

FICHES PRATIQUES



Fraude à la carte de paiement : Quels sont vos droits ?

Que ce soit en France ou à l'étranger, vous pouvez être confronté à une utilisation frauduleuse de votre carte de paiement. Quelles sont vos obligations et celle de votre banque ?

Si d'importants progrès ont été accomplis en matière de sécurisation des transactions, il convient de rester vigilant. En suivant quelques conseils de prudence, vous pouvez concourir à la sécurité de l'utilisation de votre carte de paiement. Sachez qu'en cas de paiement non autorisé effectué sur votre compte, vous disposez d'une protection.

Quelles sont les principales fraudes¹ ?

Il existe **différentes sources de fraude**, dont les principales sont :

- ▶ la carte de paiement a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;
- ▶ un fraudeur utilise la carte de paiement récupérée à la suite d'une perte ou d'un vol ;
- ▶ la carte de paiement a été falsifiée ou contrefaite ;

- ▶ le numéro de la carte a été usurpé. Il est ensuite utilisé pour les paiements frauduleux, notamment sur Internet.

Il existe **plusieurs techniques de fraude**, dont les principales sont :

- ▶ le clonage (ou *skimming*) : les pistes magnétiques de la carte de paiement sont copiées dans un commerce de proximité ou dans des distributeurs automatiques à l'aide d'un lecteur à mémoire. Le cas échéant, le code confidentiel est capturé à l'aide d'une caméra ou par le biais d'un détournement du clavier numérique ;
- ▶ l'hameçonnage (ou *phishing*) : les fraudeurs récupèrent les données personnelles de l'utilisateur de la carte, principalement par le biais de courriels non sollicités renvoyant l'utilisateur vers des sites frauduleux ayant l'apparence de sites de confiance ;

¹ Source : [Rapport annuel de l'Observatoire de la sécurité des moyens de paiement](#)

- ▶ le piratage de systèmes automatisés de données, de serveurs ou de réseaux : intrusion frauduleuse dans ces systèmes.

La fraude peut porter sur **différentes transactions**, dont les principales sont :

- ▶ les paiements à des points de vente ou sur des automates (distributeurs de carburants, de billets de transport, etc.) ;
- ▶ les paiements sur internet (alimentation, habillement, ameublement, voyage, transport, services aux particuliers, téléphonie, jeux en ligne, etc.), mais aussi par courrier et par téléphone, etc. ;
- ▶ les retraits aux distributeurs automatiques de billets.

Suivre les conseils de prudence pour concourir à la sécurité de l'utilisation de sa carte

Dès réception de votre carte de paiement, vous devez prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés.

Vous devez également utiliser votre carte conformément aux conditions régissant sa délivrance et son utilisation (article L.133-16 du Code monétaire et financier).

[L'Observatoire de la sécurité des moyens de paiement](#) a élaboré une série de conseils élémentaires de prudence pour vous aider à protéger vos transactions.

Comment se prémunir contre des opérations non autorisées sur son compte

Toute opération de paiement sur votre compte doit être autorisée par le débiteur (article L.133-6 du Code monétaire et financier).

Le prestataire de services de paiement (PSP)² qui délivre une carte de paiement à un consommateur doit s'assurer que les dispositifs de sécurité personnalisés de cette carte ne sont pas accessibles à d'autres personnes que celui-ci.

Le prestataire supporte le risque lié à l'envoi de la carte de paiement ou de tout dispositif de sécurité personnalisé de celle-ci (article L.133-15 du Code monétaire et financier).

² Il peut s'agir d'un établissement de crédit (par exemple, votre banque), d'un établissement de paiement ou d'un établissement de monnaie électronique.

A savoir

Un paiement non autorisé a été effectué sur votre compte : à qui incombe la charge de la preuve ?

Lorsque vous contestez avoir autorisé une opération de paiement, il appartient au prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre (article L.133-23 du Code monétaire et financier). Les conventions de preuve sont désormais strictement encadrées. L'enregistrement d'une opération de paiement par votre prestataire ne suffit pas nécessairement en tant que tel à prouver que vous avez autorisé cette opération ou que vous n'avez pas satisfait par négligence grave aux obligations qui vous incombent en la matière (article L.133-23 du Code monétaire et financier).

Quels sont les droits et obligations de chacune des parties ?

Dès que vous avez connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de votre carte de paiement, vous devez en informer sans tarder votre prestataire, aux fins de blocage de la carte.

Vous pouvez contacter votre prestataire ou tout service que ce dernier vous aura indiqué.

Vos obligations en tant que titulaire de la carte de paiement (articles : L.133-15, L.133-17 et L.133-24 du Code monétaire et financier)

Le prestataire doit mettre en place les moyens appropriés pour vous permettre de l'informer à tout moment d'une utilisation non autorisée de votre carte et d'en demander le blocage.

Les informations sur ces moyens sont disponibles soit dans le contrat de services de paiement, soit dans la convention de compte de dépôt.

Votre responsabilité ne peut être engagée si le prestataire ne fournit pas ces moyens, sauf agissement frauduleux de votre part.

Le prestataire doit vous fournir (sur demande et pendant 18 mois) les éléments vous permettant de prouver que vous l'avez informé d'une utilisation non autorisée de votre carte.

Votre délai maximal de signalement de l'opération de paiement non autorisée (article L.133-24 du Code monétaire et financier).

Vous devez signaler, sans tarder, à votre prestataire une opération de paiement non autorisée et au plus tard dans les 13 mois suivant la date de débit de votre compte. Après ce délai, votre demande n'est plus recevable.

Les obligations de votre prestataire après le signalement de l'opération non autorisée (articles L.133-15 et L.133-18 du Code monétaire et financier).

Le prestataire doit empêcher toute utilisation de votre carte de paiement après avoir été informé de sa perte, de son vol, de son détournement ou de toute utilisation non autorisée de la carte ou des données qui lui sont liées.

En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues par l'article L.133-24, le prestataire doit :

- ▶ vous rembourser immédiatement l'opération non autorisée
- ▶ et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu.

Une indemnité complémentaire peut éventuellement vous être versée. Elle est décidée contractuellement entre votre prestataire et vous.

Vous disposez d'une carte de paiement dotée d'un dispositif de sécurité personnalisé (par exemple, un code secret) et une opération non autorisée a été effectuée sur votre compte : dans quels cas supportez-vous des pertes financières ? Le cas échéant, quel en est le montant maximal ? (articles L.133-19 et L. 133-20 du Code monétaire et financier).

Avant la demande de blocage de la carte, c'est-à-dire avant « opposition » : lorsque l'opération est effectuée avec l'utilisation du dispositif personnalisé de sécurité, vous supportez, à concurrence de 50 euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de la carte.

Toutefois, lorsque l'opération non autorisée a été effectuée sans l'utilisation du dispositif personnalisé de sécurité, votre responsabilité n'est pas engagée. Vous ne supportez aucune conséquence financière de cette fraude.

Votre responsabilité n'est pas non plus engagée (articles L.133-19 et L.133-20 du Code monétaire et financier) :

- ▶ si l'opération de paiement non autorisée a été effectuée en détournant à votre insu l'instrument de paiement ou les données qui lui sont liées ;

- ▶ en cas de contrefaçon de la carte si elle était en votre possession au moment où l'opération non autorisée a été réalisée.

Rappel

Vous supportez toutes les pertes occasionnées par des opérations de paiement non autorisées lorsque ces pertes résultent d'un agissement frauduleux de votre part ou si vous n'avez pas satisfait (intentionnellement ou par négligence grave) à vos obligations contractuelles de sécurité, d'utilisation ou de blocage de votre carte.

Après la demande de blocage de la carte, vous ne devez supporter aucune conséquence financière résultant de l'utilisation de la carte ou de l'utilisation détournée des données qui lui sont liées, sauf agissement frauduleux de votre part.

Le cas particulier des opérations de paiement extra-européennes quelle que soit la devise utilisée pour l'opération de paiement (article L.133-1-1 du Code monétaire et financier)

Votre prestataire est situé en France métropolitaine, dans les départements d'Outre-mer, à Saint-Martin ou à Saint-Barthélemy, tandis que le prestataire du bénéficiaire de l'opération de paiement est situé dans un Etat non européen, c'est-à-dire qui n'est pas partie à l'accord sur l'EEE¹.

Votre prestataire est situé à Saint-Pierre-et-Miquelon, tandis que le prestataire du bénéficiaire de l'opération de paiement est situé hors de France.

Vous bénéficiez de la même protection.

Toutefois, des règles spécifiques sont applicables :

- ▶ le plafond de 50 euros trouve à s'appliquer pour les opérations non autorisées en cas de perte ou de vol de la carte, même si l'opération a été réalisée sans utilisation du dispositif personnalisé de sécurité ;
- ▶ le délai maximal de contestation de 13 mois est ramené à 70 jours. Ce délai peut être conventionnellement étendu à 120 jours.

¹ L'Espace économique européen (EEE) réunit les Etats membres de l'Union européenne ainsi que le Liechtenstein, la Norvège et l'Islande.

Important

Contester, de mauvaise foi, un ordre de paiement valide dont vous êtes l'initiateur constitue une fraude.

Textes de référence

Code monétaire et financier, notamment les articles :

- [L.133-15 à L.133-17](#)
- [L.133-18](#)
- [L.133-19 à L.133-20](#)
- [L.133-21 à L.133-22](#)
- [L.133-23 à L.133-24](#)

Liens utiles

[Fiche pratique sur le phishing](#) (hameçonnage ou filoutage)

[L'Observatoire de la sécurité des moyens de paiement \(OSCP\)](#)

[Le Conseil consultatif du secteur financier \(CCSF\)](#)

[La Commission nationale informatique et liberté \(CNIL\)](#)

[L'Observatoire national de la délinquance et des réponses pénales \(ONDRP\)](#)

Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer aux textes officiels.

Pour tout renseignement complémentaire, reportez-vous aux textes applicables ou rapprochez-vous d'une [direction départementale de la protection des populations \(DDPP\)](#) ou [direction départementale de la cohésion sociale et de la protection des populations \(DDCSPP\)](#).

Crédit photo : @stock.adobe.com