LIGNES DIRECTRICES RECOMMANDÉES POUR LA SURVEILLANCE DE LA FRAUDE À L'INTENTION DES MARCHANDS DU COMMERCE ÉLECTRONIQUE

En tant que commerçant du e-Commerce, être victime de fraude peut avoir une gamme variée d'effets sur votre entreprise.
Ces effets comprennent:

- Perte financière due aux stocks / bénéfices volés
- Réputation endommagée
- Perte de confiance des clients
- Perte de confiance des investisseurs
- Réduction des ventes
- Coûts supplémentaires de temps / d'argent pour gérer chaque incident de fraude
- Frais juridiques possibles
- Valeur réduite de votre stock / de vos services
- Frais bancaires supplémentaires pour le renversement de transaction
- Problèmes potentiels liés à votre compte bancaire après plusieurs transactions inversées

FRAUDE DE CARTE DE CRÉDIT

Le vol de biens et de services via les cartes de crédit est la forme la plus courante de fraudes en ligne à prendre en compte et les marchands en ligne sont particulièrement vulnérables. Parce qu'il est peu probable que vous rencontriez vos clients face à face, il est difficile de savoir si le paiement par carte de crédit que vous avez accepté est vraiment valide. Si ce n'est pas le cas, vous risquez de perdre la fois et le produit et le paiement. Et tandis que les titulaires des cartes de crédit ont généralement une responsabilité limitée, les commerçants quant à eux, assument le coût total d'une transaction frauduleuse en plus des frais connexes.

CE QU'IL FAUDRAIT PRENDRE EN CONSIDERATION

Il est important de surveiller les signes communs de fraude. Bien que les circonstances ci-dessous s'appliquent souvent aux clients honnêtes, elles peuvent aussi être des indicateurs d'activités illégales.

Faites particulièrement attention aux commandes qui sont :

- Démesurément grandes,
- Livrées à une adresse qui n'est pas l'adresse de facturation,
- Livrées dans des pays où vous ne livrez pas d'habitude (en particulier dans les zones à haut risque),
- Composées de plusieurs articles identiques,
- Dans l'impossibilité de passer un processus de vérification d'adresse,
- Hors de l'ordinaire de quelque manière que ce soit.

Faites particulièrement attention aux clients qui :

- Utilisent une adresse courriel anonyme / gratuite (comme hotmail.com) et surtout avec des noms comme john123@hotmail.com ou jane2000@yahoo.com,
- Fournissent une adresse de site Web inexistante ou sous-construction,
- Utilisent un numéro de téléphone déconnecté ou modifié,
- Fournissent une adresse physique simulée (telle que 1234 Side Street) ou seulement un numéro de boîte postale,
- Insistent que vous leur livriez le plus rapidement possible peu importe le prix,
- Se soustraient aux vérifications de crédit ou d'identité,
- N'effectuent pas de paiement intégral dans l'immédiat,
- Achètent pour leur première fois mais qui effectuent de grandes transactions.

Faites particulièrement attention aux numéros de cartes de crédit qui :

- Génèrent des commandes multiples sur une courte durée, surtout si chaque commande est envoyée à une adresse différente,
- Représentent l'un des numéros de cartes de plusieurs envoient à la même adresse.

REGIONS A HAUT RISQUE POUR LA FRAUDE EN LIGNE

Les pays / états figurant sur la liste suivante sont considérés comme des régions où les risques sont élevés pour la fraude en ligne, mais toutes les commandes venant de ces zones ne seront pas forcément frauduleuses. Et rappelez-vous: une transaction n'est pas sécurisée simplement parce que son pays de provenance n'est pas considéré comme étant une zone haut risque.

Amsterdam en Hollande	Russie
Belgique	Malmö en Suède
Bulgarie	Nigeria
Chine	Pakistan
Europe de l'Est	Palestine
Egypte	Roumanie
Ghana	Asie du Sud-Ouest
Indonésie	Turquie
Israël	Ukraine
Lituanie	Malaisie

Il est hautement recommandé d'examiner les commandes de ces zones avec plus de prudence.

MESURES PRÉVENTIVES

Vous ne voulez pas effrayer les clients avec trop de paperasserie, mais vous voulez protéger votre entreprise en établissant des mesures de prévention de fraude de base. Il y a beaucoup de choses à faire, mais assurez-vous de maintenir un équilibre entre garder votre entreprise en sécurité et la rendre agréable à la clientèle.
Et n'oubliez pas - aucune technique ne mettra votre entreprise à l'abri de la fraude.

LIVRAISON

- Utiliser une assurance postale,
- Utiliser les services de suivi des colis,
- Utilisez un courrier de confiance qui requiert la signature du destinataire lors de la livraison,
- Suspendez la livraison si vous suspectez la fraude,
- N'offrez pas de livraison dans les zones à haut risque,
- N'envoyez pas de commande jusqu'à ce que l'identité et la vérification des paiements supplémentaires soient terminées.

COMMANDES

- Validez tous les détails de chaque commande,
- Gardez un registre des statistiques des commandes afin que vous puissiez créer une image des commandes typiques,
- Si vous avez identifié des modèles de fraude, assurez-vous de déclencher une alarme lorsqu'une commande correspond au modèle de fraude.

VOS CLIENTS

- Assurez-vous que vos clients existent réellement,
- Gardez un registre sur les clients ayant de bons antécédents d'achat et sur ceux avec lesquels vous avez eu des problèmes,
- Utilisez un moyen comme AVS (Système de vérification d'adresse) pour vous assurer que l'adresse du client physique est valide,
- Assurez-vous que les adresses de facturation et d'expédition sont valides, surtout si elles sont différentes,
- Tenir des registres de tout contact que vous avez avec les clients,
- Utilisez un moyen tel que les annuaires téléphoniques en ligne pour vérifier qu'un numéro de téléphone fourni est valide,
- Assurez-vous que les adresses courriel ou Web sont valides et sécurisées,
- Prenez du temps pour vérifier les commandes de vos clients,
- Indiquez clairement à tous les clients que les commandes et les paiements devront être authentifiés avant toute livraison,
- Informez les clients que leurs informations de transaction et leur numéro IP (adresse Internet) seront enregistrés,
- Gardez un registre des achats des clients pour établir leur préférence.

CARTES DE CREDIT

- En cas de doute, demandez une copie indépendante de la signature du client,
- Demandez au client de faxer la face de sa carte de crédit,
- Conservez un registre des numéros de carte de crédit qui vous ont posé des problèmes dans le passé ou qui ont éveillé vos soupçons,
- Chercher à connaitre la banque émettrice de la carte et le pays d'origine et assurez-vous qu'elles sont conformes aux informations que vous a fourni le client,
- Utilisez un moyen tel que CVV2, Secure Code ou CID (selon le fournisseur de la carte de crédit) pour vous assurer que les informations de la carte n'ont pas été volées,
- Appeler la banque émettrice et vérifier les détails du client.

QUE FAIRE SI VOUS SUSPECTEZ UNE OPERATION DE FRAUDE

Il y a certaines choses que vous devriez faire dès que vous êtes convaincu avoir été victime de fraude. Bien qu'il puisse s'avérer difficile de récupérer des biens perdus ou des gains, vous pouvez prendre des mesures et, espérons-le, contester un rejet de débit.

- Enregistrez toutes les circonstances liées à la fraude - les détails de la commande, les informations du client, les dates, les heures, etc.
- Si la fraude implique une carte de crédit volée, contactez le détenteur légitime de la carte si possible et alertez-le à propos,
- Contacter immédiatement eLipa S.A. avec des détails sur la fraude,
- Si vous pensez avoir reçu de l'argent d'une transaction impliquant une carte de crédit volée, consultez eLipa S.A pour savoir comment rembourser l'argent au titulaire de la carte,
- Contactez la police ou les autorités locales compétentes pour signaler la fraude.

CONCLUSION

Si vous mettez les mesures préventives appropriées en place et que vous avez des systèmes qui vérifient les transactions en cas de fraude, vous pouvez minimiser le risque.

Il vous faut toujours contacter eLipa S.A., devant les situations où vous ne savez pas quoi faire.