



Délits liés aux cartes de paiement

Les institutions financières canadiennes ont signalé des pertes de près d'un milliard de dollars au cours des deux dernières années. Bien que les consommateurs canadiens ne subissent pas de pertes financières directes, au bout du compte, les pertes sont récupérées par une augmentation des frais administrés par les institutions financières. Les consommateurs peuvent également voir leur compte gelé en raison de retards dans les paiements de factures et même perdre confiance envers le système bancaire.

L'Association des banquiers canadiens (ABC) a créé les catégories suivantes en ce qui concerne l'utilisation des cartes de paiements à des fins criminelles :

- Utilisation de cartes contrefaites : il s'agit de la catégorie la plus importante de fraude par carte de crédit; les organisations criminelles se sont dotées de la technologie qui leur permet de copier les données figurant sur la bande magnétique, de fabriquer de fausses cartes et de contourner les mesures de protection comme les hologrammes.
- Le détenteur perd sa carte ou se la fait voler : habituellement, les cartes sont volées sur les lieux de travail ou dans les véhicules, les centres de santé, les clubs de golf, etc.
- Fraude commise sans l'utilisation de la carte : fraude sans carte.
- Fraude liée à des cartes non reçues par leurs détenteurs (fraude liée à des envois non reçus) : la fraude concerne des cartes interceptées avant que leurs détenteurs les aient reçues.
- Cartes obtenues frauduleusement par des criminels qui présentent de fausses demandes : l'identité de personnes solvables est usurpée afin d'obtenir des cartes de crédit.

Fraude sans carte

La fraude sans carte constitue une des fraudes par carte de paiement qui connaît la plus forte augmentation dans de nombreuses régions du monde à l'heure actuelle. En 2011, l'ABC a révélé que les pertes liées à la fraude sans carte se chiffraient à 259 498 535 \$, une augmentation de 47,35 % par rapport à 2010.

Par fraude sans carte, on entend la collecte, l'échange et l'utilisation non autorisés ou frauduleux des données de cartes de paiement dans des situations où la carte et le détenteur de la carte ne sont pas présents.

Les courriels constituent l'une des méthodes les moins sécuritaires pour effectuer des commandes par carte de paiement. Les commerçants canadiens victimes de fraude sans carte sont principalement sollicités par courriel, ainsi que dans une moindre mesure sur les sites Web de commerce électronique, par téléphone, par télécopieur, en personne et par la poste. Cela signifie que de nombreux commerçants canadiens ne sont pas au courant des protocoles de protection contre la fraude ou bien ils ne les suivent pas.

Dans la variante du paiement excédentaire, les suspects utilisent habituellement des cartes de crédit falsifiées pour acheter un produit à un prix supérieur au prix de vente normal. La sélection des cibles se fait généralement en ligne sur un site de vente aux enchères ou de petites annonces. Le fraudeur demande à la victime de lui retourner le montant excédentaire. Le consommateur et le vendeur doivent rembourser de leur poche le montant excédentaire envoyé et peuvent perdre la marchandise si elle a déjà été expédiée.

Dans une autre variante, les fraudeurs achètent des produits, comme des billets d'avion, à l'aide des données figurant sur des cartes de crédit volées, puis ils revendent le produit en l'annonçant à un prix réduit, habituellement sur un site Web ou un site de petites annonces. Non seulement les commerçants perdent le produit volé, mais ils doivent souvent rembourser les fonds aux institutions financières.

Comment se protéger?

En prenant les mesures de sécurité suivantes, vous pouvez réduire au minimum la fréquence des transactions frauduleuses ciblant votre entreprise de façon à ce que vos clients puissent effectuer des transactions en ligne, par la poste et par téléphone en toute confiance :

- Avant d'expédier les biens, appelez le client au numéro qu'il vous a donné et vérifiez les renseignements relatifs à la transaction. Souvent, les fraudeurs sont incapables de vérifier les renseignements fournis puisqu'ils font des commandes aléatoires et ne tiennent pas une liste de ce qu'ils ont demandé.
- Soyez attentif aux expéditions prioritaires de biens faciles à falsifier, il pourrait s'agir de transactions frauduleuses.
- Méfiez-vous des commandes faites au nom de clients connus, mais qui diffèrent de leurs habitudes d'achat.
- Utilisez les services de vérification d'adresse et de code de sécurité (CVC 2) des compagnies émettrices de cartes de crédit (MasterCard et Visa).
- Protégez les transactions en ligne à l'aide des protocoles de sécurité « MasterCard SecureCode » et « Vérifié par Visa ».
- Visa offre différents protocoles de prévention que les commerçants peuvent utiliser pour prévenir la fraude sans carte. Cliquez sur les liens suivants pour les consulter :

<http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf>

http://usa.visa.com/merchants/risk_management/card_not_present.html

Si vous croyez être victime ou si vous connaissez une personne qui a été victime de fraude, veuillez communiquer avec le Centre antifraude du Canada au 1-888-495-8501 ou vous rendre au www.antifraudcentre.ca. **LA FRAUDE : Identifiez-la, signalez-la, enravez-la.**