Meilleures pratiques des commerçants pour empêcher le clonage dans les établissements de détail

Qu'est-ce que le clonage d'une carte de débit ?

Le clonage de cartes de débit est le transfert de données électroniques entre la carte de débit d'un client et une autre source à des fins frauduleuses.

Objectif

Le présent document a pour objet d'identifier et de décrire les meilleures pratiques que peuvent adopter les **gérants/employés de commerces de détail afin de** combattre le clonage des cartes de débit.

Les meilleures pratiques : pourquoi s'en préoccuper?

Le clonage de cartes de débit affecte tout le monde, les commerçants aussi bien que les clients. Il est dans l'intérêt véritable de tout le monde de prévenir le clonage de cartes de débit pour éviter de compromettre votre réputation et votre clientèle. Les meilleures pratiques décrites ici vous aideront à prévenir le clonage de cartes de débit dans votre établissement.

Meilleures pratiques

Embauche

- Obtenez toujours toute l'information sur chacun des membres de votre personnel : nom complet, date de naissance, adresse de résidence, numéro de téléphone et numéro d'assurance sociale (NAS).
- Chaque nouveau candidat doit remplir un formulaire détaillé précisant ses emplois antérieurs, son adresse à domicile et ses références. Le responsable de l'embauche devrait s'assurer que l'information fournie est véridique et exacte.
- Chaque nouveau candidat doit présenter au gérant une pièce d'identité avec photo émise par un gouvernement. Conservez une photocopie de la pièce d'identité ou prenez une photo du nouvel employé au moment de son embauche et gardez-en une copie — faites de même pour chaque nouvel employé.
- Faites une entrevue approfondie en personne avec chaque nouveau candidat. Votre entreprise peut avoir recours à des tests ou à des méthodes de sélection pour contribuer à trouver les meilleurs candidats.
- Assurez-vous d'expliquer à chaque nouvel employé que le clonage est une infraction criminelle et n'est pas toléré.

Soyez attentif! Méfiez-vous si…

- Le seul numéro de téléphone que vous donne un nouvel employé est celui de son cellulaire.
- Le nouvel employé ne peut pas soumettre de pièce d'identité avec photo.
- Le nouvel employé veut seulement travailler la nuit.

Surveillance du personnel

- Gardez pendant au moins 12 mois l'emploi du temps précis des quarts de travail du personnel, avec les changements de dernière minute.
- Exigez que chaque employé écrive son nom ou son numéro au dos de chaque justificatif de transaction.
- Faites des visites au hasard, le soir ou le week-end, quand les gérants sont habituellement absents, car c'est lors de ces périodes que se produisent la plupart du temps des clonages de cartes de débit.
- Regardez périodiquement les vidéos de surveillance, surtout quand de nouveaux employés commencent à travailler ou durant les heures de faible affluence.

Soyez attentif! Méfiez-vous si…

- Les employés semblent craindre que l'on inspecte les appareils ou s'ils ont peur de répondre à des questions sur des clients suspects.
- Les employés quittent subitement leur emploi en laissant un chèque de paye derrière eux. Avertissez immédiatement votre supérieur ou votre fournisseur de service de paiement!

Meilleures pratiques des commerçants pour empêcher le clonage dans les établissements de détail (suite)

Inspection de l'équipement et des lieux

- Faites des inspections tous les jours.
- Consultez la liste des contrôles recommandés pour connaître les techniques d'inspection étape par étape.

Soyez attentif! Méfiez-vous si…

- Quelque chose semble différent dans le plafond. Des caméras miniatures pour capter le NIP des clients peuvent avoir été installées dans les tuiles du plafond.
- Les tuiles du plafond semblent avoir été déplacées ou de nouveaux fils apparaissent derrière les tuiles.
- Les caisses enregistreuses ou les appareils pour le traitement des transactions par carte de débit ont été enlevés et/ou placés dans un endroit fixe.

Équipement

- Installez des scellés de sécurité (aussi appelés étiquettes antivol) sur tous les côtés de tout clavier, pavé numérique ou autre appareil utilisé pour le traitement des transactions par carte de débit. Si ces scellés sont enlevés ou modifiés, communiquez immédiatement avec votre acquéreur et avec la police.
- Gardez une liste exacte et à jour des numéros de série de tous les appareils et vérifiez les appareils au hasard pour vous assurer que les numéros sont les mêmes.

Autocollants « Protégez votre NIP »

Apposez les autocollants « Protégez votre NIP » sur les appareils de PDV.

Procédures à suivre avec les forces de l'ordre

- Assurez-vous de connaître les méthodes mises en place au sein de votre entreprise pour communiquer avec le service de sécurité de votre entreprise ou vos gérants de territoire.
- Établissez des contacts auprès des forces de l'ordre et au sein des services de sécurité de votre entreprise, afin de savoir avec qui communiquer si vous détectez du trafiquage.
- Coopérez avec les enquêteurs/les services de sécurité et la police lors de l'inspection des lieux, en leur fournissant les détails sur les quarts de travail, l'information sur le personnel et les vidéos des caméras de surveillance.

Communication

- Tenez-vous au courant des tendances en matière de fraude par carte de débit en lisant les mises à jour ou les bulletins de votre acquéreur et de l'Association Interac.
- Assurez-vous de connaître les méthodes applicables pour déclarer toute activité suspecte ainsi que les appareils endommagés ou trafiqués.

Signature de la liste de contrôle

Vous trouverez dans cette trousse une liste de contrôle à remplir et à signer sur les tâches à effectuer pour prévenir le clonage (inspections des appareils, surveillance du personnel) puis à soumettre à votre siège social ou à votre gérant de territoire, selon les instructions de votre gérant ou de votre siège social (Regardez la Vérification de l'intégrité du point de vente).

Engagement envers les meilleures pratiques

L'application des principes qui précèdent vous aidera à protéger votre entreprise et votre clientèle.

POUR EN SAVOIR DAVANTAGE, COMMUNIQUEZ AVEC VOTRE ACQUÉREUR OU VOTRE FOURNISSEUR DE SERVICE