

## Rapports d'activité

Conformément à l'article L141-4 du Code monétaire et financier, l'Observatoire de la sécurité des moyens de paiement établit chaque année un rapport d'activité remis au ministre chargé de l'économie, des finances et de l'industrie et transmis au Parlement, ainsi que le faisait précédemment l'Observatoire de la sécurité des cartes de paiement.

### Accéder aux publications

2023 2022 2021 2020

Rapport et documents annexes

- [Données clefs sur la fraude au 1er semestre 2023](#)
- [Communiqué de presse de publication des données de fraude du 1er semestre 2023](#)
- [Support de présentation des données de fraude du 1er semestre 2023](#)

Rapport et documents annexes

- [Présentation 2022](#)
- [Rapport 2022](#)
- Dossier statistiques 2022 : [PDF](#) | [Excel](#)
- [Données-clés sur la fraude au 1<sup>er</sup> semestre 2022](#)
- [Communiqué de presse](#)  
Après une baisse globale de la fraude aux moyens de paiement, l'Observatoire engage de nouvelles actions pour améliorer la prévention de la fraude et le remboursement des victimes.
- [Communiqué de presse](#)  
L'Observatoire de la sécurité des moyens de paiement émet des recommandations sur le remboursement des victimes de fraude.

## Rapport et documents annexes

- [Présentation 2021](#)
- [Rapport 2021](#)
- [Données-clés sur la fraude au 1<sup>er</sup> semestre 2021](#)
- [Communiqué de presse](#)

## Rapport et documents annexes

- [Présentation 2020](#)
- [Rapport 2020](#)
- [Communiqué de presse](#)

- [\*\*Rapports et documents annexes, de 2007 à 2019\*\*](#)

## **Sensibilisation du grand public sur l'utilisation de ses moyens de paiements**

### **Conseils de prudence**

L'Observatoire a élaboré une série de conseils de prudence destinés aux utilisateurs de moyens de paiement. Ces conseils ont été rédigés en collaboration avec les représentants des consommateurs, des commerçants et des émetteurs, et ont vocation à être réutilisés par ceux-ci, chacun dans son contexte, auprès de leurs publics.

La liste qui suit est volontairement rédigée de façon simple et se limite aux principales mesures de précaution. L'Observatoire appelle les médias et les pouvoirs publics à relayer largement ces recommandations.

Votre comportement concourt directement à la sécurité de l'utilisation de vos moyens de paiement. Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

### **Les recommandations de l'OSMP**

## **Soyez responsables**

- Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, même pas à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.
- Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile...), gardez-le secret, ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui.
- En particulier, ne communiquez vos mots de passe, codes confidentiels et identifiants personnels ni à des autorités administratives ou judiciaires, ni à votre banque, surtout par téléphone ou par courriel. Ils ne sont jamais susceptibles de vous demander cette information.
- Lorsque vous composez un code ou un mot de passe confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal, du distributeur ou du téléphone avec votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.
- Pensez à consulter régulièrement les consignes de sécurité publiées sur le site de votre banque et assurez-vous qu'elle dispose de vos coordonnées afin de vous contacter rapidement en cas d'opérations douteuses sur votre compte. En cas de contact de votre banque, par téléphone ou par courriel pour de telles opérations, rappelez-vous que vous n'avez pas à lui communiquer vos mots de passe et identifiants personnels.
- N'acceptez jamais de payer un vendeur ou loueur de biens que vous ne connaissez pas par transfert d'argent préalable à la mise à disposition ou la livraison du bien ; il peut s'agir de fraudeurs qui, après avoir récupéré les fonds transférés, font disparaître tout lien de communication (adresse email, compte de réseau social...).

## **Soyez attentifs**

### **Lors des paiements à un professionnel ou à un particulier**

- Vérifiez l'utilisation qui est faite de votre carte bancaire par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider une transaction.

- Lorsqu'un chèque est automatiquement rempli par le commerçant, soyez attentif aux mentions indiquées avant de le signer et vérifiez plus particulièrement le montant.
- Quelques précautions lors du remplissage d'un chèque permettent de réduire les risques de fraude : évitez les ratures ou surcharges, inscrivez le nom du bénéficiaire du chèque et les montants en chiffres et en lettres sans laisser d'espace libre, puis tirez un trait sur l'espace restant non utilisé. Le lieu de paiement et la date doivent être renseignés en même temps que les autres mentions. La signature du chèque ne doit pas déborder sur la ligne de chiffres en bas du chèque. En aucun cas, la signature ne doit être apposée seule sur un chèque, c'est-à-dire sans les mentions relatives au montant et au bénéficiaire préalablement renseignées.

#### **Lors des retraits sur les distributeurs de billets**

- Vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.
- Suivez exclusivement les consignes indiquées à l'écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.
- Mettez immédiatement en opposition votre carte si elle a été avalée par l'automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l'agence.

#### **Lors des paiements sur internet**

- Ne stockez pas de coordonnées bancaires sur votre ordinateur (numéro de carte, numéro de compte, relevé d'identité bancaire...), évitez de les transmettre par simple courriel et vérifiez la sécurisation du site du commerçant en cas de saisie en ligne (cadenas en bas de la fenêtre, adresse commençant par « https », etc.).
- Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les mentions légales du commerçant ainsi que ses conditions générales de vente.
- Ne répondez pas à un courrier électronique, SMS, appel téléphonique ou autre invitation qui vous paraisse douteuse. En particulier, ne cliquez jamais sur un lien inclus dans un message référençant un site bancaire.
- Protégez votre ordinateur, en activant les mises à jour de sécurité proposées par les éditeurs de logiciel (en règle générale gratuites) et en l'équipant d'un antivirus et d'un pare-feu.
- Changez régulièrement vos mots de passe, et évitez d'utiliser la fonction d'enregistrement pour des utilisations ultérieures (une usurpation de vos identifiants et de vos coordonnées bancaires vous expose à des fraudes sur tous vos moyens de paiement).
- N'utilisez pas un mot de passe commun pour l'utilisation de vos moyens de paiement, l'accès à votre banque en ligne et l'accès aux autres sites internet sur lesquels vous avez un compte client

#### **Lors de la réception d'un ordre de paiement ou d'un moyen de paiement**

- Lors de la réception d'un mandat de prélèvement, vérifiez que les informations relatives au créancier (nom / raison sociale, adresse) sont en cohérence avec vos engagements contractuels. Si votre banque a mis en place une liste des créanciers autorisés à effectuer des prélèvements sur votre compte (appelée aussi « liste blanche »), pensez à la mettre à jour.

- Si vous êtes bénéficiaire d'un paiement à distance et que vous ne connaissez pas personnellement le payeur (par exemple, en situation de vente sur internet), vérifiez la cohérence des informations fournies (nom, adresse, identifiant du payeur...) avant de donner votre accord à la transaction. En cas de doute, vérifiez auprès de la banque du payeur la régularité du moyen de paiement proposé et la qualité du payeur.
- Si vous êtes bénéficiaire d'un chèque de banque (par exemple, en cas de vente d'un véhicule), contactez la banque émettrice en recherchant par vous-mêmes ses coordonnées (sans vous fier aux mentions présentes sur le chèque) pour en confirmer la validité avant de finaliser la transaction.
- Vérifiez la présence effective des mentions obligatoires d'un chèque, notamment la signature de l'émetteur du chèque, le nom de la banque qui doit payer, une indication de la date et du lieu où le chèque est établi, ainsi que la cohérence des informations (bénéficiaire, montant, zone numéro de chèque de la ligne magnétique) et l'absence de ratures ou surcharges pouvant indiquer une origine frauduleuse.

#### **Lors de vos déplacements à l'étranger**

- Renseignez-vous sur les précautions à prendre et contactez avant votre départ l'établissement émetteur de votre carte, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.
- Pensez à vous munir des numéros internationaux de mise en opposition de vos moyens de paiement.

**Sachez réagir**

#### **Vous avez perdu ou on vous a volé un instrument de paiement ou vos identifiants bancaires**

- Faites immédiatement opposition en appelant le numéro que vous a communiqué votre banque ou l'émetteur de votre moyen de paiement. Pensez à le faire pour toutes vos cartes, chèquiers ou appareils mobiles comportant une application de paiement qui ont été perdus ou volés. De même contactez votre banque si vous avez communiqué vos coordonnées bancaires (numéro de compte, relevé d'identité bancaire...) à un tiers qui vous paraît douteux.
- En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 150 euros. Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

#### **Vous constatez des activités suspectes sur un de vos moyens de paiement**

- N'hésitez pas à contacter votre banque afin d'évaluer la régularité des opérations de paiement non identifiées ou pour lesquelles vous avez un doute. Contactez plus particulièrement votre banque

lorsque vous recevez des informations par téléphone, courriers électronique ou SMS confirmant ou demandant la validation d'opérations de paiement en cours, que vous n'auriez pas initiées.

**Vous constatez des anomalies sur votre relevé de compte, alors que vos instruments de paiement sont toujours en votre possession**

- N'hésitez pas également à faire opposition afin de vous prémunir contre toute nouvelle tentative de fraude qui utiliserait les données usurpées de votre instrument de paiement.
- Si, dans un délai de 13 mois à compter de la date de débit de l'opération contestée (délai fixé par la loi), vous déposez une réclamation auprès de votre établissement teneur de compte, les sommes contestées doivent vous être immédiatement remboursées sans frais. Dans ces conditions, votre responsabilité ne peut être engagée. Néanmoins ceci ne vaut pas en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir). Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l'opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir néanmoins dépasser 120 jours.

Bien entendu, en cas d'agissement frauduleux de votre part, les dispositions protectrices de la loi ne trouveront pas à s'appliquer et vous resterez tenu des sommes débitées avant comme après l'opposition ainsi que des éventuels autres frais engendrés par ces opérations (par exemple, en cas d'insuffisance de provision).

## **En savoir plus**

- [La sécurité des paiements en ligne \(vidéo\)](#)
- [La fraude aux paiements en ligne \(présentation\)](#)
- [La fraude au chèque \(présentation\)](#)
- [Modalités de remboursement des opérations de paiement frauduleuses \(recommandation\)](#)

## **Commerçants et acteurs des paiements : mettre en oeuvre la DSP2**

### **Sécurité des paiements sur internet**

Documents à l'attention des commerçants élaborés par l'Observatoire de la sécurité des moyens de paiement dans le cadre de la migration DSP2 :

- [Mécanismes de traitement des flux du e-commerce en cas de panne des systèmes d'authentification](#)
- [Mise en œuvre de la DSP2 pour les transactions par carte en ligne : note à l'attention des commerçants, illustrée de certains cas d'usage](#)

## **Pour aller plus loin**

**Mieux connaître les moyens de paiement**

[En savoir plus](#)

**Arnaques aux moyens de paiement, au crédit ou à l'épargne**

[En savoir plus](#)



**Mieux connaître les moyens de paiement**

Outils statistique



**Arnaques aux moyens de paiement, au crédit ou à l'épargne**

Outils statistique