

Carte bancaire

9 RÉFLEXES SÉCURITÉ



**les clés de
la banque**

LES GUIDES BANCAIRES
N°5 / Sécurité

CE GUIDE VOUS EST OFFERT PAR :



**Pour toute information complémentaire,
nous contacter : info@lesclesdelabanque.com**

Le présent guide est exclusivement diffusé à des fins d'information du public. Il ne saurait en aucun cas constituer une quelconque interprétation de nature juridique de la part des auteurs et/ou de l'éditeur. Tous droits réservés. La reproduction totale ou partielle des textes de ce guide est soumise à l'autorisation préalable de la Fédération Bancaire Française.

Éditeur : FBF – 18 rue La Fayette 75009 Paris – Association Loi 1901

Directeur de publication : Maya Atig

Imprimeur : Concept graphique,

ZI Delaunay Belleville – 9 rue de la Poterie – 93207 Saint-Denis

Dépôt légal : février 2025

SOMMAIRE

9 RÉFLEXES SÉCURITÉ

1. Je garde ma carte en sécurité	4
2. Je garde secret mon code confidentiel	6
3. Je suis attentif quand j'utilise ma carte	8
4. Je suis vigilant quand je communique les données de ma carte	12
5. Je fais immédiatement opposition	16
6. Je signale la fraude/Je porte plainte	20
7. Je consulte régulièrement mon compte	22
8. Je signale rapidement toute anomalie	24
9. Pour tout litige commercial, je m'adresse au commerçant	26
Les réflexes clés	28

Introduction

La sécurité des paiements par carte s'améliore en continu. Cependant, des précautions simples s'imposent toujours pour éviter les fraudes comme l'utilisation, par un tiers, de la carte (perte ou vol) ou de ses données (numéro, date d'expiration, cryptogramme, ...).

1. Je garde
ma carte
en sécurité

Dès que vous avez reçu votre carte (retrait en agence ou réception par courrier à domicile) :

- signez-la au dos si un emplacement est prévu ;
- conservez votre carte en sécurité et sachez toujours où elle se trouve ;
- restituez l'ancienne carte expirée à la banque ou détruisez-la en coupant en plusieurs morceaux la puce, la bande magnétique et les numéros.

Votre carte est strictement personnelle, y compris si elle est rattachée à un compte joint. Ne la confiez jamais à quelqu'un, même à un proche ou se réclamant de votre banque ou d'une autorité.

**2. Je garde
secret
mon code
confidentiel**

- **Ne donnez jamais votre code confidentiel** à qui que ce soit, ni en personne ni à distance (Internet, téléphone...). Même votre banquier n'a pas à le connaître.
- Apprenez-le et ne le notez pas. En cas d'oubli, certaines banques permettent de le retrouver via l'application bancaire. Sinon, demandez sa réédition, moyennant d'éventuels frais (voir les tarifs de votre banque).
- Jamais aucun établissement financier, autorité publique ou quiconque ne vous demandera de le communiquer, même dans de prétendus cas d'urgence ou de contrôles.
- Tapez votre code à l'abri des regards, chez un commerçant, au distributeur de billets, sur tout automate de paiement, en cachant par exemple le clavier avec votre autre main.
- **Ne réutilisez pas votre code pour un autre usage** (connexion à la banque à distance, etc.).

3. Je suis
attentif quand
j'utilise ma carte

- **N'utilisez pas un distributeur de billets qui semble suspect**, notamment au niveau de l'insertion de la carte et/ou du clavier (surépaisseur, par exemple). Signalez-le à la banque qui tient l'appareil.
- **Ne vous laissez pas distraire par un inconnu** lors d'une opération, même s'il demande de l'aide.
- **Vérifiez toujours le montant affiché** sur le terminal de paiement lors d'un achat.
- **Ne perdez jamais de vue votre carte** lors d'un paiement, pour éviter la copie de ses données (numéro, date, cryptogramme).
- Si votre carte est avalée par le distributeur, tentez de la récupérer auprès de l'agence. Si vous n'y parvenez pas, faites opposition par précaution.
- Désactivez les paiements en ligne si vous n'en réalisez jamais.
- Désactivez les paiements à l'étranger.
- En cas de voyage, prévenez votre banque pour éviter des blocages pour suspicion de fraude.
- En cas de perte/vol de votre téléphone, prévenez votre banque et votre opérateur, et bloquez votre appareil.

La carte sans contact est sécurisée :

- ses données ne peuvent pas être interceptées ;
- la franchise de 50€ à votre charge (perte, vol) ne s'applique pas pour les opérations sans contact ;
- au-delà d'un certain montant ou nombre cumulé de paiements sans contact consécutifs, la carte doit être insérée dans le terminal et le code saisi.

Consultez les conditions de votre contrat pour utiliser votre carte en conformité.

Nouveau : Avec le sans contact +, plus besoin d'insérer la carte pour les paiements de plus de 50€. Il suffit d'apposer votre carte sur le terminal de paiement et d'y taper votre code (PIN online).



Voir le guide « Le paiement sans contact ».

4. Je suis
vigilant quand
je communique
les données
de ma carte

- Tapez vous-même l'adresse du site. **Ne suivez pas de lien** ou QR code pour accéder à un site et y procéder à un paiement.
- **Vérifiez la réputation du site commerçant**, lisez **les conditions générales de vente** et assurez-vous de la présence de coordonnées, notamment un service client.
- Assurez-vous que le site et la fenêtre de paiement sont encryptés : **un cadenas ou « https » doit s'afficher en début d'url** (adresse du site).
- **N'enregistrez pas vos coordonnées bancaires** pour vos transactions futures.
- **Évitez de communiquer les données de votre carte par courrier, mail, SMS ou téléphone**, si vous pouvez faire autrement (paiement sécurisé par Internet...).

Pour un achat ou une réservation en ligne, on peut vous demander :

- le n° de la carte bancaire (16 chiffres), sa date d'expiration (au recto) ;
- son cryptogramme (3 chiffres au verso) ;
- vos nom et prénom (au recto) ;
- une validation supplémentaire, par code ou authentification (biométrique par exemple) pour vérifier que c'est bien vous, titulaire de la carte, qui réalisez l'opération.

Cette authentification forte est obligatoire, sauf cas d'exemption (dont : montant faible ou opération récurrente).

N'acceptez jamais d'effectuer cette authentification forte à la demande d'un tiers, notamment par téléphone ou via une messagerie **si vous n'êtes pas à l'initiative de la transaction**. N'en transmettez jamais les éléments (codes à usage unique, mots de passe...), même en cas d'urgence prétendue.

Une authentification forte ne vous permettra JAMAIS d'annuler une opération ou de valider un remboursement en votre faveur ! Un tel discours d'un tiers, quel qu'il soit, doit immédiatement vous amener à rompre tout échange ou transaction en cours.

Sachez repérer les tentatives de fraude : voir le guide « Banque à distance - 10 réflexes sécurité ».

5. Je fais
immédiatement
opposition

Faites opposition **dès que vous constatez la perte, le vol, le détournement ou toute utilisation non autorisée de votre carte** ou de ses données. Votre carte sera ainsi bloquée, évitant toute opération frauduleuse par la suite.

Utilisez l'application de votre banque ou le numéro de téléphone qu'elle vous a fourni. Sinon, appelez :

- en France métropolitaine, le 0 892 705 705 (0,34 € par minute + prix de l'appel) ;
- à l'étranger, le numéro figurant sur les distributeurs de billets.

Vérifiez avec la banque si une confirmation écrite est nécessaire.

Vous ne retrouvez plus votre carte et êtes convaincu qu'elle est en sécurité ? Certains établissements offrent la possibilité de la bloquer temporairement via leur application, le temps de la chercher.

Votre responsabilité ne sera pas engagée :

- pour une opération effectuée après l'opposition ;
- en cas de détournement de la carte ou de ses données, ou de contrefaçon, dès lors que la carte est toujours en votre possession.

Vous serez responsable en cas de fraude ou de négligence grave de votre part (utilisation du code, opposition tardive...) pour les opérations passées avant opposition.

6. Je signale la fraude/Je porte plainte

Après opposition de la carte auprès de votre banque (c'est la priorité !), **signalez la fraude** via la plateforme Perceval si :

- vous avez toujours votre carte avec vous ;
- vous n'êtes pas à l'origine de ces achats en ligne.

Vous aurez besoin de vos identifiants France Connect, du numéro d'opposition, des 16 chiffres de votre carte et des relevés bancaires où apparaissent les opérations frauduleuses.

Si vous n'avez plus votre carte, portez plainte auprès de la police pour vol et utilisation frauduleuse de ses données. Depuis le 15 octobre 2024, vous pouvez déposer une plainte en ligne à condition que vous n'en connaissiez pas l'auteur. À l'étranger, renseignez-vous sur la marche à suivre en contactant l'ambassade de France.

Cette démarche citoyenne contribue à la **lutte contre la fraude**, même si ce n'est pas une condition préalable pour que votre banque vous rembourse : elle aura un recours contre l'escroc et la police pourra enquêter.

**7. Je consulte
régulièrement
mon compte**

Seule une consultation régulière du compte permet de détecter rapidement un incident.

Connectez-vous **au moins 1 fois par semaine** sur le site ou l'application mobile de votre banque. Vérifiez les opérations et le solde, notamment à l'aide des tickets de carte (y compris électroniques) et des mails de confirmation de paiement (pour les achats en ligne). À défaut, pensez à noter le montant et la date de l'opération.

Rappelez-vous que, selon le site marchand, le montant de l'achat peut être débité à la commande, à l'expédition ou encore à réception du bien acheté... Vérifiez les modalités de paiement dans les Conditions Générales de Vente.

**8. Je signale
rapidement
toute anomalie**

En cas de doute ou si vous n'êtes pas à l'origine d'une opération, prévenez immédiatement votre banque.

Elle pourra effectuer des recherches.

En cas d'opération :

- frauduleuse, faites aussitôt opposition pour bloquer la carte et la rendre inutilisable ;
- « **non autorisée** » (par ex, un paiement carte qui a donné lieu à un abonnement, sans que le client n'ait été averti) ou « **mal exécutée** » (erreur date, montant...), signalez-la rapidement à votre banque et au plus tard dans les :
 - **13 mois** suivant la date du débit sur votre compte pour un paiement **dans l'Espace Économique Européen - EEE*** ;
 - **70 jours, pour un paiement hors de l'EEE** (maximum 120 jours si prévu par le contrat carte).

En réagissant vite et en respectant ces délais, **la banque pourra rétablir votre compte** dans l'état où il serait si l'opération n'avait pas eu lieu (**sauf en cas de négligence grave** dans les précautions de sécurité...).

*Les 27 pays de l'Union Européenne + l'Islande, le Liechtenstein, la Norvège.

**9. Pour
tout litige
commercial, je
m'adresse au
commerçant**

Vous n'avez pas été livré ? Le bien n'est pas conforme ?
Contactez le commerçant directement.

Consultez ses conditions générales de vente pour
connaître la procédure de réclamation. **La banque ne**
peut pas intervenir dans les litiges commerciaux.

Vous ne devez pas faire opposition sur votre carte car
il ne s'agit pas d'un cas d'utilisation frauduleuse.

LES RÉFLEXES CLÉS

Carte bancaire

- 1. Je garde ma carte en sécurité**
- 2. Je garde secret mon code confidentiel**
- 3. Je suis attentif quand j'utilise ma carte**
- 4. Je suis vigilant quand je communique les données de ma carte**
- 5. Je fais immédiatement opposition**
- 6. Je signale la fraude/Je porte plainte**
- 7. Je consulte régulièrement mon compte**
- 8. Je signale rapidement toute anomalie**
- 9. Pour tout litige commercial, je m'adresse au commerçant**

lesclesdelabanque.com



FÉDÉRATION
BANCAIRE
FRANÇAISE

