Image not found or type unknown

Utilisation frauduleuse d’une carte bancaire

Fiche pratique publié le **22/12/2017**, vu **1453 fois**, Auteur : Assistant-juridique.fr

Il ne faut jamais transmettre de données personnelles par courriel, quel qu’en soit l’émetteur ! Sinon, cela peut coûter, comme dans l’affaire suivante.

La titulaire d’un carte bancaire fait immédiatement opposition à son utilisation lorsqu’elle reçoit de sa banque deux messages sur son téléphone portable lui communiquant un code, dit « 3D Secure », afin de valider des achats sur Internet qu’elle n’a en réalité jamais effectués.

Trop tard. 3 300 € d’achats frauduleux ont déjà été débités de son compte. Elle demande alors à sa banque de lui rembourser cette somme.

Peine perdue. Elle avait auparavant répondu à un courriel émanant soi-disant de son opérateur téléphonique et avait fourni ses coordonnées personnelles : numéro de carte, date d’expiration et cryptogramme figurant au verso de la carte ainsi que son numéro de portable. Ce faisant, même si elle a été victime d’un hameçonnage (encore appelé phishing), elle a commis une négligence grave dans la conservation des dispositifs de sécurité personnalisés mis à sa disposition. La banque n’était donc pas tenue de la rembourser.

Cass. com. 25 octobre 2017, n° 16-11644

Vente en ligne et fraude à la carte bancaire : qui est responsable ?

Articles sur le même sujet :

- Créer et gérer un site de e-commerce NOUVEAU
- Réussir la création de sa SARL

- Quelle est la loi applicable à un site de e-commerce ?
- Les obligations posées par la loi Chatel
- Le droit de rétractation
- Le délai de livraison
- La responsabilité du vendeur
- Recours en cas d’absence ou de retard de livraison
- Recours en cas de colis endommagé
- Recours en cas d’arnaque
- La délivrance d’une facture est-elle obligatoire sur internet ?
- Les litiges liés aux achats en ligne
- Les risques du paiement en ligne

Copyright © 2025 Légavox.fr - Tous droits réservés