CHASE Paymentech

Prevenir la fraude - Carte absente

Réduisez la fraude par carte de crédit et protégez votre entreprise des risques inutiles [1]

La fraude constitue un problème réel pour les entreprises, et le risque est accru chez les commerçants qui acceptent les transactions où la carte n'est pas présente.
Le marchandisage des commandes postales et téléphoniques a explosé, créant un secteur qui génère plus de 100 milliards de dollars par an. *Chez Chase Paymentech, nous prenons la fraude au sérieux. Nous espérons que vous lirez les stratégies de prévention de la fraude que nous décrivons dans cet article.

Il est important de commencer tôt à mettre en œuvre la prévention de la fraude et d'en faire une partie essentielle de la formation des nouveaux employés, vos employés étant dans une des meilleures positions pour avoir un effet significatif sur les pertes d'une entreprise attribuables à la fraude. Il convient de renforcer la formation sur la fraude donnée aux employés (y compris les employés saisonniers et à temps partiel), surtout à l'approche de la période des Fêtes et des saisons de pointe, lorsque le potentiel de fraude peut être plus élevé.

Voici quelques pratiques utiles de prévention de la fraude qui peuvent être suivies dans un environnement où la carte n'est pas présente (la liste n'est pas exhaustive):

1) Formation et éducation
Formez les opérateurs afin qu'ils se montrent particulièrement attentifs lorsqu'ils détectent quelque chose de suspect dans la façon dont l'appelant parle ou répond à leurs questions. Une longue pause ou des réponses hésitantes constituent d'excellents indices. Établissez une politique selon laquelle le nom de la banque émettrice de la carte de crédit doit être demandé pour n'importe quelle vente d'un montant supérieur à une valeur prédéterminée. Si l'appelant ne connaît pas le nom de la banque, cela peut indiquer qu'il utilise un numéro de carte de crédit volé.

2) Renseignements concernant la facturation et coordonnées du détenteur de la carte
Demandez toujours l'adresse de facturation du détenteur de la carte. Demandez au détenteur de la carte son numéro de téléphone le jour et le soir, « au cas où nous aurions une question ». Les commandes où l'adresse d'expédition est différente de l'adresse de facturation du détenteur de la carte peuvent comporter un signe avertisseur. Lorsque vous avez des soupçons, tentez de communiquer avec le détenteur de la carte sur une deuxième ligne téléphonique afin de vérifier la commande. Si votre système vous permet de le faire, comparez l'adresse d'expédition et l'adresse de facturation à l'adresse où le catalogue est envoyé.

3) Conservez une liste de « transactions négatives »
Élaborez et maintenez un « dossier négatif » de noms, d'adresses, de codes postaux, de numéros de carte de crédit et d'entreprises frauduleux sur lesquels vous tombez. Compilez une liste de codes postaux qui met en évidence les régions où vous avez subi un niveau de fraude élevé.

4) Examinez de plus près les cases postales
Si l'adresse est une case postale dans une grande ville, nous recommandons d'effectuer d'autres vérifications, surtout si la commande provient d'un nouveau client. Les services de distribution postale ont besoin d'une adresse municipale et n'expédieront pas de courrier à des cases postales.

5) Ne repoussez pas les commandes urgentes
Examinez attentivement une demande de commande « urgente », surtout si elle provient d'un nouveau client. Soyez particulièrement vigilant lorsque l'appelant semble prêt à commander n'importe quelle marchandise en inventaire, quels qu'en soient la couleur ou le style.

suite...

6) Examinez attentivement les commandes inhabituelles
Examinez de près toute commande d'une valeur particulièrement élevée, les demandes spéciales, ou toute commande qui sort de l'ordinaire. Voici d'autres commandes suspectes sur lesquelles les commerçants peuvent tomber et qui doivent être examinées de plus près:
• Des clients tentant d'utiliser plusieurs cartes
• Des clients tentant d'utiliser plusieurs cartes toutes émises par le même NIB (numéro d'identification bancaire)
• La demande d'un commerçant voulant appliquer une partie des fonds par virement (pour quelque raison que ce soit)

7) Que demander lorsque vous acceptez les cartes de crédit?
• Que demander lorsque vous acceptez les cartes **American Express** :
Dans le cas des clients d'American Express®, demandez le numéro CID de 4 chiffres (numéro d'identification de la carte) imprimé (pas imprimé en relief) qui figure sur le recto de la carte (sur le côté droit de toutes les cartes American Express).

• Que demander lorsque vous acceptez les cartes de crédit **MasterCard** :
Dans le cas des cartes MasterCard+, demandez le code de 3 chiffres imprimé au verso de la carte, après le numéro de la carte. Il devrait correspondre au code de validation de la carte (CVC2). Demandez également une description du caractère de sécurité, c'est-à-dire un MC stylisé et imprimé en relief sur la même ligne que les dates de validité, au recto de la carte.

• Que demander lorsque vous acceptez les cartes de crédit **Visa** :
Dans le cas des cartes Visa*, demandez le numéro non imprimé en relief qui figure au-dessus des 4 premiers chiffres. Il devrait correspondre aux 4 premiers chiffres du numéro de la carte de crédit. Demandez également à l'appelant de décrire le symbole imprimé en relief (CV pour les cartes Visa Classique, BV pour les cartes Visa Affaires et PV pour les cartes Visa Or) qui figure à droite de la date d'expiration. Demandez également que l'on vous décrive le motif du mot-symbole Visa imprimé sur toute la plage de signature.

Pour obtenir d'autres renseignements et des exemples de caractéristiques et de fonctions de sécurité spécifiques à chaque carte, vous pouvez consulter le site Web de chaque marque de carte :

American Express: www.americanexpress.com/canada/fr/merchants/2-4_fraud-f.shtml
MasterCard: www.mastercard.com/ca/merchant/security/mc_web_French/home.html
Visa : www.visa.ca/fr/merchant/prevention-de-la-fraude/caracteristiques-de-securite/

8) Vérifiez l'appelant
Vous pouvez peut-être utiliser l'identification automatique du numéro (ANI). Vérifiez que le numéro de téléphone qui vous est retourné correspond à celui qui vous est fourni par l'appelant..

Outils et ressources supplémentaires : service de vérification de l'adresse et codes de sécurité des cartes
Les outils fournis par les associations de cartes peuvent aider à vérifier l'identité du détenteur de la carte en temps réel et offrent aux propriétaires d'entreprise quelques mesures de sécurité supplémentaires. Cependant, celles-ci ne permettent quand même pas d'éliminer complètement la fraude et les rétrofacturations.

Authentification des cartes de crédit
Ce processus d'authentification vérifie que le détenteur de la carte est bien propriétaire du compte lors d'une transaction en ligne. Les services tels que Vérifié par Visa® (VpV) et MasterCard SecureCodeMC peuvent aider les commerçants qui acceptent les transactions où la carte n'est pas présente en ajoutant une autre mesure de validation lors de l'évaluation de la légitimité d'une transaction.

Lorsqu'un détenteur de carte effectue un achat sur un site VpV ou SecureCode participant, le processus d'achat reste le même jusqu'à ce qu'il clique sur le bouton « Acheter ». Si la carte bancaire est enregistrée auprès d'un émetteur participant, le mot de passe de VpV ou les coordonnées d'accès SecureCode spécifiques à l'émetteur seront demandés au consommateur. Grâce à ce processus de commande simple, l'émetteur de la carte peut confirmer l'identité du détenteur de la carte en temps réel.

Les commerçants doivent installer un module logiciel (appelé module d'extension du commerçant) ou développer leur propre logiciel compatible avec VpV et SecureCode. Cela permet aux commerçants de transférer les données d'identification du détenteur de la carte aux serveurs d'enregistrement des cartes et d'en recevoir des réponses. Les commerçants doivent capter et envoyer les données d'autorisation à Chase Paymentech.

Service de vérification de l'adresse (SVA)
Le SVA peut contribuer à réduire le risque d'acceptation de transactions frauduleuses en vérifiant l'adresse de facturation du détenteur de la carte, qui figure dans les dossiers de l'émetteur de la carte. Le SVA compare l'adresse de facturation que vous donne un client à l'adresse de facturation qui figure dans les dossiers de la banque émettrice de la carte de crédit. Visa, MasterCard et American Express proposent des fonctions de SVA semblables.

• Le SVA n'est qu'un outil de prévention de la fraude. Il est d'une efficacité maximale lorsque vous l'utilisez concurremment avec d'autres pratiques de détection de la fraude.

• L'incidence de fraude est généralement plus grande lorsque le SVA ne retourne pas de correspondance et lorsque le montant de la commande est élevé, lorsque l'appelant demande une livraison le lendemain à une adresse située dans un quartier où le risque de fraude est élevé, ou lorsque l'adresse de facturation est différente de l'adresse d'expédition.

Vérification de la sécurité de la carte
L'outil carte-non-présente compare le code de sécurité de la carte (le code numérique de trois ou quatre chiffres non imprimé en relief qui figure sur la carte de crédit) avec le code qui figure dans les dossiers de l'émetteur. Ces codes sont les trois chiffres imprimés dans la plage de signature au verso des cartes Visa ou MasterCard ou les quatre chiffres imprimés au recto des cartes American Express.

Les programmes de vérification des cartes de crédit sont offerts par les principales associations de cartes, et sont connus sous le nom de CVV2 (Visa), de CVC2 (MasterCard) et de DIC (American Express). Bon nombre de solutions de traitement pour les cartes non présentes permettent la validation des codes de sécurité des cartes et les demanderont lors des transactions.

- Si le client ne peut pas fournir le code de sécurité de la carte qui figure au recto ou au verso de la carte physique, cela indique que la carte n'est pas présente et que le numéro de carte a pu être volé.

- Si le client fournit le code de sécurité de la carte mais si celui-ci ne correspond pas au code qui figure dans les dossiers de l'émetteur, vous recevrez une réponse indiquant qu'il n'y avait pas de correspondance. Vous pouvez demander au client de confirmer le code, car il est possible qu'il se soit trompé en vous le donnant. S'il ne correspond toujours pas, vous devriez refuser la transaction.

Soyez toujours observateur

Vous pouvez réduire considérablement la fraude attribuable aux cartes de crédit en prenant des mesures directes et en mettant en œuvre des protocoles visant à contrer les activités potentiellement frauduleuses. Souvent, une attention accrue et une approche proactive contribuent à protéger votre entreprise contre les activités frauduleuses.

Soyez sensible à la fraude interne

Le vol effectué par les employés existe et peut affecter votre entreprise. Un type de fraude qui est unique aux agents de vente directe est le détournement de remboursements vers la carte de crédit d'un fraudeur. Les entreprises doivent surveiller les différences entre la carte de crédit utilisée pour commander et celle à laquelle un remboursement ultérieur est porté. Soyez également à l'affût d'employés qui achètent des marchandises et qui les portent au compte de la carte de crédit d'un client. De plus, il existe d'autres mesures que vous pouvez prendre pour protéger votre entreprise :

- Surveillez vos employés;
- Protégez les numéros de carte de crédit;
- Effectuez le rapprochement de vos fonds tous les jours.

Ce qu'il faut retenir

Les propriétaires d'entreprise doivent se montrer proactifs afin de minimiser leur responsabilité face à la fraude. La chose la plus importante qu'il faut retenir de ces stratégies de prévention de la fraude, c'est que les propriétaires d'entreprise doivent se renseigner et former leur personnel afin de contribuer à protéger leur entreprise et leurs clients.

Il existe un grand nombre de stratégies et d'outils de prévention de la fraude qui sont disponibles aux entreprises et qui fournissent des renseignements précieux pour aider à mettre à jour les protocoles de gestion des risques et de prévention de la fraude.

Pour de plus amples renseignements, rendez-vous à l'adresse **www.chasepaymentech.ca**