Conseils de sécurité pour Mail-/Phone-Order

L'utilisation frauduleuse de numéros de cartes dans le commerce à distance occasionne chaque année des dommages considérables, auxquels viennent s'ajouter d'importantes charges administratives. Nous avons rédigé la présente notice d'information pour vous aider à mieux vous protéger des abus.

Les escrocs agissent fréquemment de la même façon :

- Une grosse commande est passée par fax, e-mail ou telephone. La marchandise doit être livrée par exprès ou par l'intermédiaire d'un service de transports de colis, les frais étant à la charge du commettant. L'adresse de livraison se trouve la plupart du temps à l'étranger. Souvent il s'agit d'un hôtel ou bien d'une poste restante.
- Très souvent, le paiement est effectué au moyen de plusieurs cartes.

Conformément aux conditions contractuelles régissant le commerce à distance, vous avez l'obligation de demander une autorisation pour toutes les transactions de cette nature. Toutefois, la procédure d'autorisation ne fait que confirmer la validité de la carte et la solvabilité du titulaire de carte au moment de la transaction.

Il n'est pas possible de déterminer à coup sûr si le commettant est bien le titulaire légitime de la carte ou si une autre personne utilise sa carte et ses données pour passer une commande frauduleuse.

Raison pour laquelle les entreprises de cartes déclinent toute responsabilité quant aux commandes réalisées par fax ou par téléphone.

LES RISQUES SONT À VOTRE CHARGE

Tandis que les escrocs prennent livraison de la marchandise, les titulaires légitimes des cartes concernées contestent les débits. Il s'agit là d'une situation très désagréable pour le partenaire affilié lésé : il doit non seulement déplorer la perte des marchandises, mais aussi restituer le montant total de la transaction.

Quelques conseils à suivre afin de réduire vos risques :

1. ACCEPTATION DES CARTES

Conformément au contrat d'acceptation de cartes, seules les commandes passées par fax, téléphone ou par l'intermédiaire d'une boutique en ligne sont autorisées. Si vous obtenez des commandes par e-mail comportant des données de cartes, veuillez informer l'expéditeur que ce type de commande est interdit.

Supprimez le numéro de carte de l'e-mail avant d'envoyer votre réponse. Imprimez l'e-mail et supprimez le de votre « Boîte de réception » ainsi que du dossier « Corbeille ».

2. DONNÉES DE CARTES PRÉSENTES PHYSIQUEMENT

Assurez-vous que les documents papier contenant des numéros complets de cartes ne restent jamais sans surveillance et veuillez à ne surtout pas les jeter à la poubelle.

Détruisez ces documents à l'aide d'un broyeur afin qu'il soit impossible de reconstituer les informations.

3. TRANSFERT DE NUMÉROS DE CARTES

Avant de procéder au transfert d'un numéro de carte, soyez sûr(e) que le bénéficiaire ait impérativement besoin du numéro complet de celle-ci. Si tel n'est pas le cas, veuillez plutôt envoyer le numéro de carte de la façon suivante : xxxx xxxx xxxx 1234. Le numéro de carte ainsi représenté porte le nom de troncature du PAN (« PAN truncation » en anglais).

Renoncez catégoriquement à transmettre des numéros de cartes par e-mail. Communiquez les données de cartes par téléphone ou fax.

4. COMMANDES SUR INTERNET

Nous conseillons aux exploitants de boutiques en ligne de recourir à une solution de sécurité 3-D Secure 2 (p. ex. « Visa Secure » ou « Mastercard Identity Check »). Cette procédure permet de réduire considérablement le risque de fraude, ainsi la responsabilité en cas de fraude revient à l'émetteur de cartes.

Si vous utilisez votre propre bon de commande, assurez-vous qu'il soit conforme aux normes PPI DSS (à savoir pas de requête du code CVC2/CVV2). Vérifiez également le processus de commande pour la transmission et, le cas échéant, le stockage (temporaire) des données de carte.Nous vous recommandons d'intégrer notre solution Pay-per-Link Secure PayGate qui offre une alternative sécurisée pour le traitement de vos commandes par fax, e-mail ou téléphone. Quelques ajustements mineurs suffisent pour obtenir des formulaires de carte conformes aux normes PCI et ainsi de bénéficier des avantages 3-D Secure 2.

5. VÉRIFICATION DE LA COMMANDE

Soyez prudent lors de commandes de quantités et de montants bizarrement élevés, d'un rythme de commande rapide ou d'adresses e-mail de fournisseurs gratuits tels que yahoo.com, gmx.com ou hotmail.com.

6. VÉRIFICATION DE L'ADRESSE DE LIVRAISON

Vérifiez bien soigneusement l'adresse de livraison si celle-ci est différente de l'adresse de facturation de l'acheteur.

Nous vous déconseillons instamment d'effectuer des envois vers des pays en voie de développement, et notamment vers l'Afrique, l'Extrême-Orient ou l'Amérique du Sud, ainsi que vers les pays de l'ex-CEI, à moins bien sûr que vous n'entreteniez des relations d'affaires avec un partenaire connu et bien établi dans le pays.

Soyez en outre prudent lors de livraisons à une adresse de boîte postale ou un hôtel.

7. EVALUER LES RISQUES

Accepteriez-vous également de livrer la marchandise sur facture ? Les cartes de crédit et de débit (comme Maestro) sont des moyens de paiement fort pratiques mais ne constituent en aucun cas des instruments d'encaissement.

Personne ne connaît mieux que vous le déroulement ordinaire de vos opérations commerciales. Si vous avez des doutes mais que vous désirez néanmoins accepter la commande, nous vous conseillons de consulter votre banque attitrée concernant une garantie contre les risques d'exportation.

Les coordonnées de votre interlocuteur local sont disponibles sous : worldline.com/merchant-services/contacts

110.0345.03 AX BEL_FR/10.2021