

Transactions suspectes et meilleures pratiques relatives à la prévention des fraudes



Le présent document fournit aux détaillants des renseignements importants sur les tendances en matière de fraude dans le secteur des produits prépayés. Il explique comment reconnaître les transactions suspectes et prévenir la fraude

AVIS AUX DÉTAILLANTS : ALERTE DE FRAUDE

Certains détaillants ont reçu des appels téléphoniques de personnes prétendant appeler de la part de Now Prepay, d'Ezipin, de Payment Source, de votre siège social ou d'un des fournisseurs de produits ou cartes-cadeaux. Cette personne demande au détaillant d'activer un produit ou d'imprimer un NIP afin de corriger une défaillance du système ou de tester la fonctionnalité du terminal. Elle demande au détaillant de divulguer le NIP ou le numéro de carte et lui précise que le NIP et la transaction seront immédiatement annulés.

C'EST UNE ACTIVITÉ FRAUDULEUSE!

Rappelez à votre personnel de ne jamais imprimer de NIP ni activer de carte en réponse à une demande téléphonique.

Comment savoir à qui vous avez affaire :



Les employés de Now Prepay :

- Demandent le numéro de transaction pour répondre aux demandes de renseignements sur les produits
- Utilisent la carte de test fournie dans votre trousse de bienvenue pour effectuer des tests et corriger les problèmes
- Ne vous demandent jamais d'imprimer des produits actifs de quelque type que ce soit



Les fraudeurs :

- Vous demandent d'imprimer ou d'activer des produits
- Vous demandent de divulguer le NIP ou le numéro de carte
- Essaient d'acheter un produit au téléphone en se servant de cartes de crédit volées

RAPPEL:

N'utilisez que la carte de test pour tester votre terminal et donner de la formation!

VOUS NE SAVEZ PAS QUI APPELLE?

Raccrochez et appelez le service de soutien à la clientèle, au **1-800-253-2111**, pour confirmer que vous faites affaire avec un de nos représentants.

COMMENT PRÉVENIR LA FRAUDE?

- Formez votre personnel! La connaissance est la clé de la prévention des fraudes.
- Acceptez les paiements en personne; jamais par téléphone.
- Obtenez le paiement avant de conclure la transaction.
- Si le client paie avec une carte de crédit, n'hésitez pas à lui demander une pièce d'identité afin de vérifier si le nom sur la carte correspond à celui sur la pièce d'identité, surtout dans le cas d'une transaction traitée par SWIPE.
- Ne remettez pas la carte activée ou le bon de transaction du produit au client avant la confirmation du paiementbeen confirmed

COMMENT DÉTECTER LES TRANSACTIONS SUSPECTES

Soyez attentif aux indices suivants :

- Le client présente plusieurs cartes de crédit ou de débit, qui sont toutes refusées.
- Le client présente une carte de crédit ou de débit qui semble modifiée.
- Le client achète des produits d'épicerie en très petite quantité ou qui semblent choisis au hasard, ainsi qu'une grande quantité de cartes-cadeaux.
- Le client achète un produit coûteux, comme des cartouches de cigarettes, ainsi qu'une grande quantité de cartes-cadeaux.
- Le client pousse le caissier à vite conclure la transaction en utilisant la rudesse ou d'autres moyens de distraction, surtout durant les périodes achalandées de la journée ou à des heures inhabituelles. Les fraudeurs ciblent les magasins durant leurs périodes les plus achalandées ou entre minuit et cinq heures du matin.
- Le client doit se rendre à sa voiture pour pouvoir régler son achat.
- Le client semble contraint d'effectuer la transaction ou anxieux de la conclure.
- Le client est agressant et semble croire qu'il a droit à plus que les limites permises dans votre magasin, ou à une valeur de produit ou de carte-cadeau plus grande que ce qui est offert.
- Le client prétend qu'il fait un paiement à un assureur, à l'Agence du revenu du Canada, à un rançongiciel, à un logiciel malveillant ou à un nettoyeur de virus... ou qu'il envoie de l'argent à des êtres chers... ou il vous monte tout autre canular couramment utilisé.
- Dans de telles situations, il vaut mieux suggérer au client de se rendre sur le site Web du Centre antifraude de la GRC pour obtenir plus d'information.

Si une de ces situations, ou toute autre activité suspecte, se produit, dès que le client quitte les lieux, communiquez immédiatement avec le soutien à la clientèle de Now Prepay pour signaler l'incident, la raison de vos soupçons et tout autre détail susceptible de nous aider dans notre enquête.

LUTTE CONTRE LE BLANCHIMENT D'ARGENT

- Surveillez tout client qui vient régulièrement acheter de grandes quantités de produits financiers prépayés et qui paie seulement en argent comptant. L'argent est souvent blanchi de cette manière. Si vous croyez que c'est le cas, demandez au client à quoi sert le produit et notez-le au cas où nous vous contacterions pour obtenir plus d'information.
- Si une activité suspecte (mentionnée ou non dans la liste précédente) se déroule dans votre magasin, signalez-la immédiatement à votre équipe de prévention des pertes ou à toute autre ressource identifiée dans la politique de lutte contre le blanchiment d'argent de l'entreprise. Si vous ignorez le contenu de cette politique ou que vous n'avez pas une telle politique en place, communiquez avec notre équipe de soutien pour savoir qui contacter ou simplement nous signaler l'activité suspecte.

EST-CE QUE L'UN DE VOS CLIENTS OU VOUS-MÊME ÊTES VICTIME D'UNE FRAUDE?

Les victimes doivent signaler la fraude au Centre antifraude du Canada:

En ligne: <http://www.antifraudcentre-centreantifraude.ca/index-fra.htm>

Par téléphone, sans frais : 1-888-495-8501

SOYEZ VIGILANTS!!!



NOUS SOMMES LÀ POUR VOUS PROTÉGER!

visitez notre page web *alertes de fraude et conseils* pour rester au courant des plus récentes alertes à la fraude et escroqueries.