

Carte bancaire - 9 réflexes sécurité

Attention :

Même si l'amélioration de la sécurité des paiements par carte est constante, un certain nombre de précautions s'impose pour contribuer à éviter des fraudes comme : l'utilisation par un tiers de la carte (en cas de perte ou de vol) ou de ses identifiants (numéro, date d'expiration...), la contrefaçon (copie de la piste magnétique...).

1. Je garde ma carte en sécurité

Dès que vous retirez la carte au guichet de votre agence ou que vous la recevez à votre domicile, vous devez :

- **apposer votre signature** au dos sur la partie prévue à cet effet (lorsqu'elle existe),
- **noter et conserver séparément son numéro** et sa date d'expiration **pour faciliter une opposition** rapide,
- détruire l'ancienne carte qu'elle remplace en coupant en deux la puce et la piste magnétique et en plusieurs morceaux la partie sur laquelle est inscrit en relief le numéro de la carte.

Vous devez **conserver votre carte avec précaution et toujours savoir où elle se trouve**. Vous ne devez la confier à personne, même à un proche. L'usage de votre carte est strictement personnel, même si elle est rattachée à un compte joint.

2. Je garde secret mon code confidentiel

- **Ne donnez jamais votre code confidentiel, à qui que ce soit, ni en face à face ni à distance** (sur internet par exemple).
- **Apprenez-le par cœur** et ne le notez nulle part. En cas d'oubli, vous pourrez demander sa réédition moyennant d'éventuels frais (voir la plaquette tarifaire de votre établissement).
- **Tapez toujours votre code à l'abri des regards**, chez un commerçant, au distributeur de billets ou sur tout automate de paiement, en cachant par exemple le clavier avec votre autre main.

3. Je suis attentif quand j'utilise ma carte

- **N'utilisez pas un appareil avec un élément suspect** sur un distributeur de billets (DAB) ou un guichet automatique de banque (GAB), notamment sur la partie d'insertion de la carte et/ou sur le clavier de saisie du code (par exemple surépaisseur). Signalez-le à l'établissement propriétaire du DAB.

- **Ne vous laissez pas distraire par un inconnu lors d'un retrait ou d'un paiement**, même s'il vous propose ou réclame de l'aide.
- Lors d'un achat, **vérifiez** systématiquement que **le montant affiché** sur le terminal de paiement corresponde bien au montant de votre achat
- **Ne perdez jamais de vue votre carte** lors d'un paiement chez un commerçant afin d'éviter que certaines informations qu'elle contient ne puissent être copiées et réutilisées à votre insu, par exemple le cryptogramme visuel (3 derniers chiffres au dos).
- **Si elle est avalée** par le distributeur d'une agence ouverte, **essayez de la récupérer** immédiatement. **Sinon faites opposition.**

Info : utilisez la carte conformément aux conditions du contrat porteur reçu lors de la souscription.

Focus : La carte sans contact

La carte sans contact, qui utilise la technologie NFC (Near Field Communication - ondes radio de très courte portée), permet de payer sans composition du code confidentiel jusqu'à 30 euros par transaction (à compter d'octobre 2017).

Ces cartes sont sécurisées. Des limites d'usage sont prévues. Au-delà d'un certain montant cumulé de paiements sans contact consécutifs (variable selon les banques mais généralement compris entre 50 et 100 euros), **le terminal vous demandera d'introduire votre carte et de saisir votre code confidentiel.**

Les informations comme le code confidentiel, le cryptogramme visuel (les 3 chiffres au verso de la carte), votre nom et votre prénom ne sont pas transmis lors d'une transaction sans contact.

La capture frauduleuse de données est impossible du fait de la très grande proximité nécessaire (moins de 3-4 centimètres).

A noter : En cas de fraude ou de perte, **vous bénéficiez** pour votre carte sans contact **de la même protection** que pour les cartes bancaires sans cette fonctionnalité. En outre, **la franchise** (voir infra) **ne s'applique pas pour les transactions sans contact et sans code confidentiel.**

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

Ne suivez pas de lien depuis un courriel par exemple pour vous rendre sur un site. N'achetez qu'auprès d'un commerçant dont vous êtes sûr : vérifiez que « https » s'affiche devant l'adresse du site et lisez attentivement les conditions générales de vente.

Pour un achat en ligne ou pour réserver un bien ou service, **on peut légitimement vous demander** :

- **le n° de votre carte bancaire** : 16 chiffres répartis en 4 blocs de 4 chiffres (au recto),
- **la date d'expiration** (au recto),
- **le cryptogramme** : 3 derniers chiffres (au verso de la carte à côté de la zone de signature),
- **le nom et éventuellement le prénom** (au recto)

- et souvent **un code supplémentaire de type 3DSecure**. Envoyé par sms, courrier électronique, téléphone ou via un boîtier transmis par votre banque, (le sms étant le plus souvent utilisé), ce système permet de vérifier que la personne en train d'effectuer le paiement est bien le titulaire de la carte.

Il est déconseillé de stocker son numéro de carte dans son compte client.

Info : Evitez de communiquer les données de votre carte par courrier (électronique ou papier), par sms ou téléphone si vous pouvez faire autrement (paiement par internet...). Sachez repérer les tentatives de phishing (voir le guide « Banque à distance – 10 réflexes sécurité »).

5. Je fais immédiatement opposition

Vous devez faire opposition sans tarder dès que vous constatez la perte, le vol, le détournement ou toute utilisation non autorisée de votre carte ou des données qui y sont liées.

Cette opposition permet de bloquer la carte et la rend inutilisable évitant ainsi toute opération frauduleuse par la suite.

A noter : une opposition tardive vous priverait de la prise en charge par la banque des opérations contestées (art. L 133-19 IV Code monétaire et financier).

Pour faire opposition, appelez le numéro fourni par votre établissement financier. A défaut **appelez le 0.892.705.705** en France métropolitaine (0,35 € par mn + prix de l'appel). Confirmez au plus tôt par écrit à votre établissement. A l'étranger, appelez le numéro communiqué au préalable par votre établissement ou celui figurant sur les distributeurs de billets.

- En cas d'opération consécutive à la perte ou au vol de votre carte, sans utilisation de votre code confidentiel, votre responsabilité ne sera pas engagée.
Si le code confidentiel a été utilisé, vous supporterez, avant votre opposition, jusqu'à 150 euros de franchise (prochainement abaissée à 50 euros) qui peuvent éventuellement être pris en charge si vous avez une assurance sur vos moyens de paiement.
- Si des opérations sont effectuées en détournant votre carte ou les données qui lui sont liées ou en cas de contrefaçon de votre carte, dont vous êtes toujours en possession, votre responsabilité ne sera pas engagée.

Attention : vous serez responsable en cas de fraude ou de négligence grave de votre part (non-respect de l'obligation de sécurité, opposition tardive...).

6. Je porte plainte

Il est recommandé de porter plainte auprès de la police en cas de vol de votre carte mais aussi en cas d'utilisation frauduleuse de celle-ci ou des données qui lui sont liées.

Ce dépôt de plainte (ou au moins la déclaration de la police) **permettra à votre banque d'avoir un recours contre le voleur ou le fraudeur et à la police de disposer des éléments pour mener son enquête**. Il est donc important de faire cette démarche pour contribuer à la lutte contre la fraude même si ce n'est pas une condition préalable pour que votre compte soit rétabli dans l'état où il serait si l'opération n'avait pas eu lieu.

A l'étranger, renseignez-vous sur la marche à suivre en contactant l'ambassade de France.

Info : La police est tenue de recevoir les plaintes déposées par les victimes d'infractions à la loi pénale (art. 15-3 Code de procédure pénale).

Le gouvernement est en train de mettre en place une plateforme en ligne (sur <https://www.service-public.fr>) pour signaler au plus vite une fraude à la carte bancaire sur internet (achat sur internet, dont vous n'êtes pas à l'origine alors que vous êtes toujours en possession de votre carte bancaire). Cela facilitera le travail des forces de l'ordre.

7. Je consulte régulièrement mon compte

Seule une consultation régulière de votre compte peut vous permettre de détecter un incident.

Connectez-vous au moins une fois par semaine sur le site de votre banque à distance et / ou vérifiez le contenu de votre relevé de compte dès sa réception notamment à l'aide des factures de carte et des courriels de confirmation de paiement (la plupart du temps pour les achats sur internet). Dans le cas contraire, pensez à noter le montant exact et la date de l'opération.

Info : Les Conditions Générales de Vente d'un site marchand doivent décrire précisément les modalités de paiement applicables sur le site : carte débitée à la commande ou à l'expédition ou encore après réception et vérification du bien acheté...

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** par téléphone ou courrier électronique et confirmez par lettre. Selon la nature de l'opération anormale relevée, votre banque pourra faire des recherches.

Attention : s'il s'agit d'une opération frauduleuse, vous devez faire opposition pour bloquer la carte et la rendre inutilisable.

En cas d'« opération non autorisée » ou « mal exécutée », **signalez-la rapidement à votre banque et au plus tard dans les :**

- **13 mois suivant la date du débit** de votre compte **pour un paiement dans l'Espace Economique Européen – EEE***,
- **70 jours suivant la date du débit** de votre compte, **pour un paiement hors de l'EEE** (le contrat porteur peut prévoir un délai plus long ne pouvant excéder 120 jours).

La banque rétablira votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.

A noter : une opposition tardive, un manquement dans les précautions de sécurité... vous priveraient de la prise en charge par la banque des opérations contestées.

**Au 1er janvier 2017, il s'agit des 28 pays de l'Union Européenne et l'Islande, le Liechtenstein, la Norvège.*

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

En cas de litige commercial (défaut de livraison, non-conformité du bien livré...), vous ne devez pas faire opposition car il ne s'agit pas d'un cas d'utilisation frauduleuse de votre carte ou de ses données. C'est avec le commerçant que vous devrez dialoguer pour trouver une solution.

Consultez les conditions générales de vente pour connaître la procédure de réclamation.

Info : La banque ne peut pas intervenir dans les litiges commerciaux.

Info : S'il n'existe pas en tant que tel d'infraction pour « opposition illicite », des peines (emprisonnement, amendes) peuvent en revanche être encourues en cas de « faux ou d'escroquerie » commis dans un dossier d'opposition /réclamation.

9 réflexes pour la sécurité de ma 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 si je communique les données de ma carte
5. Je fais immédiatement opposition
6. 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