrie. Nous fournissons du matériel didactique et les coordonnées des fournisseurs spécialisés en solutions de sécurité qui protègent les terminaux PDV.

Qui est responsable de la protection du dispositif PDV?

Les commerçants sont responsables de protéger leurs terminaux PDV. Nous recommandons de traiter tous les dispositifs PDV comme de l'argent comptant.

Pourquoi dois-je protéger mon dispositif PDV?

En protégeant voter terminal PDV, vous protégez les données de compte stockées sur la bande magnétique des cartes de paiement. L'incidence négative sur la réputation ou la marque d'un marchand (en raison de la compromission des cartes) peut être considérable et peut avoir un effet négatif sur sa rentabilité.

Comment puis-je protéger mon dispositif PDV?

Moneris recommande d'appliquer une méthode multidimensionnelle, car aucune solution unique n'est suffisante pour éviter la fraude.

Les terminaux peuvent être protégés par des câbles d'attache en acier ou des supports assujettis. En outre, nous suggérons d'utiliser des vignettes de sécurité ainsi qu'un certain nombre de pratiques exemplaires de l'industrie (p. ex. vérifications quotidiennes de l'intégrité, des numéros de série des terminaux, l'installation de caméras vidéo et l'application de pratiques d'embauche des employés).

SOLUTIONS Moneris[MD]

PROTECTION DU TERMINAL PDV

Quels sont les avantages des supports assujettis, câbles d'attache et vignettes de sécurité?

Support assujetti : Le support est fixé au comptoir et le dispositif y est verrouillé.

Câble d'attache : Le câble d'attache offre plus de souplesse, car il permet au titulaire de carte de manipuler le dispositif afin d'entrer son NIP et au personnel de ranger le terminal sous le comptoir à l'abri des regards. Lorsqu'un câble d'attache est utilisé, le terminal peut facilement être inspecté afin d'en vérifier l'intégrité et de valider le numéro de série. Si un câble était coupé durant le vol d'un dispositif, le fraudeur risque moins de rapporter le terminal altéré pour l'installer.

Vignettes de sécurité : Les vignettes de sécurité fournissent une protection supplémentaire. Elles doivent être placées sur les joints (là où se rencontrent les deux moitiés du boîtier) ou sur un point d'entrée. La coupure ou le bris d'une vignette indique que le dispositif peut avoir été altéré. Certaines vignettes sont aussi munies d'un dispositif de sécurité qui imprime « ANNULÉ » sur le terminal si la vignette a été retirée.

Que dois-je faire si mon dispositif PDV est volé?

Les commerçants doivent immédiatement signaler le vol d'un terminal PDV à Moneris et aux autorités locales.

Si je loue mes dispositifs PDV, suis-je responsable des coûts de remplacement dans le cas d'un vol?

Oui. Veuillez consulter les modalités de la convention d'affiliation de Moneris portant sur l'équipement loué auprès de Moneris.

Quel est le coût d'un support assujetti et d'un câble d'attache?

Le coût d'un support et d'un câble d'attache varie selon le fournisseur, le type de dispositif et le volume commandé.

Où puis-je acheter un support assujetti ou un câble d'attache?

Une liste des fournisseurs de dispositifs de sécurité est affichée sur notre site Web à l'adresse **moneris.com**.

Un support assujetti, un câble d'attache ou une vignette préviendront-ils le vol ou l'altération de mon dispositif PDV?

Aucune solution de sécurité n'empêchera complètement les activités frauduleuses. En protégeant votre terminal PDV, vous pouvez aider à réduire les risques de fraude. Nous recommandons d'utiliser une méthode multidimensionnelle qui comporte des solutions de sécurité physiques et des processus liés aux pratiques exemplaires.

Quels types d'activités sont suspects?

Les exemples d'activités suspectes comportent les suivants : des individus qui rôdent autour d'un terminal laissé sans surveillance, des individus qui placent de gros articles sur le comptoir pour empêcher un employé de voir le dispositif ou des individus qui s'assurent d'être les derniers clients de la journée et les premiers clients le lendemain matin (dans certains cas pour retourner des articles qu'ils ont achetés). Cette dernière technique leur permet de voler le terminal à la fin de la journée, de laisser un terminal-leurre et de rapporter le terminal altéré le lendemain.

Quels signes m'indiqueraient que mon dispositif risque d'avoir été altéré?

- Un dispositif qui comporte un numéro de série qui ne figure pas dans votre stock.
- Un dispositif qui n'est plus fixé solidement au support (vis manquantes ou lâches).
- Une vignette de sécurité qui est repliée, coupée ou qui a été retirée.
- Un câble d'attache coupé.

Comment puis-je être certain que mon dispositif a été altéré?

Seul un technicien certifié peut confirmer qu'un dispositif a été altéré.

SOLUTIONS Moneris[MD]

PROTECTION DU TERMINAL PDV

Qu'est-ce qui se produit lorsque mon dispositif est altéré?

Dans la plupart des cas, Moneris dépêchera un enquêteur sur les lieux. Ce dernier recueillera des renseignements et des preuves sur la fraude et fera des recommandations sur les façons d'améliorer la sécurité.

Mes clients apprendront-ils que leur carte de crédit ou de débit a été compromise dans mon établissement?

Moneris ne divulgue pas cette information (à moins qu'elle ne soit tenue de le faire conformément aux lois applicables). Toutefois, dans certains cas, les titulaires de carte peuvent se parler et déterminer l'établissement où la fraude a eu lieu. Dans certaines situations, la compromission a été rapportée par les médias.

Quelle est ma responsabilité en ce qui a trait à des incidents d'écrémage et à la compromission de cartes?

Le commerçant est tenu de coopérer entièrement avec Moneris (ou son représentant) durant une enquête sur l'écrémage et de faire tout en son pouvoir pour éviter que la situation ne se reproduise.

Dois-je communiquer avec la police au sujet du vol ou de l'altération de mon dispositif PDV?

Oui. Vous devez établir un rapport de police lorsqu'un terminal a été volé ou altéré.

Que dois-je faire lorsque quelqu'un veut inspecter, retirer ou effectuer une modification de mon dispositif PDV?

À part vos clients, seules les personnes autorisées peuvent avoir accès à votre terminal. Moneris communiquera toujours avec l'établissement ou le siège social avant de dépêcher un technicien sur place. Nos techniciens et nos enquêteurs auront des pièces d'identité précisant qu'ils travaillent pour Moneris. N'hésitez pas à appeler notre centre d'appels afin de vérifier que ces personnes sont bien des employés de Moneris.

Dois-je songer à remplacer mon dispositif par un terminal plus sûr?

Si vous n'avez pas remplacé votre équipement de point de vente par un terminal pouvant traiter des cartes à puce, veuillez communiquer avec notre équipe de vente au **1 866 421-1667** pour parler de vos besoins. Le rehaussement à un nouveau terminal ne préviendra pas l'écrémage. L'application d'une méthode de protection des dispositifs multidimensionnelle constitue votre meilleur moyen de défense contre les activités frauduleuses.

Les dispositifs PDV plus récents mis en œuvre par Moneris sont-ils infraudables?

Les terminaux PDV sont résistants à la fraude, mais ils ne sont pas infraudables. Les dispositifs mis en œuvre par Moneris satisfont les normes de l'industrie et sont munis de caractéristiques de sécurité permettant de contrer la fraude.

Quelles pratiques exemplaires puis-je adopter pour prévenir les activités d'écrémage?

- Informez-vous sur l'écrémage et formez votre personnel sur cette activité frauduleuse.
- Assurez-vous de connaître votre équipement de point de vente et de reconnaître toute altération.
- Veillez à avoir en tout temps la maîtrise de votre équipement de traitement des cartes de paiement.
- Assurez-vous d'utiliser une méthode multidimensionnelle de protection des dispositifs PDV.
- Installez des caméras de sécurité (capacité de stockage de 90 jours).
- Songez à installer un système d'alarme surveillé (lorsque cela s'applique).
- Établissez de bonnes pratiques d'embauche (vérifications de sécurité, du crédit et des références).

Où puis-je obtenir de plus amples renseignements sur les pratiques exemplaires de l'industrie?

Visitez **moneris.com/fraud** pour consulter la trousse d'outils d'Interac intitulée **Protect Your PinPad** et télécharger de l'information sur une initiative d'exécution de la loi intitulée **Project Protect**.

SOLUTIONS Moneris

Visitez **moneris.com/fraud** pour consulter la trousse d'outils d'Interac intitulée « Protect Your PinPad » et télécharger de l'information sur une initiative d'exécution de la loi intitulée « Project Protect ».

SOLUTIONS Moneris MD