AIDE-MÉMOIRE

Protéger son terminal de paiement

Objectif du document

Aider les commerçants à se protéger des risques liés à la fraude et à offrir à leurs clients un environnement plus sûr. Pour votre sécurité et celle de vos clients, il est important de respecter les règles qui guident les transactions, et ce, qu'elles soient complétées en personne, en ligne, au téléphone ou par la poste.

Le document présente les bonnes pratiques à adopter pour prévenir la fraude.

Destinataire du document : Commerçants

Date de la dernière modification : juin 2018

Comment se protéger de la fraude?

Les meilleures pratiques à adopter pour tous les commerçants

- Prenez la carte du client en main; sa vérification relève de votre responsabilité.
- Veillez à ce que tous vos employés soient formés sur l'utilisation d'un terminal de paiement, qu'ils connaissent les méthodes d'acceptation des cartes et qu'ils priorisent la lecture de la puce. Cette technologie est très fiable; si la lecture d'une puce ne fonctionne pas, cela devrait éveiller la méfiance.
- Assurez-vous que la carte de crédit comporte ces caractéristiques de sécurité: impression en relief, répétition des 4 premiers chiffres imprimés sur la carte, code de sécurité (3 ou 4 chiffres) imprimé sur la carte.
- Comparez la signature qui se trouve au verso de la carte de crédit à celle sur le reçu lorsqu'une carte de crédit est glissée ou entrée manuellement.
- Comparez les 4 premiers et 4 derniers chiffres imprimés en relief sur la carte à ceux imprimés sur le reçu lorsque la lecture de la carte s'effectue par la bande magnétique.
- Ne remettez **JAMAIS** d'argent lors d'un achat payé par carte de crédit. Cette pratique est interdite. Seules les transactions avec les cartes de débit permettent les remises en argent.
- Modifiez périodiquement le numéro d'identification personnel (NIP) administrateur de votre terminal de paiement à l'aide du guide d'utilisateur. Le NIP administratif permet d'accéder aux fonctions restreintes telles que l'annulation et le remboursement des transactions.
- Ne jamais accepter de remboursement sur une carte autre que la carte de l'achat originale.
- Lors de transactions en ligne, vous pouvez toujours contacter l'émetteur afin de faire une vérification nom et adresse.

Commandes téléphoniques ou postales

Informations à demander :

- Le code de sécurité (3 ou 4 chiffres) imprimé sur la carte;
- Le nom du détenteur, tel qu'il apparait sur la carte;
- La date d'expiration, telle qu'elle apparait sur la carte;
- L'adresse de réception du compte de la carte;
- Les numéros de téléphone (domicile et cellulaire) du détenteur;
- Une signature au moment de la réception de la commande, si possible.

Paiements en ligne

Optez pour les options de sécurité telles que :

- La vérification du SVA, soit l'adresse de réception du compte de la carte;
- La vérification du code de sécurité (3 ou 4 chiffres) imprimé sur la carte;
- Les options de vérification telles que Vérifié par Visa et MasterCard SecureCode;
- La vérification de la carte dans une base de données négatives;
- La vérification de la date d'expiration et du nom du détenteur.

Astuces pour prévenir la fraude

5 conseils pour prévenir la fraude :

1. **Remise du terminal.** Remettez le terminal au client UNIQUEMENT après avoir saisi et confirmé le montant de la transaction.

2. **Observation du client.** Observez le client lorsqu'il manipule le terminal afin d'éviter qu'il n'entre des informations manuellement.

3. **Carte à puce.** Assurez-vous que la transaction s'effectue avec la puce et non avec la bande magnétique.

4. **Remboursement.** Prévenez les risques de fraudes liés aux remboursements sur cartes de débit et crédit, en choisissant un NIP Administrateur sur votre terminal.

5. **NIP Administrateur.** Modifiez régulièrement votre NIP Administrateur sur le terminal et ne le communiquez qu'à votre personnel de confiance.

Indices de détection de fraude

Rester vigilant lorsque :

- Une commande vous **semble suspecte. Téléphonez au client pour la confirmer de vive voix;** les fraudeurs utilisent souvent de faux numéros de téléphone.
- La **même carte de crédit est utilisée** pour de nombreuses commandes dans un court laps de temps.
- **Plusieurs commandes livrées à une même adresse** sont effectuées dans une courte période.
- **L'adresse IP du client ne correspond pas au pays émetteur** de la carte de crédit ou provient d'un pays jugé à haut risque.
- Un client passe une **commande extrêmement coûteuse** ou achète un **produit en très grande quantité.**

Comment bien protéger son terminal ?

Terminaux en magasin	Terminaux mobile
Fixez **votre terminal à un support spécialement conçu pour décourager le vol ou le vandalisme.**	**Fixez,** si possible, votre tablette ou votre téléphone intelligent à un support.
Ayez toujours votre terminal à l'œil, **car les fraudeurs travaillent souvent en équipe; pendant qu'un crée une distraction, l'autre en profite pour modifier le terminal.**	**Ne laissez jamais votre appareil sans surveillance.**
Restez à proximité **de votre client quand vous lui remettez le terminal à la table pour le paiement.**	Conservez votre terminal dans un **endroit sécuritaire** ; ne le laissez jamais à la vue dans votre voiture.
Rangez **les terminaux sous le comptoir ou dans un lieu sécurisé avant de fermer le commerce.**	

Vous soupçonnez un cas de fraude ?

Mesures à prendre en cas de soupçon de fraude :

- Prenez la carte du client et vérifiez les caractéristiques de sécurité.
- Assurez-vous que les quatre derniers chiffres de la carte correspondent aux quatre chiffres imprimés sur le relevé de transaction du terminal.
- Demandez deux pièces d'identité avec photo au détenteur afin de l'identifier et de vérifier sa signature, le cas échéant. Sachez toutefois que vous ne pouvez noter de l'information personnelle qui le concerne.
- Contactez le fournisseur de votre terminal de paiement pour connaître la marche à suivre en cas de fraude