J'ai subi un piratage et les coordonnées de ma carte bancaire ont été utilisées frauduleusement par un tiers

Depuis le début du confinement, les paiements par carte bancaire ont été plus nombreux. En même temps, des commerçants ont développé la vente en ligne, parfois dans l'urgence, en déployant des sites marchands pas toujours très bien sécurisés.

Les origines possibles de la fraude sont nombreuses et pas toujours identifiables : elle peut provenir le plus souvent

- D'un hameçonnage, c'est-à-dire un message incitant à fournir vos coordonnées,
- Du piratage d'un compte en ligne sur lequel les coordonnées de la carte bancaire seraient enregistrées,
- Du piratage de votre équipement informatique,
- Du piégeage d'un distributeur de billets
- D'un paiement chez un commerçant malhonnête qui aurait pu capter les données de votre carte.
- D'une escroquerie par téléphone

Quels sont vos recours en cas d'utilisation frauduleuse de votre carte bancaire ?

La première chose est de vérifier régulièrement et attentivement vos relevés de compte et vos relevés d'opérations de carte. Dans le cas où figurerait une opération que vous n'avez pas faite.

Réagissez rapidement !

Faites opposition à votre carte : Téléphonez au numéro d'opposition mis en place par votre agence bancaire ou composez le numéro interbancaire 0892 705 705. Si vous êtes à l'étranger, contactez le numéro spécifique délivré par votre banque.

Confirmez toujours votre opposition en envoyant un courrier recommandé avec accusé de réception à votre banque. Votre carte ne pourra plus être utilisée et vous pourrez demander le remboursement des opérations effectuées frauduleusement.

Signalez la fraude bancaire sur la plateforme PERCEVAL du ministère de l'Intérieur. C'est un site gouvernemental, destiné à gérer la cybercriminalité liée à la carte bancaire. Il concerne uniquement l'utilisation, à votre insu, de vos coordonnées bancaires, non le vol de votre carte. Le signalement sur la plateforme facilite le remboursement des sommes dérobées et centralise les plaintes afin de faciliter les recherches sur les auteurs de ces fraudes. Pour accéder à cette plateforme, vous devez vous rendre sur le site service-public.fr et vous identifier à l'aide du système "France Connect" ».

Déposez plainte auprès du commissariat ou de la gendarmerie dont vous dépendez en fournissant tous les éléments de preuve en votre possession.

Assurez-vous que vos comptes en ligne n'ont été piratés. Si vous avez un doute, changez vos mots de passe et activez la double authentification. Celle-ci vous alertera et vous

demandera une confirmation chaque fois qu'une nouvelle personne essaiera de se connecter à votre compte.

Vous devez agir *"sans tarder"* après la découverte de l'opération non autorisée **dans un délai maximum de 13 mois** à compter du débit en compte pour un paiement dans l'Espace Economique Européen (EEE) (article L.133-24 du code monétaire et financier). Si l'opération contestée a été réalisée hors de l'Espace économique européen (les 27 États membres de l'Union européenne plus l'Islande, le Liechtenstein et la Norvège), **le délai de contestation est seulement de 70 jours**. Il peut être prolongé contractuellement, sans pouvoir dépasser 120 jours.

Que doit vous rembourser la banque ?

En cas de débit indu alors que vous êtes toujours en possession de votre carte, la banque doit vous rembourser immédiatement le montant de l'opération non autorisée et le cas échéant rétablir le compte débité en l'état où il se serait trouvé si l'opération de paiement n'avait pas eu lieu (article L. 133-18 du code monétaire et financier). Vous ne pourrez pas être remboursé par la banque si vous n'avez pas satisfait intentionnellement ou par une négligence grave aux obligations vous incombant et notamment à celle de notification sans tarder, ou si vous avez agi frauduleusement

L'enregistrement de l'opération de paiement ne suffit pas nécessairement à prouver qu'elle a été autorisée par le titulaire de la carte. **Il appartient à la banque de prouver la fraude ou la négligence grave du client** (article L.133-23 du code monétaire et financier). Cette preuve ne peut se déduire du seul fait que la carte bancaire ou les données qui lui sont liées aient été effectivement utilisées.

Quelles précautions devez-vous prendre pour éviter une utilisation frauduleuse de votre carte bancaire ?

- Ne communiquez jamais vos coordonnées bancaires par messagerie ou par téléphone.
- Faites attention aux demandes de validation ou de remboursement d'un achat que vous n'avez pas réalisé.
- Attention aux mails ou appels téléphoniques dans lesquels on vous demande de communiquer vos données bancaires, identifiants, mots de passe, code confidentiel.
- Conservez précieusement et séparément votre carte bancaire et votre code confidentiel.
- Pensez à masquer le cryptogramme au verso de votre carte.
- Vérifiez régulièrement vos relevés de compte.
- Pour des achats sur internet, n'enregistrez pas vos données bancaires et vérifiez qu'elles n'aient pas été enregistrées sans votre accord.
- Mettez à jour vos outils informatiques notamment vos antivirus.
- Utilisez un ordinateur privé (c'est-à-dire non partagé en public) pour des achats en ligne.
- Faites attention aux pièces jointes des mails reçus et aux applications que vous pourriez télécharger : celles-ci peuvent contenir des virus.

(Sources : UFC QUE CHOISIR, Institut National de la Consommation)

NOUS POUVONS VOUS AIDER
N'HESITEZ PAS A NOUS CONTACTER
PAR TELEPHONE, DANS NOS PERMANENCES,
EN LIGNE VIA NOTRE MESSAGERIE OU NOTRE SITE

UFC ARTOIS
Tony MORALES responsable de la commission litiges