

## Comment réagir en cas de fraude à la carte bancaire ?

Dès que vous avez connaissance d'une opération de paiement ou de retrait par carte non autorisée, il convient :

- **Dans un premier temps, d'informer sans tarder votre banque ou le centre d'appel dédié afin de mettre votre carte en opposition** (il en va de même si votre carte est perdue ou volée) :
  - en contactant directement votre conseiller en agence ;
  - en vous rendant sur votre Espace Client ;
  - en appelant le numéro d'opposition propre à votre banque (qui figure sur votre contrat, mais également au dos des tickets de retrait et à côté des distributeurs de billets) ;
  - en appelant le numéro spécial du serveur interbancaire : **0 892 705 705** (Tarif : 0,34 € la minute). Ce service est ouvert 24 h sur 24, 7 jours sur 7, et oriente votre appel vers le centre d'opposition compétent.
- **Ensuite, de confirmer par écrit et sans délai l'opposition selon les modalités prévues par votre banque.**

**En outre**, vous devez signaler **sans délai** l'opération non autorisée auprès de votre établissement qui vous indiquera les démarches à effectuer.

### Attention :

Cette information doit se faire au plus tard **13 mois** après le débit. Ce délai est ramené à 70 jours (le contrat carte peut prévoir un délai plus long, ne pouvant dépasser 120 jours) lorsque l'établissement du bénéficiaire du paiement se situe en dehors de l'Union Européenne ou de l'Espace Économique Européen - EEE (les États de l'Union ainsi que l'Islande, le Lichtenstein et la Norvège).

Enfin, il est possible de déclarer la fraude auprès de la police ou de la gendarmerie. Cette démarche n'est cependant pas une condition préalable pour que la banque vous rembourse. Si vous êtes toujours en possession de la carte, vous pouvez signaler la fraude sur la plateforme en ligne Perceval.

## Quelle est votre responsabilité en cas fraude à la carte bancaire ?

Dès que vous vous apercevez de la perte, du vol ou du détournement de votre carte, vous devez en informer sans tarder votre banque afin de faire procéder à son blocage.

**En cas de perte ou de vol, vous supportez, avant le blocage de votre carte, les conséquences financières liées à son utilisation dans la limite d'un plafond qui ne peut dépasser 50 euros.**

Cette franchise ne sera pas appliquée lorsque :

- l'opération en cause a été effectuée sans frappe de votre code confidentiel ;
- la perte ou le vol ne pouvait pas être détecté(e) avant le paiement ;
- votre préjudice financier résulte d'une faute ou d'une négligence de votre banque ou de son

prestataire ;

- le dispositif d'authentification forte n'a pas été demandé par votre banque.

**En cas de détournement de votre carte, (votre carte bancaire est toujours physiquement en votre possession), votre responsabilité n'est pas engagée. Vous devez néanmoins signaler sans délai la ou les opérations non autorisées à votre agence bancaire.**

Pour en savoir plus :

Qu'est-ce que l'authentification forte des paiements ?

Quels sont vos droits au remboursement en cas de fraude à la carte bancaire ?

## **Quels sont vos droits au remboursement en cas de fraude à la carte bancaire ?**

En cas d'opérations non autorisées résultant de la perte, du vol ou du détournement (utilisation frauduleuse à distance ou contrefaçon) de la carte, votre banque doit rembourser :

- **le montant de la transaction contestée** (sauf en cas de fraude du titulaire de la carte) ;
- **éventuellement, les agios et frais d'incidents** que l'opération a pu générer.

Ce remboursement doit intervenir **immédiatement et au plus tard à la fin du premier jour ouvrable** suivant la réception de la contestation. Il n'est pas nécessaire d'avoir souscrit une assurance spécifique pour bénéficier de cette disposition légale.

**À noter :**

**Pour refuser le remboursement, l'établissement doit démontrer l'agissement frauduleux ou la négligence grave de l'utilisateur de la carte soit dans la conservation de ses données bancaires, soit dans l'obligation de signaler, sans tarder, le vol, la perte ou toute utilisation frauduleuse de l'instrument de paiement à fin de blocage de ce dernier.** La charge de la preuve lui appartient.

Si l'opération de paiement non autorisée a été effectuée **sans que la banque** (ou le prestataire de services de paiement) **n'ait exigé une authentification forte du client, ce dernier**, hors agissement frauduleux de sa part, **ne supporte aucune conséquence financière et doit être remboursé.**

Si vous êtes victime d'une fraude à la carte bancaire, **signalez-la immédiatement à votre banque et au plus tard dans un délai de 13 mois après le débit.**

Pour en savoir plus :

Qu'est-ce que l'Observatoire de la sécurité des moyens de paiement et quelles sont ses missions ?

Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2019 (publié en septembre 2020)

Qu'est-ce que l'authentification forte ?

Comment réagir en cas de fraude à la carte bancaire ?

**Attention :**

- Si la réglementation des opérations non autorisées par carte bancaire est protectrice des

intérêts du consommateur, il n'en demeure pas moins que celui-ci ne dispose pas d'un droit inconditionnel au remboursement.

- Vérifiez régulièrement vos comptes bancaires.
- Restez vigilant, et en cas de doute, contactez votre banque.

## **Quiz : à vous de jouer... Vérifiez que vous avez les bons réflexes pour vous prémunir de la fraude à la carte bancaire !**

- **Je reçois un email m'indiquant que je suis éligible à un remboursement d'impôt et m'invite à cliquer sur un lien et à renseigner les données de ma carte bancaire. Dois-je donner suite à cette demande ?**

Réponse :

**Non.**

La Direction générale des Finances publiques (DGFiP) dispose déjà de vos informations bancaires et ne vous demandera jamais, pour un remboursement d'impôt, de renseigner les données de votre carte bancaire. Des fraudes similaires de phishing peuvent utiliser le logo de la Sécurité sociale par exemple.

- **Un individu me contacte par téléphone et m'indique travailler pour ma banque. Cette personne prétend que des opérations frauduleuses sont en cours et me demande les données de carte bancaire et/ou le code d'authentification reçu sur mon mobile afin de sécuriser mon compte ou éviter que le compte soit bloqué. Dois-je contacter ma banque et ne pas donner suite à l'appel ?**

Réponse :

**Oui.**

Il s'agit d'une fraude. Votre banque ne vous demandera jamais par téléphone les données de votre carte et/ou des codes d'authentification pour débloquer votre compte ou le sécuriser. Raccrochez et contactez votre banque afin de l'informer de cet appel frauduleux.

- **Suite à une commande sur internet, je reçois un SMS indiquant que mon colis est bloqué à la frontière et que pour le recevoir je dois régler des frais de douane en cliquant sur le lien. Dois-je renseigner les données de carte bancaire sur le formulaire, après avoir cliqué sur le lien de renvoi contenu dans le SMS ?**

Réponse :

**Non.**

Les frais de transport ont été réglés au moment de la commande. Ce type de message est également une fraude et il convient de le supprimer et de ne pas cliquer sur le lien. Le smishing (par SMS) est une fraude similaire au phishing (par Email) et il est important de se protéger et ne pas y donner suite.

- **Je suis en train de régler mon stationnement à l'horodateur d'un parking. Un individu s'approche et me dit avoir oublié sa carte bancaire. Il me demande de régler son stationnement avec ma carte et propose un billet de 5 euros en échange. Faut-il**

### **procéder à l'échange ?**

Réponse :

**Non.**

À l'instar de l'arnaque dites « du collet » au distributeur de billets, les fraudeurs installent un dispositif permettant de bloquer votre carte, dans l'horodateur, pour la récupérer après votre départ. Si votre carte est bloquée à l'intérieur de l'horodateur, faites immédiatement opposition à votre carte bancaire et déposez sans délai une plainte.

Mis à jour le : 22/01/2022