OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2025

BANQUE DE FRANCE

EUROSYSTÈME

Observatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

« Aucune représentation ou reproduction, même partielle, autre que celles prévues à l'article L. 122-5 2e et 3e a) du Code de la propriété intellectuelle ne peut être faite de la présente publication sans l'autorisation expresse de la Banque de France ou, le cas échéant, sans le respect des modalités prévues à l'article L. 122-10 dudit Code. »

© Observatoire de la sécurité des moyens de paiement – 2026

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2025

Adressé à
Monsieur le Ministre de l'Économie, des Finances
et de la Souveraineté industrielle,
énergétique et numérique,
Monsieur le Président du Sénat,
Madame la Présidente de l'Assemblée nationale

par Denis Beau,
premier sous-gouverneur de la Banque de France,
président de l'Observatoire de la sécurité
des moyens de paiement

SEPTEMBRE 2026

SOMMAIRE

SYNTHÈSE 4

2025 EN CHIFFRES 6

CHAPITRE 1
ÉTAT DE LA FRAUDE EN 2025 9

1.1 Vue d'ensemble 10

1.2 État de la fraude sur la carte de paiement 13

1.3 État de la fraude sur le chèque 20

1.4 État de la fraude sur le virement 21

1.5 État de la fraude sur le prélèvement 22

1.6 État de la fraude sur les effets de commerce 23

1.7 État de la fraude par manipulation 24

CHAPITRE 2
ACTIONS CONDUITES PAR L'OBSERVATOIRE AU TITRE DE LA PRÉVENTION DE LA FRAUDE 29

2.1 Plan d'action de lutte contre la fraude par manipulation 29

2.2 Prévention de la fraude sur les paiements par carte à distance 40

2.3 Suivi des autres actions et recommandations de l'Observatoire 44

CHAPITRE 3
LA SÉCURITÉ DES PAIEMENTS PAR CRYPTO-ACTIF 55

3.1 Introduction 55

3.2 La typologie des paiements par crypto-actif 57

3.3 Le fonctionnement technique sous-jacent 59

3.4 Les enjeux de sécurité 62

3.5 Les enjeux de conformité 65

ANNEXES 71

A1 Conseils de prudence pour l'utilisation des moyens de paiement 73

A2 Missions et organisation de l'Observatoire 86

A3 Liste nominative des membres de l'Observatoire 88

A4 Méthodologie de mesure de la fraude aux moyens de paiement scripturaux 91

A5 Dossier statistique sur l'usage et la fraude aux moyens de paiement 101

ENCADRÉ 25

Indicateurs des services du ministère de l'Intérieur sur la fraude aux moyens de paiement en 2025 25

SYNTHÈSE

La dynamique de progression des moyens de paiement scripturaux s'est poursuivie en 2025 à un rythme soutenu *(+ 5,5 % en nombre de transactions en un an, pour des montants en hausse de 4,2 %), portée par les usages les plus innovants. Ainsi, le paiement par mobile concerne désormais un paiement par carte sur cinq au point de vente. Le montant annuel de flux de virement instantané a doublé entre 2024 et 2025. Il représente dorénavant 17 % du nombre de virements émis.*

Le ***chapitre 1*** *du rapport de l'Observatoire souligne que le montant annuel de fraude a progressé à un rythme plus faible (+ 3,8 %, à 1,2 milliard d'euros), avec un nombre de transactions frauduleuses en repli sensible (– 8 %, soit 7,2 millions d'opérations).*

- ***Cette moindre progression de la fraude s'explique par le niveau historiquement bas des taux de fraude sur la carte*** *(47 euros de fraude pour 100 000 euros de paiement)* ***et sur le chèque*** *(69 euros pour 100 000 euros). En effet, ces deux moyens de paiement bénéficient des plans d'action que l'Observatoire a mis en place ces dernières années pour renforcer leur sécurité ;*

- *Dans ce contexte de progression modérée de la fraude,* ***les modes opératoires évoluent. La fraude par manipulation s'accentue****, telle que la fraude au faux conseiller bancaire, la fraude au Président et la fraude à la substitution d'IBAN. Ce type de fraude atteint ainsi 516 millions d'euros en 2025. Cela représente un peu plus de 40 % du montant annuel total de fraude aux moyens de paiement. Sa part a doublé en quatre ans.*

Le chapitre 2 dresse un état des lieux des actions engagées ou soutenues par l'Observatoire en matière de prévention de la fraude*, ce qui recouvre notamment :*

- ***Les actions conduites avec les secteurs des télécommunications et du numérique pour prévenir en amont la fraude par manipulation.*** *Ces actions assurent un renforcement des outils et une meilleure coordination trans-sectorielle en matière de lutte contre les usurpations d'identité sur les différents canaux de communication. Cela comprend les messageries numériques et les réseaux sociaux ;*

- ***La mise en place de mécanismes de partage d'informations entre prestataires de services de paiement. On relève en particulier le service de vérification du bénéficiaire instauré en octobre 2025 et, depuis mai 2026, le fichier national des comptes signalés pour risque de fraude.*** *Ces dispositifs constituent des infrastructures supplémentaires permettant de mutualiser des informations utiles pour la détection de virements à risque, notamment dans le cas de fraude par manipulation ;*

- ***La conduite d'un plan d'action visant à sécuriser les paiements par carte à distance ne recourant pas au protocole technique*** **3-D Secure.** *Il associe des mesures collectives axées sur les canaux les plus vulnérables à des mesures individuelles ciblant les commerçants les plus exposés à la fraude. Ce plan a déjà contribué à l'amélioration du taux de fraude sur les paiements par carte sur internet en 2024 et 2025, et sera poursuivi en 2026 ;*

- ***Le suivi des recommandations de l'Observatoire pour renforcer la sécurité du chèque****, notamment pour ce qui concerne l'envoi des chéquiers par voie postale et l'ouverture de l'accès au Fichier national des chèques irréguliers qui permet aux banques de protéger leurs remettants.*

Le chapitre 3 rend compte des travaux de veille de l'Observatoire sur la sécurité des paiements par crypto-actif*, et émet des recommandations à l'attention des professionnels des paiements, des commerçants et des utilisateurs. Celles-ci portent sur les conditions d'une utilisation qui assure un niveau de sécurité aussi proche que possible de celui des instruments de paiement de détail traditionnels, comme la carte ou le virement.*

Dans un contexte d'évolution rapide des moyens de paiement, mais aussi des techniques de fraude, ***l'Observatoire reste mobilisé pour veiller à la sécurité de l'ensemble des moyens de paiement. L'objectif est d'offrir à tous les utilisateurs, particuliers comme entreprises, une réelle liberté de choix dans leurs usages au quotidien****. Dans son programme de travail pour 2026-2027, l'Observatoire orientera ses travaux de veille technologique sur la sécurité des nouvelles techniques d'authentification et leur intégration dans les nouveaux parcours de paiement. Ces travaux de veille traiteront des enjeux de sécurité liés au commerce au travers d'agents d'intelligence artificielle. L'Observatoire approfondira aussi son analyse des risques à venir concernant l'informatique quantique afin de clarifier la feuille de route du marché français en la matière, dans le prolongement de l'étude de veille publiée dans son rapport annuel 2023. Enfin, il poursuivra les actions de prévention de la fraude, engagées en partenariat avec les acteurs du secteur des télécommunications et du numérique, ainsi que les actions de sensibilisation auprès du grand public.*

L'USAGE DES MOYENS DE PAIEMENT EN 2025

36 264
Mds€ ÉCHANGÉS

+4,2 %
DE PAIEMENTS SCRIPTURAUX PAR RAPPORT À 2024

-46 %
DE MONTANT DES TRANSACTIONS PAR CHÈQUE PAR RAPPORT À 2020

63 %
DES PAIEMENTS SONT RÉALISÉS PAR CARTE

17 %
DES VIREMENTS SONT INSTANTANÉS

19 %
DES PAIEMENTS DE PROXIMITÉ PAR CARTE SONT RÉALISÉS PAR PORTEFEUILLE MOBILE

L'ÉVOLUTION DE LA FRAUDE EN 2025

0,047 %
BAISSE SENSIBLE DU TAUX DE FRAUDE SUR LA CARTE, PLUS BAS NIVEAU HISTORIQUE

- 50 %
TAUX DE FRAUDE POUR LES PAIEMENTS PAR CARTE SUR INTERNET DEPUIS 2020

0,069 %
STABILISATION DU TAUX DE FRAUDE SUR LE CHÈQUE

1,241
Md€ DE PRÉJUDICE

+ 3,8 %
DE FRAUDE EN VALEUR

0,041 %
TAUX DE FRAUDE SUR LES VIREMENTS INSTANTANÉS

516 M€
DE FRAUDE PAR MANIPULATION

2025 EN CHIFFRES

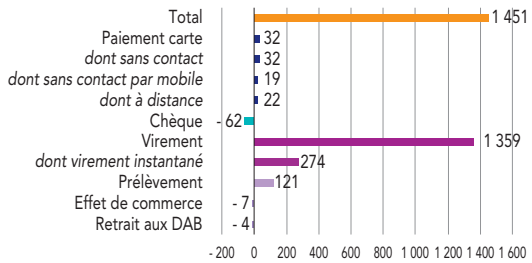
1

ÉTAT DE LA FRAUDE EN 2025

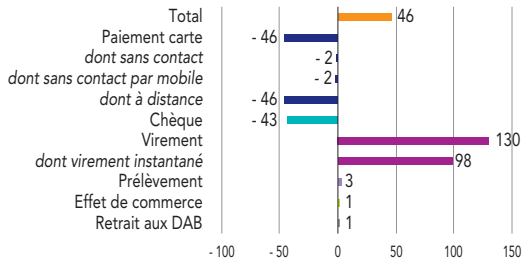
Données clés

G1 Évolution des moyens de paiement entre 2024 et 2025

a) Flux de paiement (en milliards d'euros)



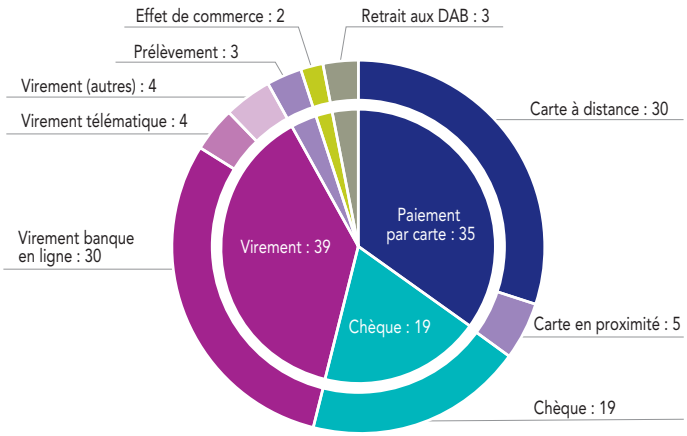
b) Fraude (en millions d'euros)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

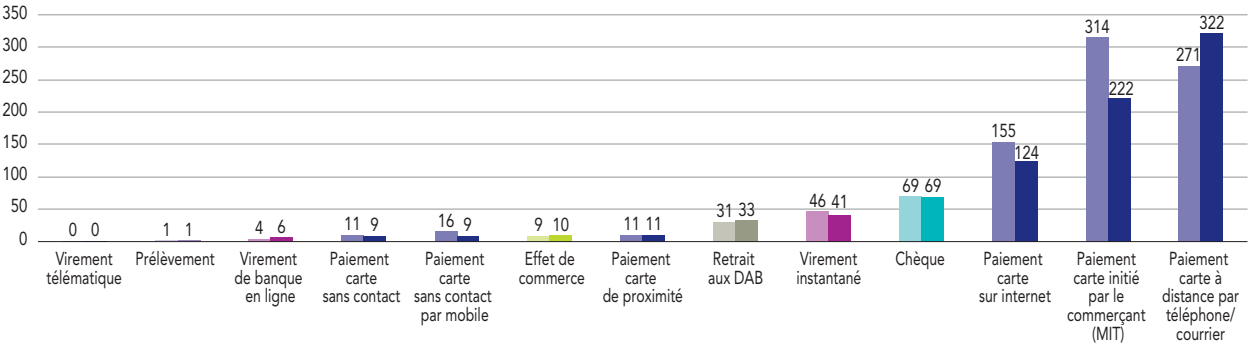
G2 Les principales sources de fraude en valeur (en %)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

G3 Vulnérabilité des principaux canaux de paiement à la fraude en 2024 et 2025 (en euros de fraude pour 100 000 euros de paiement)



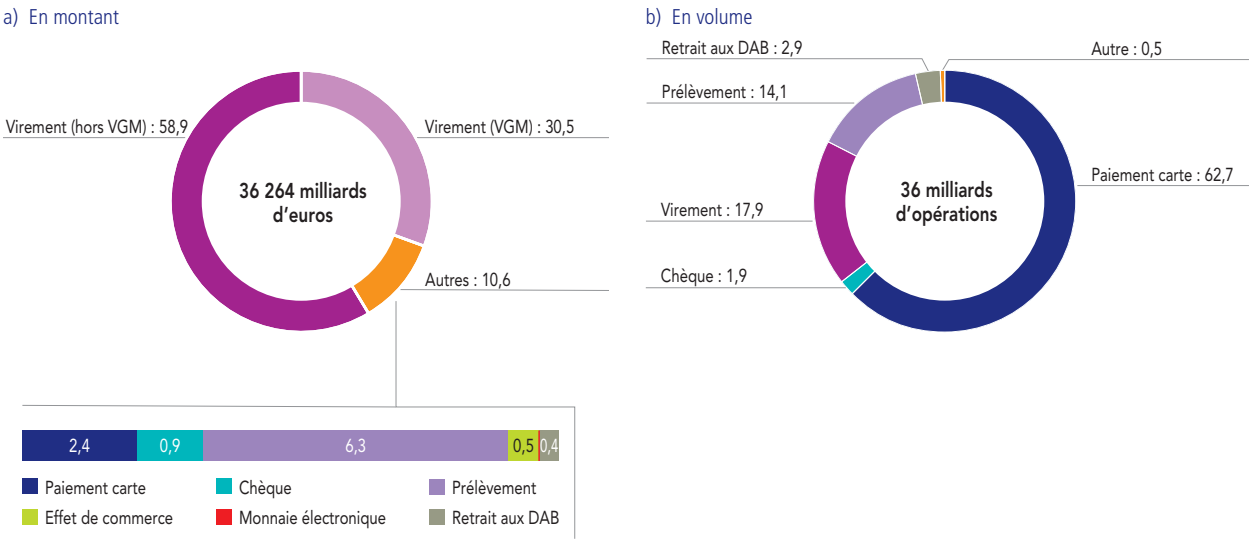
Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

1.1 Vue d'ensemble

1.1.1 Cartographie des moyens de paiement

G4 Usage des moyens de paiement scripturaux en 2025 (en %)



Note : VGM, virement de gros montant ; DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

Les opérations de paiement scripturales réalisées par les particuliers, les entreprises et les administrations ont atteint 35,6 milliards de transactions en 2025 (+ 5,5 % par rapport à 2024), pour un total de 36 264 milliards d'euros (+ 4,2 % par rapport à 2024).

À l'instar de ce qui a pu être observé ces dernières années, l'usage de moyens de paiement innovants affiche des taux de croissance soutenus, tandis que l'usage du chèque continue de fléchir : avec un repli de 16 % en montant, il ne représente plus que 1,9 % des transactions en volume.

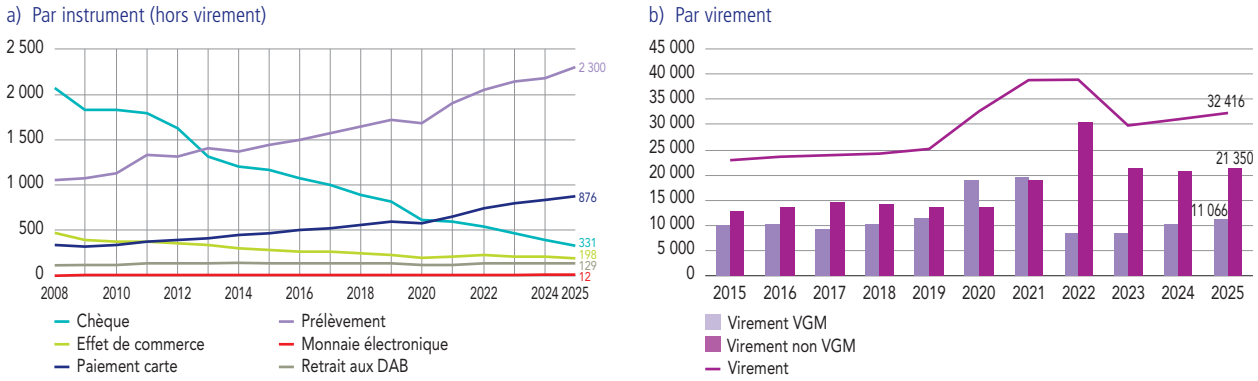
Les virements demeurent prédominants dans le total des flux en montant, avec une part stable à 89 %. Les virements de gros montant (VGM) représentent 34 % des montants échangés par virement, pour seulement 0,2 % de leur nombre. L'usage du virement instantané s'accélère (+ 78 % en volume et + 118 % en montant) et représente désormais 17 % des virements en volume (contre 10 % en 2024).

La carte bancaire demeure le moyen de paiement scriptural préféré des Français, et son usage continue de progresser. Sa part, hors retraits, dans les volumes de transactions passe de 62,1 % en 2024 à 62,7 % en 2025. La croissance des flux en volume se retrouve aussi dans le paiement sans contact (72 % des paiements par carte de proximité, contre 68 % en 2024). La dynamique du paiement sans contact est sous-tendue par celle du paiement par mobile, qui continue de se développer et représente dorénavant plus de 19 % des paiements par carte de proximité, contre 15 % en 2024.

Pour la deuxième année consécutive, les retraits d'espèces par carte baissent (– 5 % en volume et – 3 % en montant).

Le prélèvement suit la tendance générale observée sur l'ensemble des moyens de paiement : + 5 % en volume et + 6 % en montant par rapport à 2024.

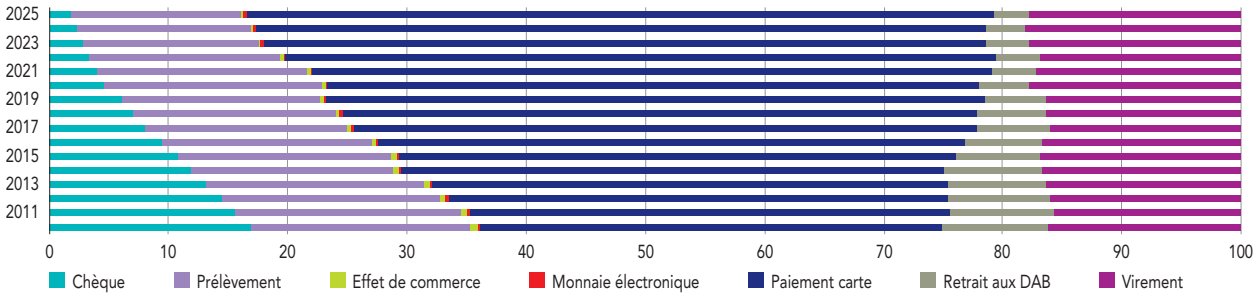
G5 Flux de paiement en montant (en milliards d'euros)



Notes : DAB, distributeurs automatiques de billets ; VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

G6 Évolution de l'usage des moyens de paiement en volume (en %)



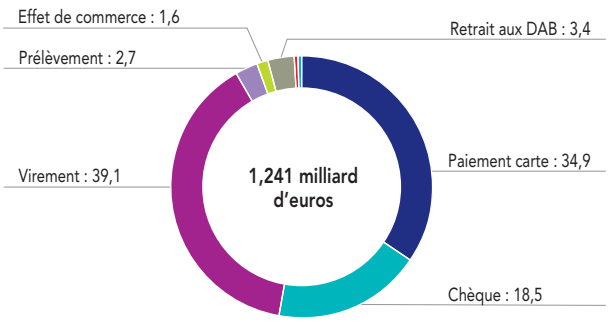
Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

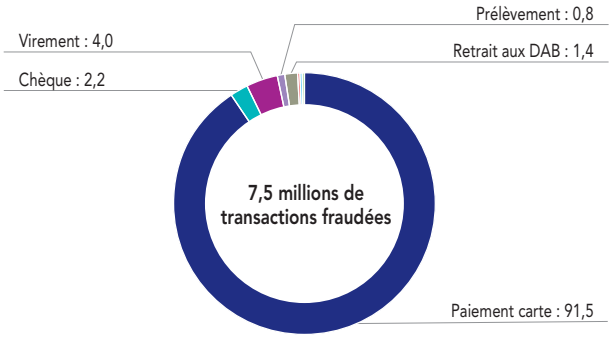
1.1.2 Panorama de la fraude aux moyens de paiement

G7 Répartition de la fraude (en %)

a) En valeur

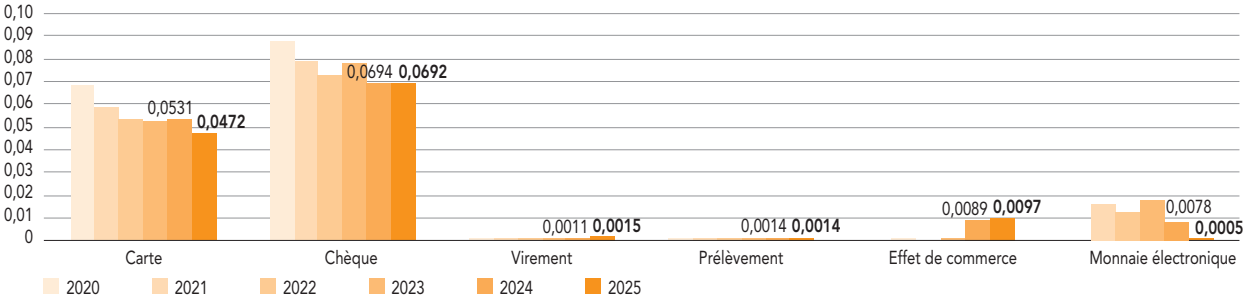


b) En volume



Note : DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

G8 Évolution du taux de fraude en valeur par moyen de paiement (en %)



Note : À partir de 2021, le taux de fraude sur le chèque est calculé selon la nouvelle approche. Celle-ci exclut les fraudes qui sont déjouées après la remise du chèque à l'encaissement et son règlement.
Source : Observatoire de la sécurité des moyens de paiement.

La progression des transactions scripturales s'accompagne d'une augmentation du montant de la fraude qui atteint 1,241 milliard d'euros, dans des proportions toutefois plus faibles qu'en 2024 (+ 3,8 %, contre une progression des flux en montant de + 4,2 %). Toutefois, le nombre de transactions fraudées fléchit de 7,6 % pour atteindre 7,2 millions d'opérations.

Ces évolutions résultent d'une augmentation de la fraude sur le virement (+ 130 millions d'euros, dont 98 millions sur le virement instantané) et dans une moindre mesure i) de la fraude sur le prélèvement (+ 3 millions d'euros), ii) sur le retrait par carte (+ 1,3 million d'euros) et iii) sur les effets de commerce (+ 1,1 million d'euros). Cette tendance est en partie contrebalancée par la baisse de la fraude sur le paiement par carte à distance (– 46 millions d'euros), qui constitue l'essentiel de l'évolution sur ce moyen de paiement, et de la fraude sur le chèque (– 43 millions d'euros).

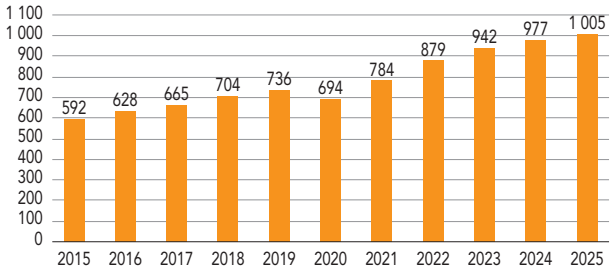
Le virement devient ainsi la principale source de fraude en valeur en 2025 (39 % de la fraude, contre 30 % en 2024).

1.2 État de la fraude sur la carte de paiement

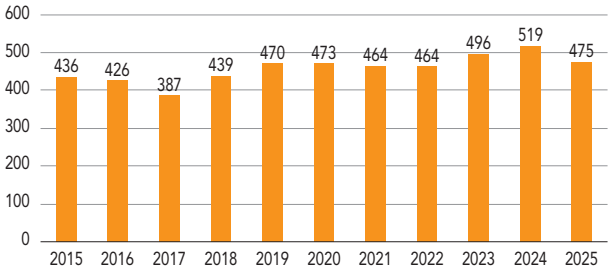
1.2.1 Vue d'ensemble – Cartes émises en France

G9 Les cartes émises en France en 2025

a) Montant total des opérations (en milliards d'euros)



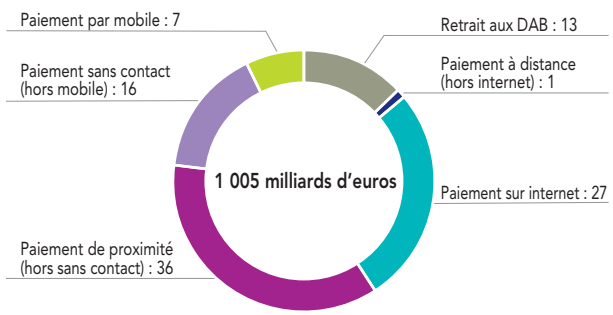
b) Valeur totale de la fraude (en millions d'euros)



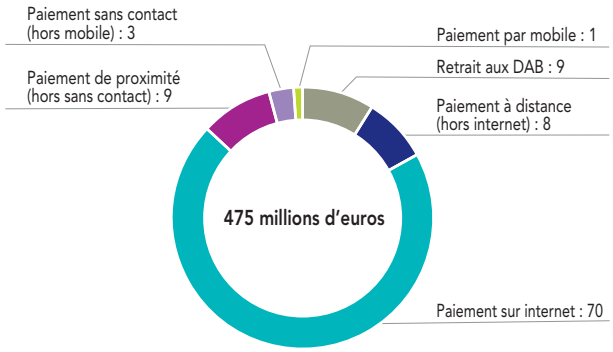
Source : Observatoire de la sécurité des moyens de paiement.

G10 Le canal d'utilisation des cartes émises en France en 2025 (en %)

a) Répartition du montant des opérations



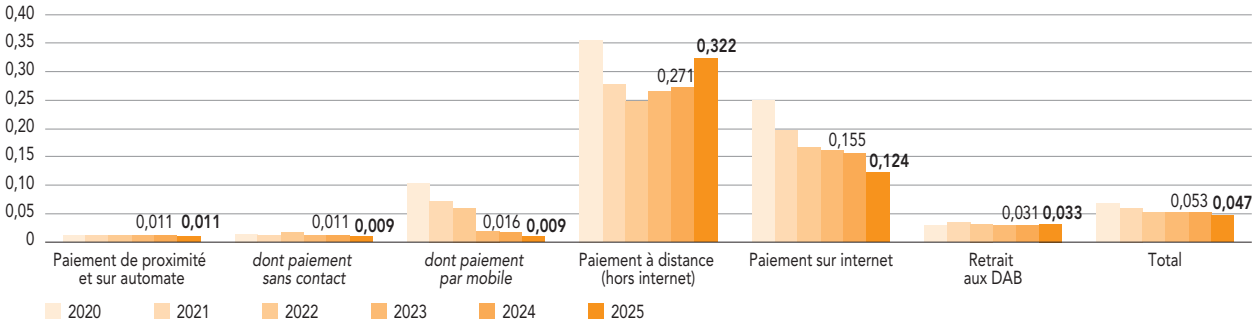
b) Répartition de la valeur de la fraude



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

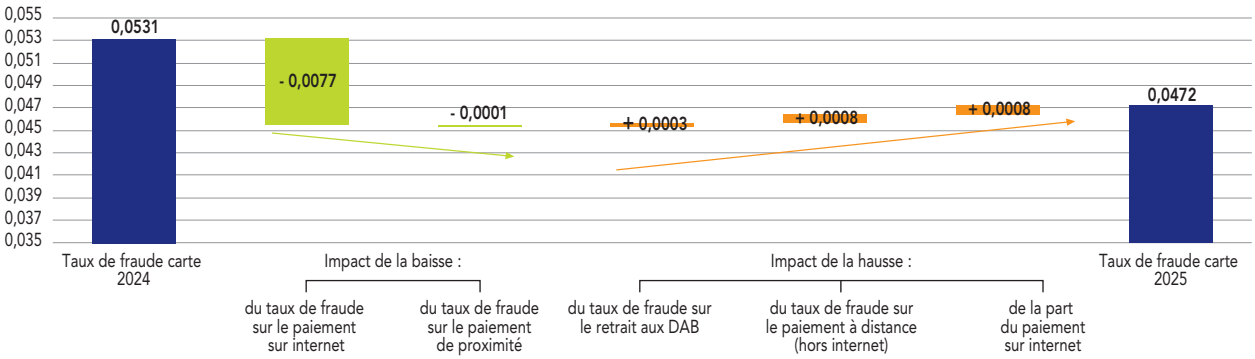
G11 Évolution des taux de fraude en valeur sur les cartes françaises par canal d'initiation (en %)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

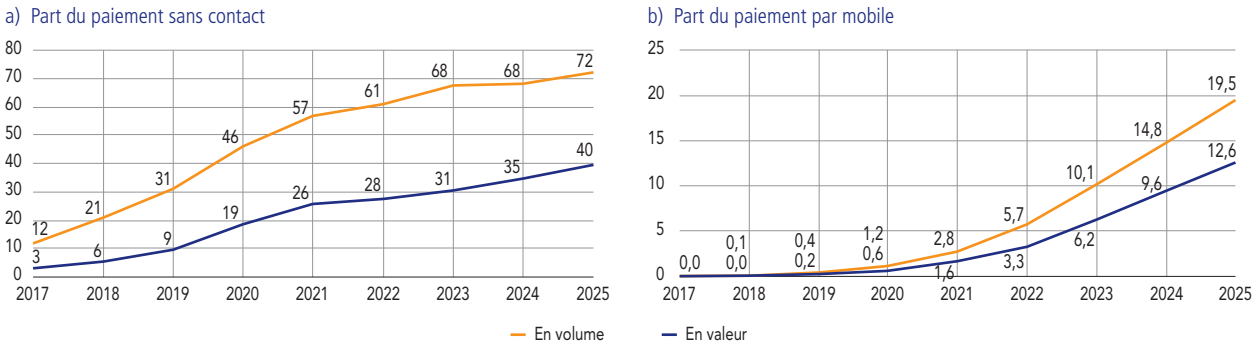
G11 *bis* Impact de l'évolution des taux de fraude par canal sur le taux de fraude global (en %)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

G12 Paiement par carte de proximité (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La carte conserve son statut de moyen de paiement principal du quotidien, avec des flux qui continuent de progresser en 2025 en volume comme en valeur (respectivement de + 6,5 % et + 4 %). Les paiements effectués par mobile poursuivent leur croissance (+ 38 %), et concentrent désormais 19 % du montant des paiements de proximité.

Dans un contexte d'augmentation des flux, la valeur de la fraude baisse à 475 millions d'euros (– 8,6 % par rapport à 2024). Le canal des paiements par carte sur internet reste le plus exposé même si la fraude est en net recul : il représente 70 % de la valeur de la fraude, pour seulement 27 % du montant total des opérations.

Après trois années de stabilisation, le taux de fraude sur les opérations par carte émise en France repart à la baisse et atteint un taux de 0,047 %, dorénavant le niveau historique le plus bas. Alors que les paiements de proximité et sur automate conservent un taux de fraude stable et très bas (0,011 %), les paiements sur internet voient leur taux de fraude diminuer à nouveau et de manière significative (à 0,124 % en 2025, contre 0,155 % en 2024). Ce résultat reflète les effets du plan d'action de l'Observatoire de la sécurité des moyens de paiement (OSMP) en ce domaine et les efforts déployés par l'ensemble de l'écosystème des paiements. Le taux de fraude sur les paiements à distance hors internet, qui concernent les paiements pour lesquels les clients communiquent les informations relatives à leur carte de paiement à des entreprises par téléphone ou courrier (*Mail order – telephone order*, MOTO), progresse sensiblement (à 0,322 % en 2025, contre 0,271 % en 2024). En effet, sous l'effet des mesures déployées dans le cadre de la prévention de la fraude sur les paiements par carte à distance [1] – dont la limitation des usages et la mise en œuvre d'une limite de vélocité – les flux reculent plus rapidement (– 21 %) que ceux de la fraude (– 7 %).

La baisse du taux de fraude des paiements par mobile s'accélère (– 43 % en 2025 comparé à 2024). Cette tendance durable est directement liée à un meilleur contrôle de l'enrôlement de l'utilisateur dans la solution de paiement mobile. Il s'agit du recours systématique à une authentification forte du porteur, qui fait suite au rappel des exigences réglementaires de l'Autorité bancaire européenne et de l'Observatoire en la matière. Ces progrès sont d'autant plus remarquables que ce moyen de paiement est en plein développement depuis quelques années.

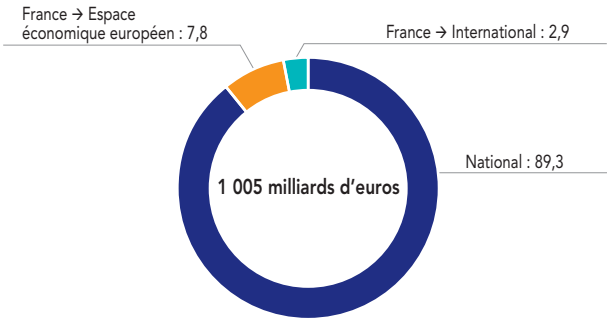
Enfin, le retrait par carte enregistre une hausse de son taux de fraude (à 0,033 % en 2025, contre 0,031 % en 2024) sous l'effet de l'augmentation des fraudes aux faux coursiers.

1 Cf. chapitre 2, section 2 « Prévention de la fraude sur les paiements par carte à distance ».

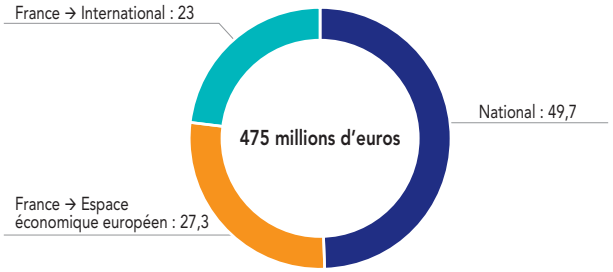
1.2.2 Répartition de la fraude par zone géographique – Cartes émises en France

G13 Cartes émises en France par zone géographique (en %)

a) Répartition du montant des opérations

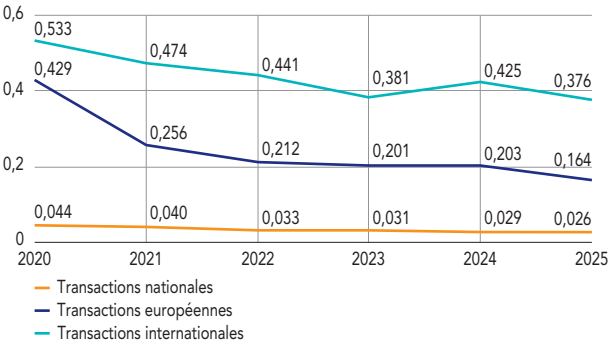


b) Répartition de la valeur de la fraude



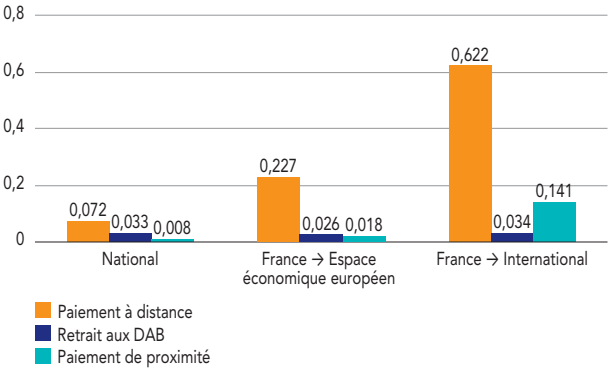
Source : Observatoire de la sécurité des moyens de paiement.

G14 Évolution des taux de fraude sur les cartes émises en France par zone géographique (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G15 Taux de fraude par zone géographique et par canal (en %)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

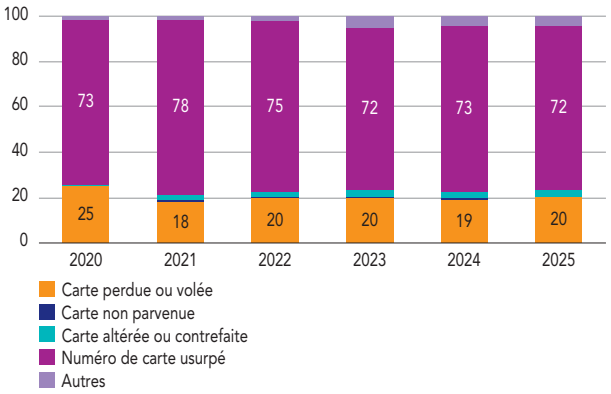
En 2025, les transactions internationales (incluant celles vers l'Espace économique européen) concentrent, de manière stable, la moitié des montants de fraude à la carte (50 % en 2025, contre 52 % en 2024), alors qu'elles ne constituent que 11 % des opérations.

Bien que les transactions par carte à l'international sont par nature plus sujettes à la fraude, leur taux de fraude continue de s'améliorer après un léger rebond en 2024 (0,376 % en 2025, contre 0,425 % en 2024, pour les transactions internationales hors Espace économique européen et 0,164 % en 2025, contre 0,203 % en 2024, pour les transactions européennes).

Les transactions internationales hors Espace économique européen sont constituées à 85 % de paiements à distance, qui sont historiquement plus fraudés que leurs équivalents nationaux. Les paiements de proximité à l'international restent aussi plus exposés à la fraude que ceux réalisés en France ou dans l'Espace économique européen, en raison de technologies moins robustes et donc plus vulnérables à la contrefaçon, comme la lecture de piste magnétique ou la prise d'empreinte physique de la carte.

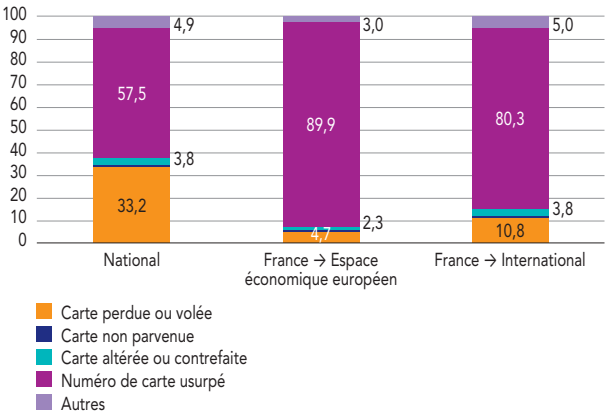
1.2.3 Répartition de la fraude par mode opératoire – Cartes émises en France

G16 Évolution de la typologie dans la valeur de la fraude depuis 2020 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G17 Typologie dans la valeur de la fraude par zone géographique en 2025 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La part de la fraude liée à l'usurpation de numéros de carte continue de représenter une part prépondérante, mais stabilisée (72 % en 2025, 73 % en 2024). La technique employée reste principalement l'hameçonnage par courriel ou par SMS.

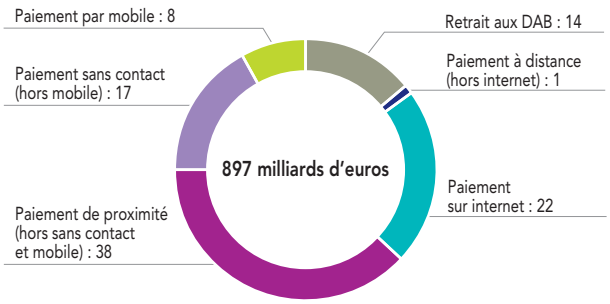
La part de la fraude liée à la perte ou au vol de carte se stabilise, toujours à un faible niveau (20 % en 2025, contre 19 % en 2024). Très logiquement, l'usage des cartes perdues ou volées se manifeste d'abord sur le territoire national (33 % de la fraude). En parallèle, la fraude par usurpation du numéro de carte se concrétise d'abord sur internet, constat partagé dans l'ensemble des zones géographiques, même si elle est encore plus prépondérante sur les transactions européennes et internationales.

Les autres types de fraude à la carte, tels que ceux mettant en œuvre des cartes non parvenues ou contrefaites, restent marginaux.

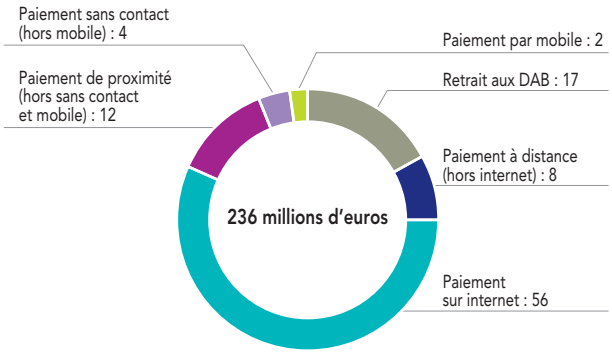
1.2.4 Répartition de la fraude sur les opérations nationales

G18 Transactions nationales par carte en montant (en %)

a) Répartition des transactions

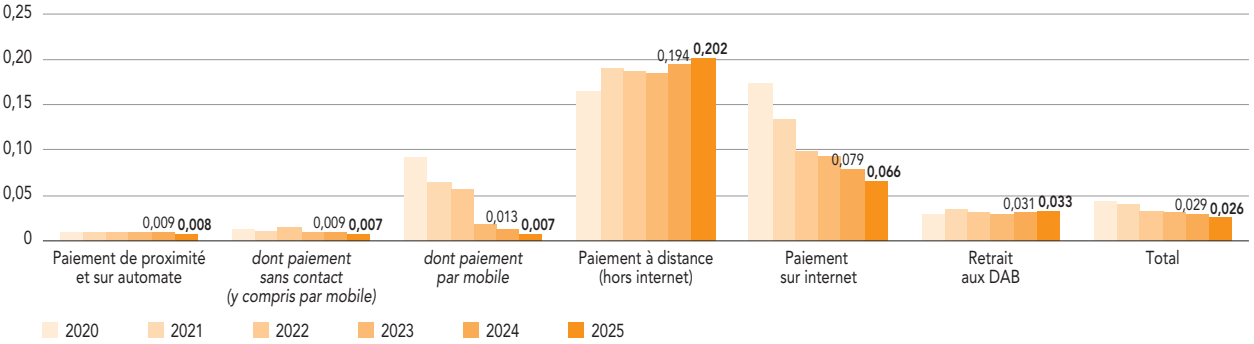


b) Répartition de la fraude



Note : DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

G19 Évolution des taux de fraude sur les transactions nationales par carte (en %)



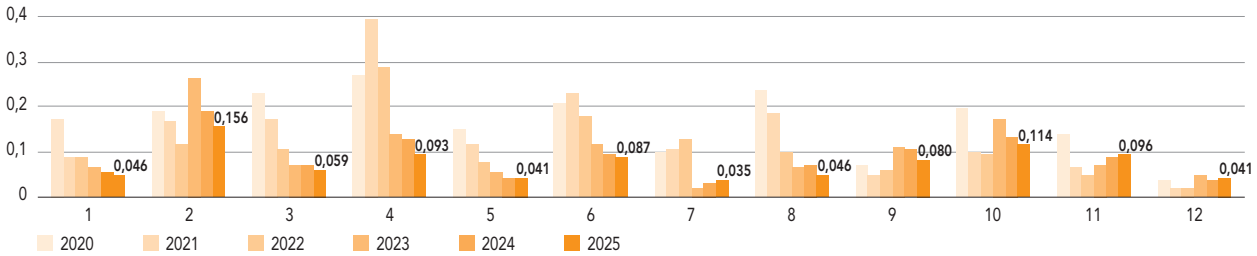
Note : DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

Les transactions nationales sont de plus en plus sécurisées, avec un taux de fraude qui atteint à nouveau un plus bas niveau historique à 0,026 % (contre 0,029 % en 2024).

Avec 152 millions d'euros de fraude, les paiements à distance (sur et hors internet) pèsent pour 64 % dans le total de la fraude nationale, quand ils ne représentent que 23 % des montants échangés. Le taux de fraude cumulé sur ces paiements recule encore de 8 % par rapport à 2024 pour s'établir à 0,072 % (contre 0,079 % en 2024), et a été divisé par plus de deux depuis 2020.

1.2.5 Focus sur la fraude aux paiements nationaux par carte sur internet

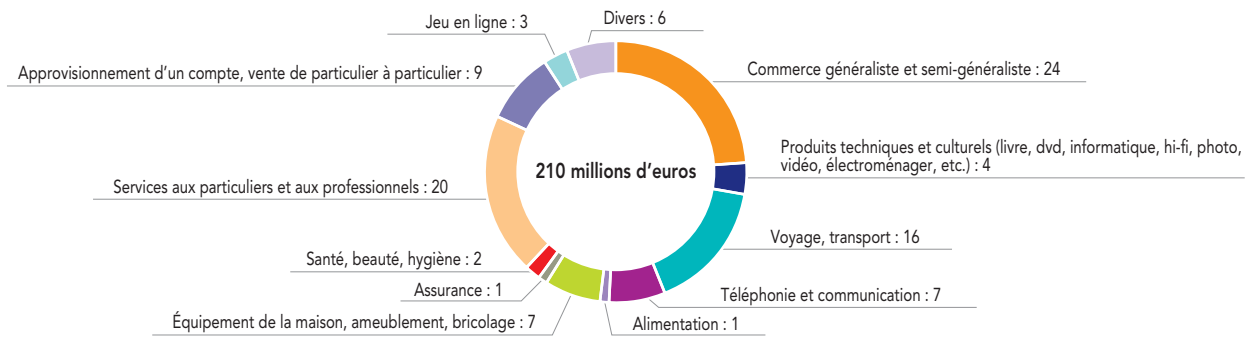
G20 Évolution du taux de fraude sur les paiements nationaux par carte sur internet, par secteur (en %)



1 Commerce généraliste et semi-généraliste
2 Services aux particuliers et aux professionnels
3 Téléphonie et communication
4 Produits techniques et culturels
5 Voyage, transport
6 Approvisionnement d'un compte, vente de particulier à particulier
7 Équipement de la maison, ameublement, bricolage
8 Jeu en ligne
9 Divers
10 Santé, beauté, hygiène
11 Alimentation
12 Assurance

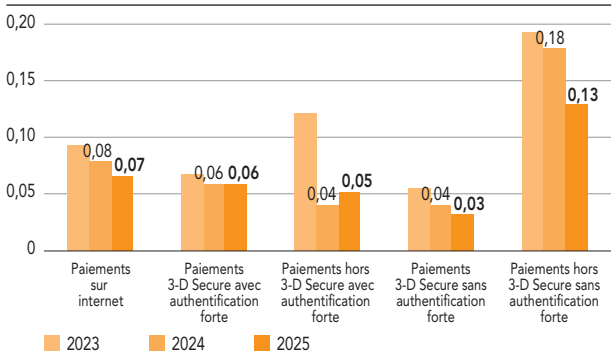
Source : Observatoire de la sécurité des moyens de paiement.

G21 Répartition de la fraude sur les paiements nationaux par carte sur internet en montant, par secteur en 2025 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G22 Taux de fraude des paiements nationaux sur internet, par canal (en %)



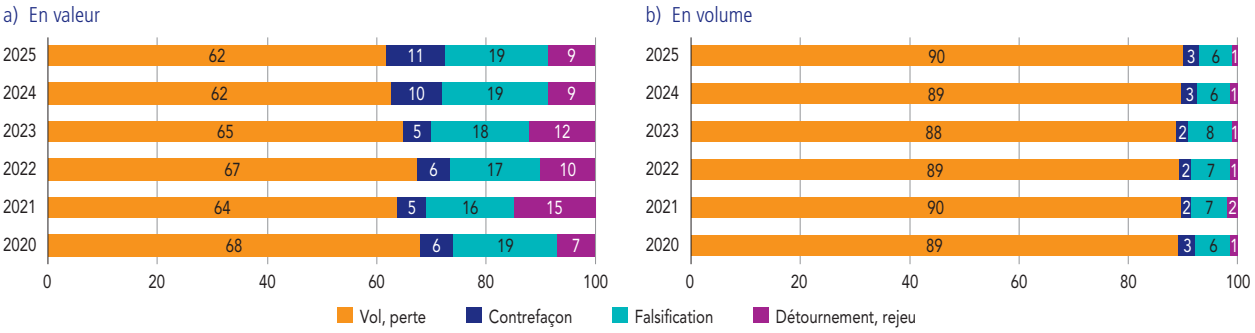
Source : Observatoire de la sécurité des moyens de paiement.

Les paiements nationaux par carte sur internet qui i) n'ont pas recours au protocole *3-D Secure* (ou protocole privatif équivalent) et ii) ne mettent pas en œuvre l'authentification forte restent proportionnellement deux fois plus fraudés que les autres canaux (trois fois plus en 2024). Ce taux de fraude structurellement plus élevé justifie les mesures mises en place depuis juin 2024 par l'Observatoire sur ce type de paiement, dont le déploiement se poursuivra dans les années à venir *(cf. chapitre 2, section 2 « Prévention de la fraude sur les paiements par carte à distance »)*. Grâce à ce plan, le taux de fraude lié à ces paiements est toutefois en nette baisse (0,13 % en 2025, contre 0,18 % en 2024). Parmi ceux-là, les paiements initiés par les commerçants (*merchant initiated transactions*, MIT) – qui s'apparentent à des prélèvements avec la carte comme support (abonnements, paiements différés ou réservations par exemple) – représentent une part majoritaire de ces flux (58 %) et de la fraude (65 %).

Par ailleurs, les dispositifs d'exemption à l'authentification forte s'avèrent toujours efficaces lorsqu'ils s'appuient sur *3-D Secure*. En effet, le taux de fraude reste deux fois inférieur aux transactions avec authentification forte (0,03 %, contre 0,06 %), ce qui souligne que les exemptions prévues continuent de bien identifier les transactions les moins risquées.

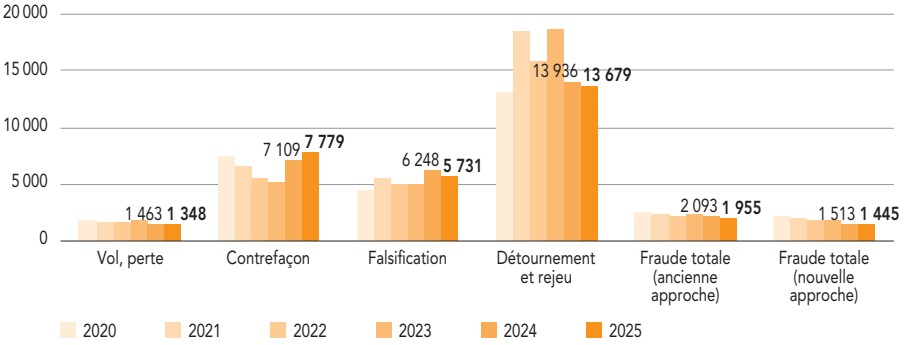
1.3 État de la fraude sur le chèque

G23 Typologie de la fraude sur le chèque (en %)



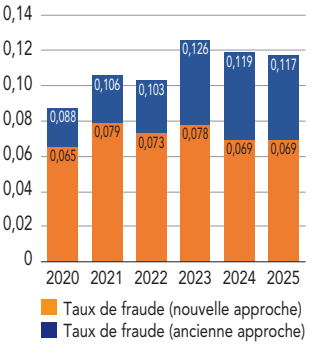
Source : Observatoire de la sécurité des moyens de paiement.

G24 Montant moyen de la fraude sur le chèque par type de fraude (en euros)



Source : Observatoire de la sécurité des moyens de paiement.

G25 Effet de la fraude déjouée sur le taux de fraude au chèque (en %)



Source : Observatoire de la sécurité des moyens de paiement.

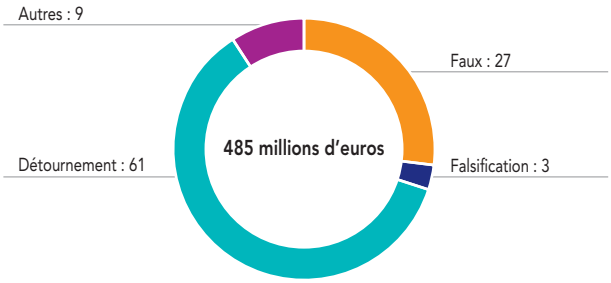
En 2025, la valeur des opérations frauduleuses continue de décroître pour s'établir à 229 millions d'euros (– 16 % par rapport à 2024). Le taux de fraude sur le chèque reste stable à 0,069 % après déduction de la fraude déjouée. Ces bons résultats attestent des effets durables de la mise en place des recommandations contre la fraude au chèque publiées en 2021 par l'Observatoire, parmi lesquelles les dispositifs de blocage ou de temporisation des remises de chèques. C'est ainsi 41 % des remises frauduleuses qui ont été neutralisées, pour 158 millions d'euros de fraude déjouée.

Le principal type de fraude reste, de loin, l'utilisation de chèques perdus ou volés, en remise directe à l'encaissement par le fraudeur ou en règlement auprès de commerçants ou de particuliers. Par conséquent, l'acheminement des chéquiers demeure un point de vulnérabilité important dans le cycle de vie des chèques.

Enfin, le chèque demeure le moyen de paiement affichant le taux de fraude le plus élevé. L'Observatoire appelle donc l'ensemble des acteurs de la filière du chèque à poursuivre les progrès et en particulier ceux qui portent sur la mise en place des recommandations liées à la protection des chèques lors de leur acheminement chez le client et à la simplification des procédures de mise en opposition pour perte ou vol *(cf. chapitre 2, section 3.1 « Recommandations de l'Observatoire contre la fraude au chèque », pour plus de détails).*

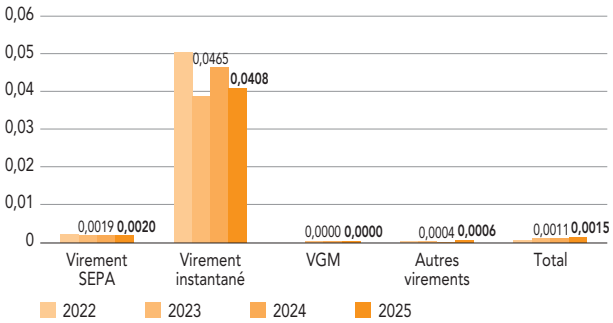
1.4 État de la fraude sur le virement

G26 Répartition de la fraude au virement en valeur par type de fraude en 2025 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

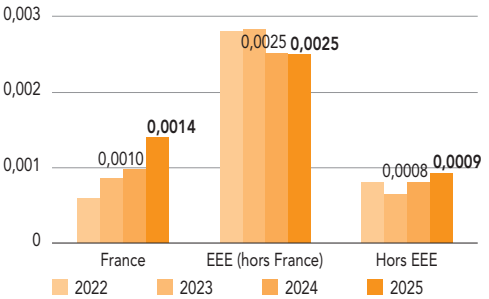
G27 Taux de fraude par type de virement (en %)



Note : SEPA, *Single Euro Payment Area* ; VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

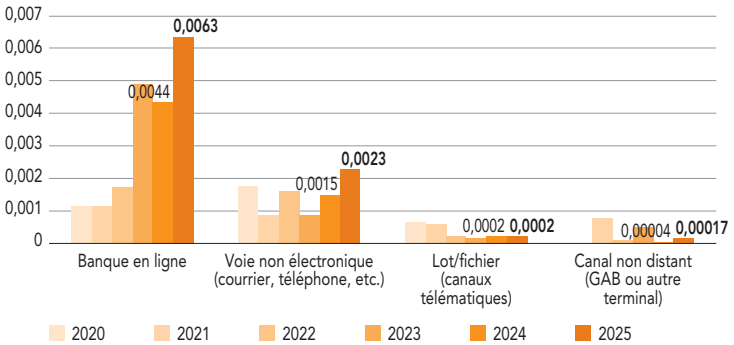
G28 Évolution du taux de fraude par zone géographique (en %)



Note : EEE, Espace économique européen.

Source : Observatoire de la sécurité des moyens de paiement.

G29 Évolution du taux de fraude sur virement par canal d'initiation (en %)



Note : GAB, guichet automatique bancaire.

Source : Observatoire de la sécurité des moyens de paiement.

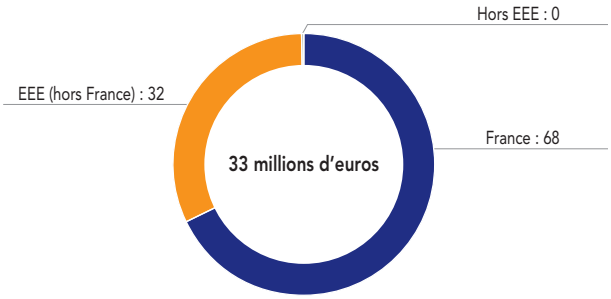
La fraude au virement progresse de 37 % en valeur pour atteindre 485 millions d'euros en 2025. Cette hausse résulte d'une évolution structurelle de la fraude : les canaux télématiques utilisés par les entreprises restent très peu exposés à la fraude (taux de fraude extrêmement faible de 0,0002 %), tandis que les fraudeurs attaquent davantage les solutions de banque en ligne (taux de fraude de 0,0063 %). Les fraudeurs mobilisent à la fois des techniques de récupération d'accès à ces solutions par hameçonnage et des techniques de manipulation pour convaincre leurs victimes de fournir une donnée sensible ou de valider une opération. Par ailleurs, les fraudeurs recourent de plus en plus aux comptes ouverts en France pour récupérer leurs fonds (+ 45 % sur le taux de fraude au niveau domestique), même si les virements européens restent proportionnellement presque deux fois plus fraudés que les virements nationaux, en dépit d'un taux de fraude en légère baisse (– 1 %).

Cela étant, le taux de fraude du virement instantané recule (0,041 % en 2025, contre 0,046 % en 2024) et se situe toujours en dessous de celui de la carte (0,049 %), alors même que ces deux moyens de paiement – majoritairement utilisés par les consommateurs – s'appuient sur des mécanismes de sécurité semblables (avec en particulier le recours aux mêmes dispositifs d'authentification forte du payeur pour les paiements en ligne).

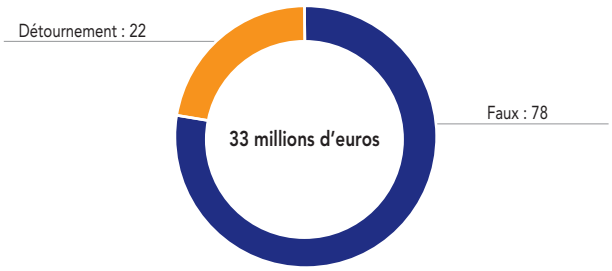
1.5 État de la fraude sur le prélèvement

G30 Répartition de la fraude au prélèvement en valeur (en %)

a) Par zone géographique



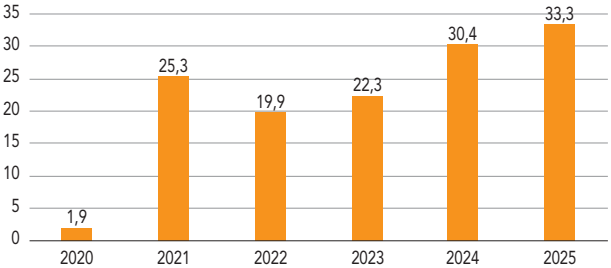
b) Par type de fraude



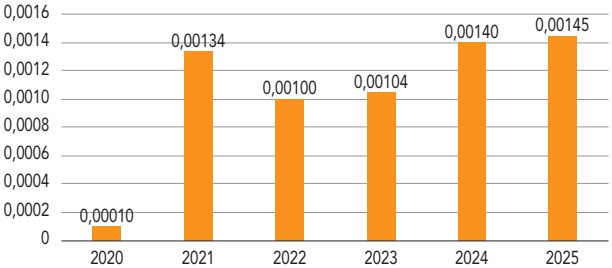
Note : EEE, Espace économique européen.
Source : Observatoire de la sécurité des moyens de paiement.

G31 Fraude au prélèvement

a) En valeur (en millions d'euros)



b) Taux (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La valeur de la fraude au prélèvement augmente de 9 % pour atteindre 33 millions d'euros, tandis que son taux de fraude reste relativement stable à 0,0014 %.

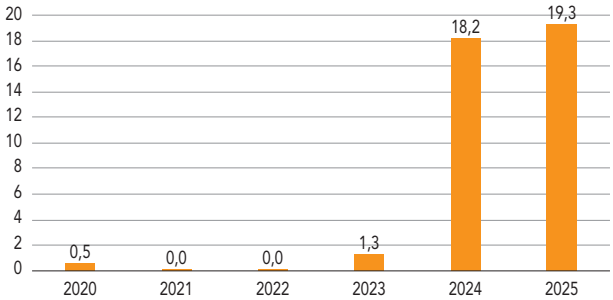
La fraude émane principalement – à 78 %, contre 96 % en 2024 – de créanciers fraudeurs, qui émettent de faux ordres. C'est-à-dire que ces créanciers ne disposent d'aucun mandat de prélèvement, ni de relation économique avec la victime. La fraude par détournement – moyen par lequel le fraudeur débiteur usurpe l'identité et le numéro de compte bancaire international (IBAN) d'un tiers pour signer un mandat de prélèvement – progresse par rapport à 2024 (22 % en 2025, contre seulement 4 % en 2024).

Les débiteurs français restent les plus touchés, même si les victimes débitrices au sein de l'Espace économique européen sont deux fois plus impactées qu'en 2024 (leur part passe ainsi de 16 % en 2024 à 32 % en 2025).

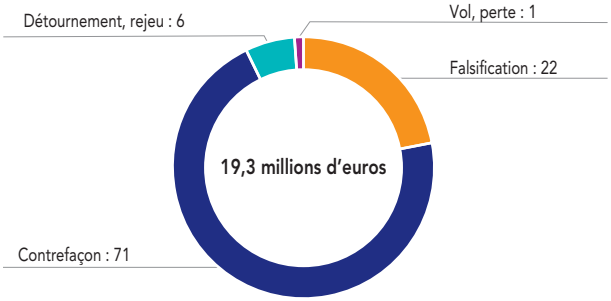
1.6 État de la fraude sur les effets de commerce

G32 Fraude sur les effets de commerce

a) En valeur (en millions d'euros)



b) Par type de fraude (en %)



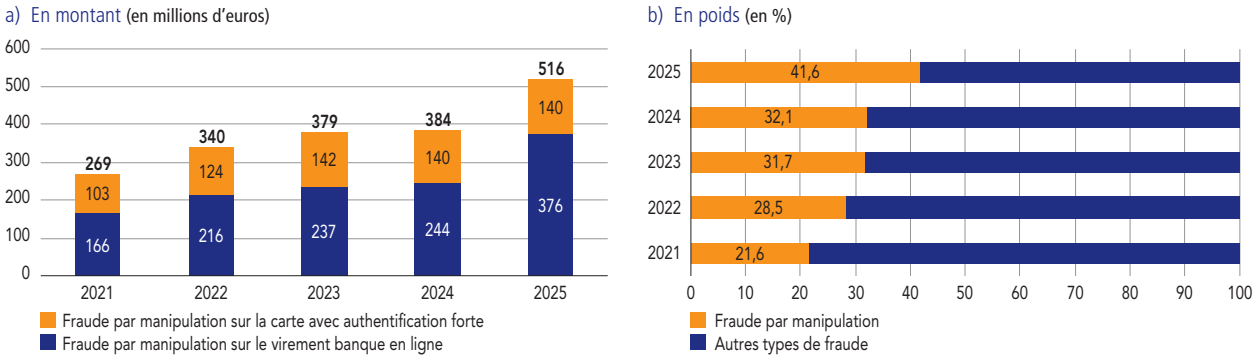
Source : Observatoire de la sécurité des moyens de paiement.

Après une progression significative en 2024, le montant de la fraude sur les effets de commerce tend à se stabiliser en 2025 (+ 6 %) pour atteindre 19,3 millions d'euros, ce qui reste marginal dans le montant total de la fraude au moyen de paiement (moins de 2 %). Le montant des flux échangés étant en recul par rapport à 2024 (– 3,5 %), le taux de fraude évolue mécaniquement à la hausse. Le montant moyen de la fraude croît et atteint 60 912 euros en 2025, contre 51 888 euros en 2024.

La typologie de la fraude reste semblable à 2024 avec une prépondérance d'effets de commerce contrefaits, c'est-à-dire des faux effets de commerce créés de toutes pièces par des fraudeurs. La falsification représente 22 % des fraudes en montant, il s'agit d'effets de commerce réguliers qui sont interceptés, puis altérés par le fraudeur.

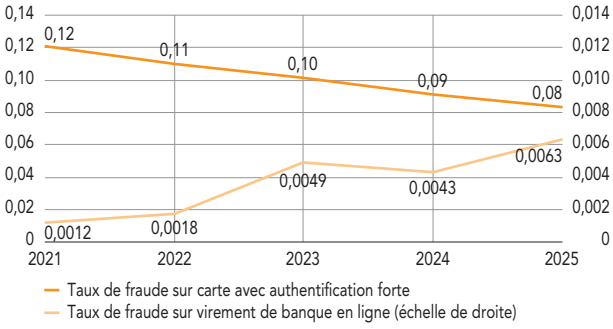
1.7 État de la fraude par manipulation

G33 Évolution de la fraude par manipulation en valeur



Source : Observatoire de la sécurité des moyens de paiement.

G34 Évolution des taux de fraude par manipulation (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La fraude par manipulation couvre les cas où le client est manipulé par le fraudeur lors d'une conversation téléphonique, souvent en usurpant l'identité du prestataire de services de paiement (fraude au faux conseiller bancaire ou au faux service anti-fraude). L'Observatoire mesure l'ampleur de cette fraude au travers d'un proxy faisant la somme des opérations frauduleuses par carte avec authentification forte et par virement de banque en ligne.

Alors que la fraude par manipulation poursuit une tendance haussière depuis 2021 (+ 43 % entre 2021 et 2024), son évolution s'accélère en 2025 avec une progression de 34 % sur l'année et atteint 516 millions d'euros. Si la fraude sur les opérations par carte fortement authentifiées reste stable à 140 millions d'euros, la fraude opérée depuis la banque en ligne augmente sensiblement. Elle passe ainsi de 244 millions d'euros en 2024 à 376 millions d'euros en 2025. Le taux de fraude des virements opérés depuis la banque en ligne repart nettement à la hausse en 2025, après une baisse ponctuelle en 2024 (0,0063 % en 2025, contre 0,0044 % en 2024). Cette augmentation importante s'explique par une accélération rapide de la valeur de la fraude (+ 54 %) dans un contexte de hausse plus mesurée des flux échangés (+ 18 %). Le taux de fraude sur les opérations par carte fortement authentifiées, quant à lui, poursuit sa décrue (0,08 % en 2025, contre 0,09 % en 2024).

Enfin, on observe que, en valeur, toute technique de fraude confondue, la part de la fraude par manipulation continue à croître pour atteindre 41,6 % en 2025 (contre 32,1 % en 2024). Face à cette tendance, l'Observatoire invite les différents acteurs de l'écosystème à i) intensifier leurs efforts de sensibilisation, ii) mettre en place des mesures concrètes pour lutter contre ce type de fraude (adaptation des parcours d'authentification sur la banque en ligne et l'application bancaire, enrichissement des outils de *scoring* et exploitation des nouveaux mécanismes de partage de données, etc.) et iii) renforcer leur coopération avec les secteurs des télécommunications et du numérique *(cf. chapitre 2, section 1 « Plan d'actions de lutte contre la fraude par manipulation »).*

ENCADRÉ

❶

Indicateurs des services du ministère de l'Intérieur sur la fraude aux moyens de paiement en 2025

Le ministère de l'Intérieur est représenté à l'Observatoire de la sécurité des moyens de paiement (OSMP) par l'Unité nationale cyber de la Gendarmerie nationale et la Direction nationale de la police judiciaire (DNPJ) de la Police nationale. Comme chaque année, ces deux services ont communiqué à l'Observatoire leurs principales observations sur les fraudes aux moyens de paiement constatées en 2025.

1. Les statistiques du ministère de l'Intérieur : un périmètre plus large que celui de l'OSMP, mais des enseignements convergents et complémentaires

Le 9 juillet 2026, le Service statistique ministériel de la sécurité intérieure (SSMSI) a publié l'atlas complet des statistiques 2025 sur l'ensemble du champ infractionnel, dont les escroqueries et les fraudes aux moyens de paiement [1].

1.1 Les sources et méthodologies du ministère de l'Intérieur se différencient de celles de l'Observatoire

La méthodologie d'enregistrement de la fraude aux moyens de paiement du SSMSI – qui est aujourd'hui agrégée systématiquement aux escroqueries – se distingue fortement de celle de l'Observatoire. En effet, en agrégeant les fraudes aux moyens de paiement aux escroqueries, la méthodologie du SSMSI retient un périmètre beaucoup plus large que celui de l'OSMP. Le périmètre du SSMSI inclut toutes les escroqueries liées aux crédits et aux investissements, les fausses ventes sur internet, les escroqueries aux rançongiciels ainsi que les escroqueries à la romance, qui ne sont pas comptabilisées par l'OSMP comme des fraudes aux moyens de paiement. Par ailleurs, le SSMSI évalue le nombre de victimes enregistrées [2] à partir des dépôts de plainte, alors que l'OSMP comptabilise les transactions frauduleuses déclarées par les prestataires de services de paiement et les réseaux de paiement par carte. Enfin, l'évaluation par le SSMSI du préjudice subi est issue du croisement des données enregistrées lors du dépôt de plainte et des données provenant des enquêtes de victimation [3]. L'OSMP s'appuie sur le montant précis des transactions frauduleuses déclarées par les établissements concernés. Ainsi, toutes ces différences de méthodologie et de périmètre empêchent le rapprochement direct des données publiées par le SSMSI et de celles publiées par l'Observatoire.

1.2 Le bilan du SSMSI et celui de l'Observatoire affichent les mêmes tendances

Malgré des méthodes et des sources différentes, un certain nombre de similitudes peuvent être mises en lumière entre le bilan publié par le SSMSI et les évolutions de la fraude aux moyens de paiement constatées par l'Observatoire.

Le nombre de victimes d'escroquerie et de fraude aux moyens de paiement enregistrées par les services de police et de gendarmerie nationales continue d'augmenter et passe ainsi de 417 300 victimes en 2024 à 448 300 en 2025 (+ 7 % entre 2024 et 2025, contre + 1,4 % entre 2023 et 2024).

Ainsi, **la fraude aux moyens de paiement repose de plus en plus sur la manipulation des victimes (par exemple, la fraude au faux conseiller bancaire, la fraude au président ou encore la fraude aux coordonnées bancaires) et continue de cibler davantage les personnes physiques que les personnes morales**. En effet, d'après l'étude du SSMSI, les personnes morales représentent 8 % des victimes en 2025, contre 16 % en 2016.

1. Cf. ministère de l'Intérieur, *Insécurité et délinquance en 2025 : bilan statistique*, édition 2026.

2. D'après l'enquête Vécu et ressenti en matière de sécurité (VRS) de 2023 du SSMSI, un peu plus d'une victime d'escroquerie sur dix porte plainte.

3. L'enquête de victimation est une enquête statistique, auprès d'un échantillon de la population, dont les questions portent sur les crimes et délits dont ont été victimes les personnes interrogées.

Le rapport souligne qu'en 2025, **plus de la moitié des escroqueries et fraudes aux moyens de paiement sont liées au numérique (53 % en 2025, contre 50 % en 2024)**. Cette part est en forte augmentation depuis 2016, puisqu'elle représentait 31 % des escroqueries. L'essor de ces infractions marque le rôle croissant du numérique dans les escroqueries et fraudes aux moyens de paiement.

Les jeunes adultes sont plus souvent victimes d'escroquerie ou de fraude aux moyens de paiement. Le nombre de victimes d'escroquerie ou de fraude aux moyens de paiement connues des services de sécurité augmente significativement à partir de 18 ans, atteignant un maximum entre 20 et 24 ans, avec un taux de 9,6 victimes pour 1 000 habitants dans cette tranche d'âge (contre 9 en 2024).

Les 18-44 ans, à eux seuls, comptent pour plus de 70 % des victimes en 2025 (contre 45 % en 2024) alors qu'ils ne constituent que 33 % de la population.

Les escroqueries aux « faux ordres de virement » (FOVI) visant les personnes morales (entreprises, administrations, collectivités territoriales) sont par ailleurs particulièrement suivies par les forces de l'ordre. Ces dernières les appréhendent comme des arnaques financières consistant à obtenir de la victime un virement qu'elle pense légitime vers un compte bancaire géré par l'escroc.

Les deux modes opératoires principaux sont :

- La fraude aux coordonnées bancaires (changement de RIB) : l'escroc usurpe l'identité d'un fournisseur de sa cible et prétexte auprès d'elle un changement de coordonnées bancaires aux fins de détourner le paiement des factures.
- La fraude au président : l'escroc usurpe l'identité d'un haut responsable de l'entreprise ou d'un de ses représentants (avocat, consultant, etc.) pour obtenir d'un collaborateur de l'entreprise la réalisation d'un virement à destination d'un nouveau compte. L'escroc insiste auprès de sa victime sur le caractère confidentiel et urgent de ce virement.

Ainsi, en 2025, pour les seuls FOVI à l'encontre des personnes morales, la Direction nationale de la police judiciaire (DNPJ) a été informée de 640 affaires pour un préjudice total de 43 millions d'euros, contre 680 [4] affaires en 2024 pour un préjudice total de 36 millions d'euros [5]. Le nombre de FOVI reste à un niveau élevé, même s'il baisse légèrement de 6 %. La valeur, quant à elle, augmente de 19 %. Le développement des outils d'intelligence artificielle, permettant de produire des courriels parfaitement falsifiés ou des voix ou des images usurpant l'identité de dirigeants d'entreprise, pourrait contribuer à entretenir la dynamique des escroqueries aux faux ordres de virement.

De leur côté, les acteurs des paiements remontent à l'Observatoire une hausse sensible de la fraude au virement par détournement en valeur (+ 62 %) comme en volume (+ 276 %).

2. Focus sur les plateformes Perceval (signaler les fraudes à la carte bancaire) et Thésée (porter plainte en ligne pour certains cas d'escroquerie)

Depuis 2018, **la plateforme Perceval** de la gendarmerie permet de recueillir auprès des utilisateurs le signalement des usages frauduleux de cartes bancaires sur internet. Les enregistrements effectués sur cette plateforme peuvent être plus facilement rapprochés des tendances constatées par l'Observatoire. Elle fait état de 206 902 signalements en 2025, contre 227 711 en 2024, soit une baisse de 9 %. Il convient de noter qu'un signalement sur la plateforme Perceval peut couvrir plusieurs transactions initiées frauduleusement à partir des mêmes données de carte usurpées.

Le taux de signalement des fraudes sur Perceval reste globalement stable. Ainsi, 39 % de la fraude à la carte sur les paiements internet telle que quantifiée par l'Observatoire aurait été signalée sur Perceval en 2025, contre 37 % en 2024 et 44 % en 2023. Les victimes ont tendance à ne déclarer que les fraudes les plus importantes : en 2025, le montant moyen par transaction frauduleuse est de 60 euros d'après les

4. Les chiffres 2024 présentés ici peuvent être légèrement supérieurs à ceux présentés dans le rapport annuel de l'OSMP de 2024. Cela s'explique par le temps de latence qui existe entre d'une part la date des faits et celle de la plainte, et d'autre part la date à laquelle la DNPJ reçoit l'information. Il peut arriver que certaines plaintes parviennent à la DNPJ plusieurs mois après les faits, ce qui oblige à réactualiser régulièrement à la hausse les totaux des années concernées.

5. Les cas remontés à la DNPJ représentent un échantillon représentatif, mais non exhaustif, des cas de FOVI à l'encontre de personnes morales commis sur le territoire.

statistiques de l'Observatoire, contre 178 euros d'après Perceval (622 euros par signalement qui comprend en moyenne 3,49 transactions).

Une seconde plateforme, appelée Thésée, ouverte en mars 2022 et gérée par l'Office anti-cybercriminalité (OFAC) de la Police nationale, permet aux particuliers victimes de certains types d'escroquerie en ligne de déposer plainte à distance [6]. En 2025, cette plateforme a recensé 55 300 dépôts de plainte relatifs à une escroquerie ou une fraude aux moyens de paiement. Cela représente 12 % du total des victimes d'escroquerie ou de fraude aux moyens de paiement recensées par le SSMSI, taux stable par rapport à 2024 (11 %).

L'Observatoire rappelle aux victimes l'utilité de déclarer leurs fraudes sur les plateformes Perceval ou Thésée, ou, à défaut d'éligibilité, de se rendre au commissariat de police ou à la gendarmerie pour porter plainte. Les forces de l'ordre peuvent ainsi disposer des informations nécessaires aux démantèlements des réseaux de fraudeurs.

3. Les piratages de terminaux de paiement et de retrait : en baisse depuis plusieurs années

Les piratages peuvent cibler des automates de paiement ou de retrait d'argent (distributeurs automatiques de billets [DAB], distributeurs automatiques de carburant, automates d'autoroutes, dispositifs de règlement de parking, etc.). Les terminaux de paiement, y compris les terminaux portatifs ou les boîtiers d'acceptation sans contact, peuvent également être compromis ou détournés de leurs finalités, par exemple en étant remplacés par un dispositif d'acceptation frauduleux.

La fraude par *skimmer* [7] consiste à récupérer, par le biais de terminaux de paiement trafiqués ou usurpés, les données bancaires stockées sur la bande magnétique de la carte. Dans les deux cas, les données de la carte ainsi obtenues par les réseaux de délinquance sont ensuite réencodées sur des cartes à piste magnétique. Ces cartes contrefaites sont alors utilisées pour des paiements de proximité ou des retraits pour lesquels la lecture de la puce est facultative, comme pour les paiements aux péages autoroutiers ou dans les pays où la carte à puce est encore peu déployée (pays d'Amérique ou d'Asie du Sud-Est). Ces données usurpées peuvent aussi être utilisées pour des paiements à distance, principalement sur les sites de e-commerce non européens qui n'ont pas mis en œuvre l'authentification forte du porteur de la carte.

La fraude au ***shimming*** [8], qui repose sur des procédés similaires au ***skimming***, vise à récupérer les données contenues dans la puce de la carte. La très forte complexité de cette technique de fraude a limité ce type d'attaques jusqu'à présent.

Les chiffres du Groupement des Cartes Bancaires CB mettent en lumière une baisse générale des piratages des terminaux de paiement et de retrait sur ces dernières années. Néanmoins, les gestionnaires de station-essence, les gestionnaires de DAB et les commerçants doivent rester vigilants quant au risque de tentative de substitution d'un terminal de paiement légitime par un terminal compromis ou de toute installation par un tiers d'un dispositif externe frauduleux (lecteur, caméra, clavier, etc.).

6. La démarche en ligne sur la plateforme Thésée se substitue à un dépôt de plainte effectué en présentiel au commissariat de police ou en gendarmerie pour un certain nombre d'escroqueries (faux site de vente, fausse location en ligne, escroquerie aux petites annonces, escroquerie à la romance, chantage en ligne, piratage de boîte e-mail et rançongiciel). Pour le reste des escroqueries (celles dites « au président », au changement de RIB, au faux conseiller bancaire, au faux service de support informatique ou à l'investissement), le dépôt de plainte doit être effectué en présentiel, au commissariat ou en unité de gendarmerie. Les données issues de Thésée sont intégrées au nombre de victimes d'escroquerie ou de fraude aux moyens de paiement publié par le SSMSI le 9 juillet 2026 dans son bilan statistique sur l'insécurité et la délinquance en 2025.

7. Matériel se glissant dans la fente d'un automate tout en laissant de l'espace pour qu'une carte bancaire puisse y être glissée naturellement. Une copie des données de la piste magnétique sera alors réalisée par le matériel sans que cela n'ait une quelconque incidence sur le bon fonctionnement de la carte bancaire.

8. Matériel un peu similaire au *skimmer* dans son intégration dans un automate mais qui intercepte les données de la puce de la carte bancaire, dont son code confidentiel.

2

ACTIONS CONDUITES PAR L'OBSERVATOIRE AU TITRE DE LA PRÉVENTION DE LA FRAUDE

2.1 Plan d'action de lutte contre la fraude par manipulation

2.1.1 Contexte des travaux

La directive européenne n° 2015/2366 du 25 novembre 2015 sur les services de paiement, dite « DSP2 », a renforcé les exigences réglementaires en matière de sécurité des paiements à distance. L'Observatoire a accompagné sa mise en application, notamment dans le cadre d'un plan de migration pour la mise en œuvre de l'authentification forte, à la fois pour les paiements par carte sur internet et aussi pour les virements depuis la banque en ligne.

Les mesures techniques se sont donc renforcées en matière de sécurisation des paiements. Ce renforcement a conduit à l'évolution des scénarios de fraude. Les fraudeurs privilégient désormais la manipulation de leur victime. Par exemple, dans le cadre de la fraude dite au « faux conseiller bancaire », le fraudeur se fait généralement passer pour un conseiller bancaire ou un service anti-fraude de la banque. Son objectif est d'amener la victime à valider des opérations frauduleuses, par le biais d'une authentification forte, sous le prétexte de les annuler ou de les bloquer. Pour entrer en contact avec leurs victimes et usurper l'identité des prestataires de services de paiement (PSP), les fraudeurs passent par les moyens de communication bien connus du grand public (appels téléphoniques, applications de messagerie, réseaux sociaux, etc.).

La lutte contre ce type de fraude nécessite une approche globale, tenant compte des leviers utilisés par les fraudeurs :

- Sensibiliser les utilisateurs est un sujet clé, face à des attaques qui les ciblent directement. L'enjeu est à la fois d'éviter la communication en amont de données sensibles, notamment lors de campagnes d'hameçonnage, qui sont ensuite réutilisées lors des tentatives de manipulation, et de permettre aux utilisateurs de détecter les tentatives de manipulation et de savoir comment réagir.
- Au niveau des prestataires de services de paiement, renforcer l'information et l'interaction avec le client constitue un enjeu primordial pour contrer la manipulation. Il convient ainsi d'offrir différentes occasions de faire prendre conscience au client, tout au long de son parcours de paiement, qu'il peut s'agir d'une fraude. Pour les PSP, l'objectif est aussi d'adapter leurs outils de gestion des risques afin de mieux identifier ces tentatives et temporiser voire bloquer les opérations quand cela s'avère nécessaire.
- Enfin, il s'agit de mieux sécuriser les canaux de communication par lesquels les utilisateurs sont confrontés à différentes formes d'usurpation : faux mails, sms ou messages instantanés ; sites miroirs ; fausses publicités en ligne. Une telle ambition nécessite pour l'Observatoire de développer la coopération avec des acteurs qui ne relèvent pas *stricto sensu* du secteur des paiements, tels que les opérateurs de télécommunications ou de réseaux sociaux.

2.1.2 Les actions des prestataires de services de paiement

Les techniques de manipulation sont de plus en plus sophistiquées et tendent à altérer la capacité de l'utilisateur à être réceptif aux messages qui lui sont adressés. Pour y remédier, les prestataires de services de paiement sont confrontés à l'impératif d'arriver à protéger leurs clients malgré eux. Il s'agit à la fois d'approfondir les mécanismes de prévention de la fraude déjà en place afin de continuer à accroître leur efficacité face aux évolutions de la menace, tout en tirant parti des évolutions technologiques et réglementaires.

2.1.2.1 Renforcer l'efficacité des mesures de prévention existantes face au risque de fraude par manipulation

Un certain nombre de recommandations en matière de prévention de la fraude émises par le passé par l'Observatoire constituent encore aujourd'hui des leviers d'action contre la fraude par manipulation. C'est le cas notamment :

- Des recommandations portant sur l'usage de l'intelligence artificielle (IA) à des fins de lutte contre la fraude *(cf. section 2.4 de ce chapitre, tableau 8)*. Celles-ci invitent les établissements à enrichir en continu leurs systèmes de détection basés sur l'IA, notamment en matière de périmètre de données. À ce titre, l'exploitation de métadonnées issues du téléphone de l'utilisateur, permettant de déterminer s'il est en communication avec un tiers (que ce soit par échange téléphonique ou par service de visioconférence) au moment de la validation d'une opération atypique, est une piste à considérer.
- Des recommandations portant sur la sécurité des paiements en temps réel *(cf. section 2.4 de ce chapitre, tableau 12)*, en particulier les recommandations n° 3 et 4. La première invite les prestataires de services de paiement à faire usage de mesures de paramétrage des conditions d'utilisation de ces paiements (notamment en matière de plafonds). La recommandation n° 4, quant à elle, invite à détecter l'enchaînement d'opérations à risque (par exemple : clôture de comptes d'épargne, création d'un nouveau bénéficiaire et augmentation de plafond précédant une demande d'émission de virement d'un montant inhabituel).
- De la mise en place du fichier national des comptes signalés pour motif de fraude *(cf. section 2.3.2 de ce chapitre, « Recommandations concernant la fraude aux paiements SEPA »* [1]*)*. Ce fichier constitue un levier supplémentaire de lutte contre les fraudes par manipulation, en permettant aux prestataires de services de paiement de partager des informations sur les comptes utilisés par les fraudeurs.

L'Observatoire suivra la mise en œuvre de ces recommandations, dans une logique continue d'amélioration des mécanismes de détection de la fraude et de renforcement des capacités de temporisation, voire de blocage, des opérations présentant un risque de fraude par manipulation manifestement élevé.

2.1.2.2 Les apports des recommandations sur les modalités de remboursement des opérations de paiement frauduleuses

Les recommandations relatives aux modalités de remboursement des opérations de paiement frauduleuses ont été publiées par l'Observatoire le 16 mai 2023 et dans son rapport annuel 2022. Cet ensemble de treize recommandations a été constitué dans un contexte de développement important des cas de fraude utilisant des techniques de manipulation de la victime. Il a pour objectif de clarifier les conditions d'application du cadre législatif en matière de remboursement des opérations contestées et de renforcer les dispositifs de prévention de la fraude.

Après dix-huit mois d'application, le bilan des recommandations dressé dans le rapport annuel 2024 faisait état notamment i) d'un renforcement de la sécurité des parcours de paiement, en particulier sur internet et sur les applications bancaires, ii) d'une amélioration du traitement des contestations pour motif de fraude et iii) du remboursement systématique et immédiat des paiements frauduleux n'ayant pas fait l'objet d'authentification forte. En revanche, il soulignait les efforts à poursuivre concernant le remboursement des paiements frauduleux par virement sans authentification forte.

En lien avec l'Autorité de contrôle prudentiel et de résolution (ACPR), la Banque de France continuera le suivi des pratiques individuelles des établissements, et en particulier de ceux qui présentent encore des marges de progression dans l'application des recommandations. Pour ce faire, la Banque de France s'appuiera notamment sur des indicateurs statistiques de qualification des contestations et de remboursement. Ceux-ci seront rassemblés par une collecte de données menée pour le compte de l'Observatoire auprès des principaux établissements actifs en France.

1 SEPA – *Single Euro Payment Area*, espace unique de paiement en euros.

T1 Recommandations de l'Observatoire relatives au remboursement des cas de fraude *(pour mémoire : recommandations émises dans le rapport annuel 2022)*

Recommandations	Destinataires
1 – Délai maximum des investigations Les prestataires de services de paiement sont invités à mettre en œuvre les investigations dès la réception de la contestation, en prenant en compte les éventuels éléments de description fournis par l'utilisateur (tels que précisés par la recommandation n° 8), et à en limiter la durée à 30 jours, sauf situation exceptionnelle.	Prestataires de services de paiement
2 – Information du client en cas de reprise des fonds En cas de remboursement susceptible de donner lieu à une reprise de fonds ultérieure en fonction du résultat d'investigations engagées, le prestataire de services de paiement informe son client de cette éventualité au moment du remboursement, et veille à ne pas procéder à la reprise des fonds dans un délai excédant 30 jours à compter de la date à laquelle le remboursement a été effectué, sauf situation exceptionnelle.	Prestataires de services de paiement
3 – Justification du refus de remboursement Lorsque le prestataire de services de paiement refuse le remboursement ou procède à la reprise des fonds, il veille à informer le client de cette décision et lui en communique le motif, en prenant soin le cas échéant de joindre les éléments qui la justifient (par exemple, mandat de prélèvement, éléments transmis par le commerçant, preuve de négligence grave, etc.). En outre, il détaille dans cette même communication les modalités suivant lesquelles une réclamation peut être déposée.	Prestataires de services de paiement
4 – Principes applicables aux opérations sans authentification forte Lorsqu'un utilisateur du service de paiement conteste une ou plusieurs opérations qu'il nie avoir autorisées et que ces opérations n'ont pas été authentifiées de manière forte, le prestataire de services de paiement du payeur rembourse sans délai le montant de ces opérations, sauf lorsqu'il a de bonnes raisons de soupçonner une fraude de l'utilisateur lui-même. Ce soupçon de fraude ne peut résulter de la seule utilisation de l'instrument de paiement. Ce remboursement immédiat ne fait pas obstacle à la reprise ultérieure des fonds lorsque le prestataire de services de paiement réunit des éléments prouvant soit que l'opération a été autorisée (par exemple, par l'existence d'un mandat de prélèvement SEPA), soit qu'une fraude a été commise par l'utilisateur lui-même. En revanche, la négligence, même grave, commise par le payeur ne peut fonder le refus de remboursement d'une opération qui n'a pas été authentifiée de manière forte. Dans le cas particulier des paiements initiés par le bénéficiaire (prélèvement ou paiement par carte de type MIT – *merchant initiated transaction,* paiements initiés par les commerçants), le payeur bénéficie en outre d'un droit à remboursement immédiat dans un délai de huit semaines qui suit le débit en compte : • pour le prélèvement, ce remboursement est sans condition, indépendamment de l'existence ou non d'un mandat de prélèvement ; • pour le paiement par carte ordonné par le bénéficiaire, si l'autorisation donnée n'indiquait pas le montant exact de l'opération de paiement et si le montant de l'opération dépassait le montant auquel le payeur pouvait raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances propres à l'opération.	Prestataires de services de paiement
5 – Principes applicables aux opérations réalisées avec une application mobile se substituant à l'instrument de paiement Lorsque l'utilisateur du service de paiement conteste une opération de paiement qu'il nie avoir autorisée et qui a été réalisée au moyen d'une solution mobile pour laquelle l'enrôlement de l'instrument de paiement n'a pas donné lieu à authentification forte, le prestataire de services de paiement du payeur procède sans délai au remboursement du montant de cette opération.	Prestataires de services de paiement

T1 Recommandations de l'Observatoire relatives au remboursement des cas de fraude (suite)

Recommandations	Destinataires
6 – Principes applicables aux opérations authentifiées de manière forte Lorsqu'un client conteste une opération de paiement qu'il nie avoir autorisée et que cette opération a été authentifiée de manière forte, le prestataire de services de paiement doit procéder dans le délai d'un jour ouvré à une première analyse de cette opération. Cette analyse vise à apprécier, en prenant en compte les trois familles de paramètres mentionnées ci-après, si l'utilisateur est susceptible d'avoir consenti à l'opération ou s'il s'agit d'une opération non autorisée : • les paramètres techniques associés à l'opération (tels que l'origine de la transaction, le terminal utilisé pour l'achat ou la connexion à la banque en ligne, la localisation géographique, etc.), pour évaluer la possibilité que l'utilisateur en soit à l'origine ; • les modalités de l'authentification forte mise en œuvre (telles que le type de solution – intégrité des facteurs d'authentification et du canal de communication –, la preuve d'une utilisation précédente de la solution par l'utilisateur ou, au contraire, du caractère récent de l'enrôlement, etc.), pour s'assurer du rôle effectif de l'utilisateur ; • les éléments de contexte dont il dispose : tels que les informations délivrées à l'utilisateur lors de l'authentification *(cf. recommandation n° 11)* ; les éventuelles alertes liées à l'opération et adressées à l'utilisateur par différents canaux de communication ; les éléments rapportés par l'utilisateur *(cf. recommandation n° 8)*, tels que les procédés manipulatoires auxquels il a pu être confronté. À l'issue de cette première analyse : • soit le prestataire de services de paiement constate que l'opération n'a pas été autorisée ou a un doute sur le consentement donné à l'opération, auquel cas il procède sans délai au remboursement de la transaction ; • soit le prestataire de services de paiement dispose de bonnes raisons de soupçonner une fraude de l'utilisateur et il communique ses raisons à la Banque de France, auquel cas il peut refuser de rembourser immédiatement la transaction dans les conditions prévues à la recommandation n° 3 ; • soit le prestataire de services de paiement a suffisamment d'éléments de preuve pour considérer que l'opération a été autorisée par l'utilisateur ou que ce dernier a été gravement négligent ou qu'il n'a pas satisfait intentionnellement à ses obligations, auquel cas il peut refuser le remboursement de l'opération contestée au client, dans les conditions prévues à la recommandation n° 3. Dans les deux premiers cas, et à partir notamment des mêmes critères susmentionnés et des éléments nouveaux qu'aurait pu rapporter l'utilisateur, le prestataire de services de paiement est invité à poursuivre si nécessaire les investigations dans les conditions prévues aux recommandations n° 1 à 3 en vue de déterminer le droit à remboursement de l'utilisateur.	Prestataires de services de paiement
7 – Bonnes pratiques pour la sécurité des moyens de paiement Les consommateurs doivent s'efforcer de rester vigilants quant à la préservation de la sécurité des données de sécurité associées à un instrument de paiement (mot de passe, code confidentiel, cryptogramme, etc.), en respectant les bonnes pratiques en la matière : • ne jamais communiquer ces données à un tiers ; • ne pas conserver ces données de sécurité sur quelque support que ce soit, physique (carnet, post-it, etc.) ou informatique (messagerie électronique, disque dur, portable, etc.) ; • ne pas répondre aux sollicitations de personnes se présentant comme des collaborateurs des prestataires de services de paiement (conseillers bancaires, service de lutte contre la fraude, etc.). Toujours utiliser un canal sécurisé et connu pour établir un contact avec son prestataire de services de paiement. Ne jamais ouvrir un lien reçu par messagerie électronique ou SMS dont l'origine n'est pas sûre ; • ne jamais confier son instrument de paiement à une tierce personne (proche, coursier, etc.) : • être attentif aux communications de son prestataire de services de paiement et des autorités en matière de sécurité. Il est rappelé que le personnel du prestataire de services de paiement ne sera jamais amené à demander ces informations en cas d'appel de son client et n'en a pas besoin pour annuler une opération frauduleuse. En outre, les consommateurs sont invités à privilégier la solution d'authentification la plus sûre proposée par leur prestataire de services de paiement, dès lors qu'ils sont en capacité de l'utiliser. Il s'agit généralement des solutions reposant sur un élément matériel robuste comme l'application bancaire sur un *smartphone* (solution majoritaire en France) ou un dispositif physique autonome mis à disposition par le prestataire de services de paiement (lecteur de carte, clé USB, etc.).	Consommateurs

T1 Recommandations de l'Observatoire relatives au remboursement des cas de fraude (suite)

Recommandations	Destinataires
8 – Devoir de transparence de la part des victimes de fraude Lors des démarches de déclaration auprès de leur prestataire de services de paiement ou des forces de l'ordre (qu'il s'agisse d'une déclaration sur l'honneur, des démarches en ligne sur les plateformes Perceval ou Thésée, ou du dépôt de plainte au commissariat de police ou dans une unité de gendarmerie), les consommateurs et leurs représentants veillent à fournir l'ensemble des éléments dont ils disposent concernant la fraude dont ils ont été victimes. Les utilisateurs veillent notamment à fournir tous les éléments connus sur : • la nature et le contexte de l'opération : par exemple leur niveau de connaissance du bénéficiaire, les procédés techniques ou manipulatoires que le fraudeur est supposé avoir mobilisés, l'instrument et les terminaux utilisés pour l'opération de paiement, les messages ou appels reçus, les actions réalisées sous le coup d'une manipulation par le fraudeur, etc. • Les actions entreprises une fois la fraude découverte : par exemple le blocage de l'instrument, le récépissé des démarches Perceval ou Thésée, le dépôt de plainte auprès des forces de l'ordre, etc.	Consommateurs
9 – Application d'une authentification forte lors de l'accès à la banque en ligne depuis un nouveau point d'accès à internet ou un nouveau terminal Les prestataires de services de paiement sont invités à exiger une authentification forte en cas de consultation des comptes depuis la banque en ligne ou l'application mobile depuis un terminal et/ou un point d'accès à internet qui n'a pas été précédemment utilisé par le client.	Prestataires de services de paiement
10 – Modalités d'enregistrement des IBAN bénéficiaires de virements [a)] Les prestataires de services de paiement sont invités à indiquer clairement, à chaque ajout d'un bénéficiaire de virement, si un contrôle de concordance entre IBAN et nom du bénéficiaire a été mis en œuvre. À défaut, il doit être précisé à l'utilisateur que le champ « Nom du bénéficiaire » est exclusivement destiné à faciliter le suivi des opérations par le client qui émet des virements, et que son contenu ne fait l'objet d'aucun contrôle de concordance avec l'identité du titulaire de l'IBAN du bénéficiaire. Par ailleurs, les prestataires de services de paiement établis en France sont encouragés à explorer par anticipation la possibilité d'implémenter au plus tôt un service de confirmation du bénéficiaire tel qu'envisagé par la Commission européenne dans sa proposition de révision du règlement SEPA.	Prestataires de services de paiement
11 – Information et options présentées à l'utilisateur au moment de l'authentification forte Les prestataires de services de paiement veillent à présenter à l'utilisateur, à chaque étape du processus d'authentification, une information explicite quant à la nature de l'opération et mentionnant notamment le montant, le bénéficiaire, le caractère unique ou récurrent de l'opération, la périodicité dans le cas d'une opération récurrente, ainsi que le caractère irrévocable de la validation de l'ordre de paiement. Dans le cas d'un premier virement vers un compte donné, lorsque la concordance entre l'identité du bénéficiaire et l'IBAN fournis n'a pas fait l'objet d'un contrôle, le parcours d'authentification le rappelle explicitement. Par ailleurs, les prestataires de services de paiement veillent à ce que le parcours d'authentification propose de manière explicite une option permettant de refuser l'opération.	Prestataires de services de paiement
12 – Simplicité d'accès aux procédures de blocage des instruments de paiement Les prestataires de services de paiement mettent à disposition de leurs utilisateurs des mécanismes de blocage pour chacun des instruments de paiement et veillent à ce qu'ils soient facilement accessibles, gratuits et utilisables à tout moment.	Prestataires de services de paiement
13 – Rôle des fournisseurs de services et technologies de l'information Les acteurs du secteur des technologies de l'information (opérateurs de téléphonie, hébergeurs de contenu, éditeurs de sites de référencement, moteurs de recherche, fournisseurs de services de messagerie, etc.) veillent à protéger les utilisateurs contre les risques d'usurpation d'identité et d'atteinte à l'intégrité et la confidentialité de leurs données. Ils œuvrent à empêcher l'utilisation de techniques frauduleuses telles que l'hameçonnage, le *spoofing* (usurpation du numéro d'appelant) ou le *SIM-swapping* (duplication d'une carte SIM au bénéfice du fraudeur).	Fournisseurs de services et technologies de l'information

a) Depuis le 9 octobre 2025, le service de vérification du bénéficiaire a été rendu obligatoire par la réglementation européenne (Règlement (UE) n° 260/2012 du 14 mars 2012 modifié par le règlement (UE) 2024/886 du 13 mars 2024) et permet ainsi de limiter les fraudes et les erreurs lors de la saisie des IBAN (*international bank account numbers*, numéros de compte bancaire internationaux). Les prestataires de services de paiement doivent néanmoins veiller à informer explicitement leurs clients lorsque le service de vérification du bénéficiaire n'est pas disponible (par exemple virements internationaux, virements en devises, etc.). Ils sont également invités à rappeler les bons réflexes auprès de leurs clients (revoir régulièrement les listes de leurs bénéficiaires, réaliser un contre-appel en cas de doute, ne pas répondre aux démarches non sollicitées portant sur l'enregistrement de leurs bénéficiaires, etc.).

Note : SEPA – *Single Euro Payment Area*, espace unique de paiement en euros ; IBAN – *international bank account numbers*, numéros de compte bancaire internationaux ; *spoofing*, usurpation de numéro d'appelants ; *SIM-swapping*, duplication d'une carte SIM.

Source : Observatoire de la sécurité des moyens de paiement.

2.1.3 La coopération avec les secteurs des télécommunications et du numérique

En 2023, la composition de l'Observatoire a en conséquence été étendue aux acteurs du secteur des télécommunications : d'une part, les principales organisations professionnelles de ce secteur (Fédération française des télécoms – FFTélécoms, Association française pour le développement des services et usages multimédias multi-opérateurs – AF2M), et d'autre part l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). En lien avec celles-ci, l'Observatoire suit la mise en œuvre du mécanisme d'authentification des numéros (MAN) [2], en vue d'éviter l'usurpation de numéros de téléphone par les fraudeurs pour les appels qu'ils passent à leurs victimes. En outre, l'Observatoire accompagne le secteur des télécommunications et les PSP dans la mise en œuvre des recommandations émises dans son rapport annuel 2024. Celles-ci visent principalement à prévenir l'usage illégitime des canaux téléphoniques traditionnels et à renforcer la coopération entre les PSP et le secteur des télécommunications *(cf.* « Recommandations visant à renforcer la sécurisation des canaux de télécommunications » *infra*).

Toutefois, la sécurisation croissante du canal téléphonique conduit les fraudeurs à exploiter les fonctionnalités aujourd'hui proposées par les applications de messagerie instantanée ainsi que par les réseaux sociaux. C'est à ce titre que l'Observatoire a publié, dans son rapport annuel 2024, une feuille de route pour le développement d'une coopération avec les principaux acteurs du numérique, tels qu'Apple, Google, Meta ou encore TikTok *(cf.* feuille de route à destination des acteurs du numérique *infra*).

Contre les fraudes par manipulation, la coopération renforcée avec les secteurs des télécommunications et du numérique est complémentaire aux autres mesures de prévention et de sensibilisation. Celles-ci sont suivies et promues par l'Observatoire (par exemple l'amélioration des parcours d'authentification forte, la vérification du bénéficiaire, ou le fichier national des comptes signalés pour risque de fraude). Cette coopération renforcée doit notamment déboucher sur des actions concrètes de la part des acteurs du numérique (tels que les plateformes et réseaux sociaux) pour limiter les risques de fraude et sécuriser l'environnement numérique.

2.1.3.1 Vue d'ensemble des progrès observés

La coopération avec les acteurs des télécommunications a permis d'importants progrès dans la prévention de la fraude par manipulation, même si certaines actions restent à concrétiser. En complément du mécanisme d'authentification des numéros (MAN) qui est largement opérationnel depuis janvier 2025, plusieurs actions devraient encore renforcer la sécurité des communications :

- Le masquage des numéros de téléphone mobile français (affichés en numéro inconnu) lorsque les appels sont passés depuis l'étranger (itinérance) et qu'ils ne peuvent pas être authentifiés, ainsi que l'impose l'Arcep dans son plan national de numérotation modifié en décembre 2025 ;
- L'expérimentation, à compter de juin 2026, du mécanisme *Do Not Originate* (DNO) pour les numéros identifiés par les PSP comme étant destinés uniquement à recevoir des appels : ce mécanisme complète le MAN en renforçant la protection contre l'usurpation des numéros les plus sensibles, par exemple les numéros des centres d'opposition aux cartes bancaires perdues ou volées ;
- La mise en place, après la réalisation d'une étude de faisabilité préalable, d'un numéro unique permettant aux utilisateurs de services de paiement, en cas de suspicion de fraude, de solliciter leur PSP. Cette solution s'inspire du modèle appliqué au Royaume-Uni, avec le numéro 159, promu par l'initiative *Stop Scams UK*.

Par ailleurs, l'Observatoire a engagé un premier dialogue avec les acteurs du numérique, principalement Google, Meta et TikTok. Ces derniers se sont montrés sensibles et favorables à cette démarche. Ces travaux doivent s'inscrire dans la durée. Cette coopération doit inciter les acteurs du numérique à renforcer leurs mécanismes de surveillance et de contrôle de leurs publications avant toute diffusion. Elle vise également à renforcer l'échange d'informations sur les usages et contenus frauduleux, grâce à l'exploitation croisée des éléments dont disposent d'une part les PSP (dans le cadre notamment des dossiers de fraude qu'ils instruisent et de leurs outils contre la fraude), et d'autre part les acteurs du numérique (par le biais non seulement des signalements de leurs utilisateurs mais également des résultats de leur analyse proactive s'appuyant sur l'usage de l'intelligence artificielle).

2.1.3.2 Meilleure sécurisation des communications entre les prestataires de services de paiement, et leurs clients et renforcement de la coopération avec les opérateurs de télécommunications

La loi [3] impose désormais aux opérateurs qui exploitent des numéros de téléphone français d'authentifier le numéro utilisé pour émettre un appel. Cette obligation légale constitue une innovation au sein de l'Union européenne. Elle a conduit les opérateurs à mettre en œuvre le mécanisme interopérable d'authentification des numéros (MAN), qui constitue le dispositif technique permettant de se conformer à l'obligation légale. Ainsi, un appel émis est signé par

l'opérateur de l'appelant. Les opérateurs qui acheminent ensuite cet appel jusqu'à son destinataire vérifient, à l'aide de certificats numériques, que la signature associée à l'appel est valide. Dans le cas contraire, l'acheminement de l'appel doit être interrompu. Le MAN constitue donc un outil majeur pour lutter contre l'usurpation du numéro d'appelant (*spoofing*).

Cependant, la persistance de quelques cas de fraude au faux conseiller bancaire avec *spoofing* a conduit l'Observatoire à proposer l'expérimentation du mécanisme *Do Not Originate* (DNO). Celle-ci, menée par les principaux opérateurs de télécommunications, a débuté en juin 2026. Ainsi, le PSP titulaire de la ligne identifie les numéros destinés exclusivement à recevoir des appels. C'est par exemple le cas de certains numéros destinés à recevoir les demandes d'opposition sur une carte perdue ou volée. Un appel émis depuis un tel numéro est donc présumé frauduleux et le DNO permettra de le couper automatiquement, avant même que le fraudeur ne puisse débuter une conversation avec la victime. En complément du MAN, dont l'efficacité repose sur la rigueur des opérateurs téléphoniques dans l'application de leur processus de vérification, le DNO renforce ainsi la lutte contre le *spoofing* pour les numéros les plus sensibles et exposés.

Pour lutter contre les SMS frauduleux et les risques d'hameçonnage, l'Observatoire promeut l'usage des OAdC (*Originator Address Code*) lorsque les PSP envoient des SMS à leurs clients. Un OAdC – aussi appelé *Sender ID,* champ émetteur ou identifiant d'émetteur –, est le libellé alphanumérique qui identifie l'expéditeur d'un SMS à la place d'un numéro court à 5 chiffres (par exemple, « Banque ABC » plutôt que « 38123 »). Les PSP alimentent désormais les listes d'OAdC protégés, établies par l'AF2M. Parallèlement, les PSP exploitent progressivement le flux des déclarations au numéro de téléphone 33700, correspondant à la plateforme qui reçoit les SMS signalés comme potentiellement frauduleux par leurs destinataires. L'AF2M transmet aux PSP concernés les SMS signalés au 33700 qui mentionnent leur nom. Si le SMS est effectivement frauduleux, le PSP peut demander le blocage d'un site usurpant son identité dont le lien est contenu dans le SMS.

Ces mesures permettent de renforcer la sécurité du canal de communication que constitue le SMS, et qui est encore utilisé par de nombreux PSP. À terme, le remplacement du SMS par le protocole RCS (*Rich Communication Services*)[4], appelé à devenir la messagerie par défaut sur les téléphones, apportera une meilleure sécurité pour les utilisateurs. En effet, pour les communications envoyées par des entreprises ou administrations, le protocole RCS intègre un mécanisme de vérification préalable de l'expéditeur.

Plusieurs PSP ont par ailleurs mis en place des mesures de lutte contre le *SIM swapping*. Cette fraude consiste à détourner la ligne téléphonique mobile d'un utilisateur de façon à recevoir à sa place les codes de validation à usage unique. Ainsi, pour lutter contre cette typologie de fraude, les PSP exploitent l'interface applicative *SIM verify*, proposée par l'AF2M. Cet outil permet d'identifier si une nouvelle carte SIM a été récemment délivrée (cas de figure qui peut correspondre à un usage légitime, mais également à un cas de *SIM swapping*). Le PSP associe cette information à d'autres facteurs (tels que le caractère anormal de l'opération au regard des habitudes de l'utilisateur des services de paiement), pour évaluer le niveau de risque de l'opération et la refuser lorsque le risque apparaît trop élevé.

Suivant une démarche similaire, certaines applications bancaires détectent si l'utilisateur, au moment où il initie ou valide un paiement, est en train de converser au téléphone avec un tiers (cas de figure qui peut notamment correspondre à celui d'une fraude par manipulation). Cette détection repose sur l'exploitation des métadonnées du téléphone, et plus précisément de l'indicateur *call in progress* (appel en cours)[5]. Les PSP coopèrent désormais avec l'AF2M pour déterminer les axes d'amélioration de l'interface applicative *SIM verify* et la possibilité d'exploiter plus largement les métadonnées du téléphone et de la ligne téléphonique.

Enfin, sous l'égide de la Fédération bancaire française (FBF), les principaux groupes bancaires et les organisations professionnelles du secteur des télécommunications étudient la faisabilité d'un numéro court « anti-fraude ». Ils s'inspirent du le modèle fondé sur le numéro téléphonique 159 disponible au Royaume-Uni et fédérant les principaux établissements bancaires britanniques. En cas d'appel suspect ou de risque de fraude, tout particulier pourrait ainsi appeler un numéro court (à déterminer) pour être rapidement mis en communication avec le service de lutte contre la fraude de son établissement bancaire.

2 Le MAN permet d'authentifier le numéro utilisé pour émettre un appel, conformément à l'article L. 44 du Code des postes et des communications électroniques, dans sa version en vigueur depuis juillet 2023, et donc de lutter contre l'usurpation, par les fraudeurs, des numéros de téléphone appartenant à des tiers (PSP, autorités, etc.).

3 Article L. 44 du Code des postes et des communications électroniques.

4 RCS est un protocole de messagerie qui apporte des fonctionnalités enrichies par rapport au SMS et au MMS. Une application de messagerie RCS sera présente par défaut sur les deux principales plateformes (iOS et Android). Contrairement aux messageries propriétaires telles que WhatsApp ou iMessage, RCS présente un caractère standard et interopérable.

5 Cette exploitation des métadonnées à des fins de lutte contre la fraude a donné lieu à un éclairage de la Commission nationale de l'informatique et des libertés (CNIL), publiée le 15 juillet 2025, sur les règles à respecter pour protéger le droit des personnes : *https://www.cnil.fr/fr/controle-appel-en-cours-utilisation-dune-application-bancaire-reglementation*

2.1.3.3 Développement de la coopération avec les plateformes numériques

Bien que les fraudeurs continuent d'utiliser le canal téléphonique, les nouveaux canaux offerts par les plateformes numériques tels que les messageries instantanées et les réseaux sociaux sont aujourd'hui une porte d'entrée privilégiée tant pour la fraude par manipulation que pour les escroqueries financières de manière générale. Ces plateformes constituent ainsi une surface d'attaque mondiale à faible coût. Elles facilitent la collecte d'informations sur les victimes (identité, habitudes, localisation, relations, etc.). Elles permettent de ce fait aux escrocs de personnaliser leurs messages afin de paraître crédibles et légitimes, rendant la manipulation particulièrement efficace. C'est dans ce contexte que l'Observatoire s'est engagé en 2025 à lancer, structurer et faciliter la coopération entre les grands acteurs du numérique et l'écosystème des paiements pour lutter contre les fraudes bancaires et en particulier contre celle par manipulation. Après avoir défini une feuille de route structurée autour de quatre axes *(cf.* feuille de route à destination des acteurs du numérique *infra*), l'Observatoire a identifié trois acteurs du numérique prioritaires : Google, Meta et TikTok. Les premières réunions de travail, sous l'égide de l'Observatoire, avec ces différents acteurs ont eu lieu au cours du premier semestre 2026.

Celles-là ont confirmé la nécessité d'intensifier la coopération avec l'écosystème français des paiements et des télécommunications. Cette coopération passe d'abord par une meilleure connaissance des stratégies de sécurité déployées par les acteurs du numérique pour lutter contre les contenus illégaux et frauduleux au regard des besoins exprimés par les experts en fraude de l'écosystème des paiements. Trois piliers semblent se dessiner de leurs actions et initiatives contre la fraude.

Les acteurs du numérique rencontrés par l'Observatoire s'engagent i) à sécuriser davantage leurs produits et services, et ii) à continuer de renforcer l'éducation ainsi que la sensibilisation de leurs utilisateurs aux techniques de fraudes dont ils pourraient être la cible (pilier n° 1). Cela peut passer par l'introduction de procédures d'authentification, des messages d'alerte ou des programmes de vérification des annonceurs. En matière de publicité, les acteurs du numérique doivent apporter une vigilance croissante à la légitimité des annonceurs et renforcer la lutte contre les contenus frauduleux et les escroqueries en ligne. Par exemple, dans le cas spécifique des publicités portant sur des produits et services financiers, ils doivent chercher à vérifier l'agrément de leurs annonceurs directement auprès des registres officiels tenus par les régulateurs [6]. L'efficacité des dispositifs déjà déployés par les acteurs du numérique doit toutefois être vérifiée et peut certainement encore s'améliorer.

Les acteurs du numérique s'engagent également à renforcer leurs mécanismes existants visant à détecter et arrêter les comptes et contenus frauduleux en temps réel (pilier n° 2). Ils s'appuient pour ce faire très largement sur des modèles d'intelligence artificielle (IA), qui analysent les comportements anormaux (création massive de comptes, messages identiques, etc.), identifient des schémas de manipulation (faux investissement, usurpation de l'identité de dirigeants d'entreprise ou de responsables politiques) ou détectent des liens malveillants ou des contenus trompeurs à grande échelle et en temps réel. Ces outils d'IA avancés ont déjà permis à ces plateformes de bloquer ou supprimer en 2025 une dizaine de milliards d'annonces malveillantes et de suspendre plusieurs dizaines de millions de comptes dans le monde. En complément de cette détection en amont, les acteurs du numérique indiquent traiter en aval les signalements qui leur sont remontés par les utilisateurs, et de façon plus privilégiée, par les autorités publiques. Toutefois, la question du respect du cadre règlementaire européen par ces acteurs se pose et nécessite un suivi particulier.

Plusieurs participants aux travaux de l'Observatoire ont relevé l'intérêt majeur que présente la vérification préalable de l'annonceur pour prévenir la diffusion de publicités frauduleuses. Un contrôle en amont pourrait s'apparenter à un KYB (*Know Your Business,* connaissance du client) des clients qui diffusent leurs publicités sur ces plateformes internet. Cette vérification permet de s'assurer de l'existence de la personne qui souhaite diffuser des publicités et, dans le cas d'une publicité pour des services financiers (tels que des propositions d'investissement), que cette personne dispose d'une autorisation pour exercer dans le pays dans lequel la publicité est diffusée. Les acteurs du numérique soulignent que ces vérifications pourraient toutefois gagner en efficacité si les registres officiels évoluaient dans leur format et leur contenu (registres des sociétés tenus aux niveaux national et européen, registre des entités agréées pour exercer dans le secteur financier, etc.).

Enfin, les acteurs du numérique sont convaincus que la lutte contre la cybercriminalité passe par une coopération de l'ensemble des acteurs publics et privés, ainsi que par l'échange d'informations entre ces parties (pilier n° 3). Ils sont donc particulièrement disposés à accompagner l'intégration des PSP français dans leurs programmes d'échange d'informations existants : *Priority Flagger Program* pour Google [7], *Fraud intelligence reciprocal exchange* (FIRE, programme d'échange réciproque de renseignements sur la fraude) pour Meta, ou encore le

Global Signal Exchange[8] lancé et soutenu par une alliance de grands acteurs du numérique, dont Google et Meta. Ces programmes, auxquels adhèrent déjà certaines banques françaises, ont pour objectif de partager, avec les acteurs du numérique, les informations recueillies et les alertes de risque produites en matière de fraude. Ils présentent cependant certaines limites à ce jour, étant davantage réactifs que proactifs.

L'intégration des institutions financières et des acteurs des télécommunications dans les programmes de partage d'informations permettrait d'enrichir encore davantage les outils de prévention et de détection de la fraude des acteurs du numérique. En parallèle, ces mêmes programmes doivent permettre aux PSP d'accéder plus rapidement aux informations liées à la diffusion de contenus frauduleux sur internet, les applications de messagerie ou les réseaux sociaux. En ce sens, le 16 mars 2026, de nombreux acteurs du numérique[9] ont signé l'accord volontaire international contre les escroqueries et fraudes en ligne (*Industry accord against online scams and fraud*) lors du sommet mondial contre la fraude organisé par les Nations unies (*UN Global fraud summit),* à Vienne en Autriche. Cet accord vise à organiser une réponse collective, transversale et structurée contre la fraude en ligne à l'échelle mondiale. Cette initiative doit contribuer à accélérer le partage de signaux sur les fraudes et à mieux tracer les réseaux criminels multicanaux.

L'Observatoire prend acte des engagements pris par les acteurs du numérique, tels que Google, Meta et TikTok, ainsi que de leur disposition à intensifier leur coopération opérationnelle avec l'écosystème français des paiements, tant pour la détection que la prévention des fraudes. Il invite dans le même temps les acteurs français des paiements à explorer les programmes de coopération existants. Cette démarche de coopération engagée au niveau national a vocation à se poursuivre et s'approfondir dans les mois et années à venir. Elle pourra par la suite être étendue au niveau européen, dans la perspective notamment de l'entrée en application du règlement européen sur les services de paiement (RSP), qui devrait faciliter cette coopération.

6 Cette vérification devrait de surcroît être requise par le futur règlement européen sur les services de paiement (RSP), qui devrait être publié au journal officiel de l'Union européenne d'ici la fin 2026.

7 Programme de signalement prioritaire offrant un canal de réception dédié aux organisations expertes pour informer Google des violations potentielles de ses politiques concernant certains produits et services ou de contenus potentiellement frauduleux.

8 Échange mondial de signaux. Plateforme d'échange mondiale, multipartite et intersectorielle, de signaux d'activité malveillante lancée en octobre 2024 par le *Global anti-scam alliance* (GASA, Alliance mondiale anti-escroquerie). Son objectif est de mieux comprendre le déroulement des escroqueries et d'identifier leurs auteurs.

9 Parmi les signataires : Google, Meta, Microsoft, Amazon, LinkedIn, OpenAI, Pinterest et Match Group.

RECOMMANDATIONS VISANT À RENFORCER LA SÉCURISATION DES CANAUX DE TÉLÉCOMMUNICATIONS *(POUR MÉMOIRE : RECOMMANDATIONS ÉMISES DANS LE RAPPORT ANNUEL 2024)*

Recommandation n° 1 :

Afin de lutter contre les fraudes par manipulation, les prestataires de services de paiement (PSP) sont encouragés à étudier les différentes pistes permettant de mieux sécuriser leurs communications avec leurs clients, en s'inspirant des meilleures pratiques sur le marché, par exemple :

- Recenser et réguler les canaux de communication avec le client de façon à réduire, voire à supprimer, les échanges par SMS ou courriel, en privilégiant autant que possible l'application mobile qui est réputée plus sécurisée, y compris pour les échanges téléphoniques ;
- Envoyer une notification sur l'application mobile, lorsqu'un appel légitime de l'établissement est en cours, de façon à certifier l'appel auprès du client. En l'absence de notification sur l'application mobile, le client doit alors suspecter que l'appelant est un fraudeur ;
- Utiliser les métadonnées du téléphone portable pour identifier l'existence d'un appel en même temps que la réalisation d'opérations sensibles depuis l'application mobile, afin de déceler un éventuel scénario de fraude par manipulation. À cet égard, la Commission nationale de l'informatique et des libertés (CNIL) a publié le 15 juillet 2025 sur son site internet des articles indiquant les conditions sous lesquelles les banques pouvaient contrôler l'existence d'un appel en cours pendant l'utilisation d'une application bancaire ;
- Renforcer la sécurité de certains parcours d'authentification, en particulier la déclaration d'un nouveau numéro de téléphone (par exemple, en recourant au standard *Number Verify* de la GSMA [*Global System for Mobile Communications*], l'association mondiale des opérateurs de téléphonie mobile) ou l'installation de l'application sur un nouveau terminal (par exemple, en complétant l'authentification forte d'une courte capture vidéo).

Recommandation n° 2 :

Les PSP sont invités à communiquer aux opérateurs téléphoniques les numéros destinés à recevoir uniquement des appels de façon à déployer concrètement d'ici 2026 un mécanisme de protection de ces numéros particulièrement exposés au *spoofing*.

Recommandation n° 3 :

L'Observatoire appelle les PSP et les acteurs de télécommunications à étudier l'opportunité de mettre en place un numéro unique permettant de joindre les services anti-fraude de leur établissement bancaire. En cas d'appel suspect, le consommateur serait invité à raccrocher et appeler ce numéro unique pour vérifier la légitimité de l'appel.

Recommandation n° 4 :

Les professionnels des paiements ainsi que les grandes entreprises et administrations, qui sont régulièrement ciblées dans les campagnes de *phishing*, sont invités à se rapprocher de l'AF2M pour i) protéger les libellés utilisés dans leur SMS (OAdC sensibles), ii) alimenter la liste noire (OAdC strictement interdits) et iii) souscrire au flux d'information proposé par la plateforme 33700 de façon à identifier les nouveaux risques d'usurpation dans les messages signalés et entreprendre les actions de démantèlement nécessaires, comme la coupure des liens URL contenus dans les messages signalés.

Recommandation n° 5 :

Les PSP qui recourent au SMS-OTP (*one-time password*, code à usage unique) comme facteur d'authentification sont encouragés à étudier l'intégration de l'interface de programmation d'application (API, *application programming interface*) multi-opérateurs « *SIM Verify* » dans leurs processus de prévention de la fraude en temps réel, ainsi que tout autre outil qui permettrait de détecter une récente demande de portabilité de la ligne vers un nouvel opérateur.

FEUILLE DE ROUTE VISANT À RENFORCER LES ACTIONS DES ACTEURS DU NUMÉRIQUE AINSI QUE LEUR COOPÉRATION AVEC L'ÉCOSYSTÈME FRANÇAIS DES PAIEMENTS *(POUR MÉMOIRE : ORIENTATIONS ÉMISES DANS LE RAPPORT ANNUEL 2024)*

Axe n° 1 :

L'échange d'informations entre les acteurs du numérique et les prestataires de services de paiement

À l'image du programme FIRE au Royaume-Uni (*Fraud Intelligence Reciprocal Exchange*) entre les acteurs bancaires et Meta, il s'agit de structurer un canal efficace d'échange d'informations relatives à l'activité des fraudeurs. Celui-ci pourrait notamment permettre aux PSP français de signaler, y compris à travers le mécanisme prévu à l'article 16 du règlement européen (UE) 2022/2065 sur les services numériques (DSA, *Digital Services Act*), aux acteurs du numérique des escroqueries ayant pris racine sur une de leurs plateformes (Facebook, Instagram, WhatsApp, TikTok, etc.), de façon à ce que celle-ci puisse fermer les comptes utilisés par les fraudeurs ou retirer les contenus frauduleux qui seraient portés à leur connaissance et dont il serait possible d'établir l'illicéité « sans examen juridique détaillé », sous peine d'engager leur responsabilité.

Par ailleurs, pour les très grandes plateformes en ligne désignées par la Commission européenne, l'ensemble des informations susceptibles de leur être remontées, notamment par les PSP, pourraient les amener à nourrir l'identification des risques systémiques liés à la diffusion de contenus frauduleux en ligne, mieux surveiller les activités suspectes et adapter en conséquence les mesures d'atténuation qu'elles doivent adopter pour y répondre.

Axe n° 2 :

L'échange d'informations sur le signalement des numéros suspects

Il existe de nombreux mécanismes propriétaires de signalement mis en place par les acteurs du numérique, qu'il s'agisse des outils de messagerie, des systèmes d'exploitation ou des fabricants de téléphones portables. Ceux-là coexistent avec le 33700 mis en place par l'AF2M, sans que tous ces acteurs ne communiquent entre eux.

Axe n° 3 :

La lutte contre l'usurpation d'identité dans les usages numériques

Les fraudeurs invitent souvent leurs victimes à basculer leurs communications sur des applications de messagerie propriétaires censées être plus sécurisées (par exemple WhatsApp, Signal, Telegram). Or, en l'absence de procédures de vérification d'identité et de connaissance client, aussi approfondies que dans le secteur financier, les fraudeurs parviennent aisément à usurper l'identité des PSP sur ces applications numériques, par exemple en affichant le logo d'un établissement bancaire comme image de profil, ou à usurper l'identité de commerçants par le biais d'annonces en ligne renvoyant vers des sites miroirs. Par ailleurs, les procédures d'authentification des acteurs du numérique restent souvent fondées sur le seul couple identifiant-mot de passe. Ceci permet par exemple aux fraudeurs d'accéder facilement à des outils de messagerie, d'y intercepter des données sensibles ou d'y commettre des fraudes au virement, en annonçant par exemple à des interlocuteurs légitimes un changement de coordonnées bancaires.

Axe n° 4 :

La lutte contre les publicités frauduleuses

Il sera notamment étudié la possibilité pour les acteurs du numérique de renforcer les procédures de connaissance client des annonceurs qui opèrent des ventes depuis leurs plateformes, de façon à vérifier que les liens renvoient vers des sites légitimes sans usurpation de l'identité d'un commerçant tiers. À cet égard, il pourra être demandé aux plateformes d'enlever tout lien ou toute référence vers des sites identifiés dans les listes noires de l'Autorité de contrôle prudentiel et de résolution (ACPR) et de l'Autorité des marchés financiers (AMF), de leurs équivalents européens ou des autres listes noires mises en place par des autorités publiques.

2.2 Prévention de la fraude sur les paiements par carte à distance

2.2.1 Contexte des recommandations

Les différentes catégories de paiement par carte à distance ne sont pas égales face à la fraude. Ce constat a conduit l'Observatoire à adopter en juin 2024 un ensemble de recommandations portant sur les paiements à distance les plus affectés. Il s'agit de ceux qui ne transitent pas par le protocole d'authentification *3-D Secure*. Ce plan de sécurisation couvre, d'une part, les paiements sur internet hors *3-D Secure*, et d'autre part, les paiements à distance pour lesquels le numéro de la carte est communiqué par téléphone ou par écrit (*Mail Order Telephone Order*, MOTO).

Ce plan repose notamment sur la mise en œuvre d'une limite de vélocité. Elle est calculée comme le montant cumulé des achats effectués avec une même carte auprès d'un même commerçant sur une période de 24 h glissante [10]. Au-delà de cette limite, les transactions ne répondant pas aux recommandations de l'Observatoire doivent être rejetées par les établissements émetteurs.

La conduite de ce plan de sécurisation des paiements par carte à distance est assurée par un Comité de pilotage *ad-hoc* de l'Observatoire. Il réunit, sous l'égide de la Banque de France, les prestataires de services de paiement, les prestataires d'acceptation technique et les représentants des commerçants. En fonction des décisions du comité prises lors des échanges avec ses membres, le plan de sécurisation est régulièrement actualisé et publié en français et en anglais sur le site internet de l'Observatoire. Une vision synthétique des recommandations est fournie dans le tableau 2, avec un aperçu de leur niveau d'avancement.

Ce plan repose sur la mise en œuvre coordonnée de mesures par l'ensemble des PSP émetteurs établis en France, ainsi que par l'implication des commerçants dans le déploiement desdites mesures. Les principaux PSP émetteurs français appliquent correctement ce plan. Toutefois, l'Observatoire renouvelle son appel auprès des émetteurs indépendants ou filiales de grands groupes à assurer la bonne mise en œuvre des recommandations formulées dans le cadre de ce plan de sécurisation.

2.2.2 Plan d'action

Depuis 2025, le Comité de pilotage a travaillé à la mise en œuvre du plan de sécurisation autour de deux axes.

Axe 1 : sur les paiements dits MOTO

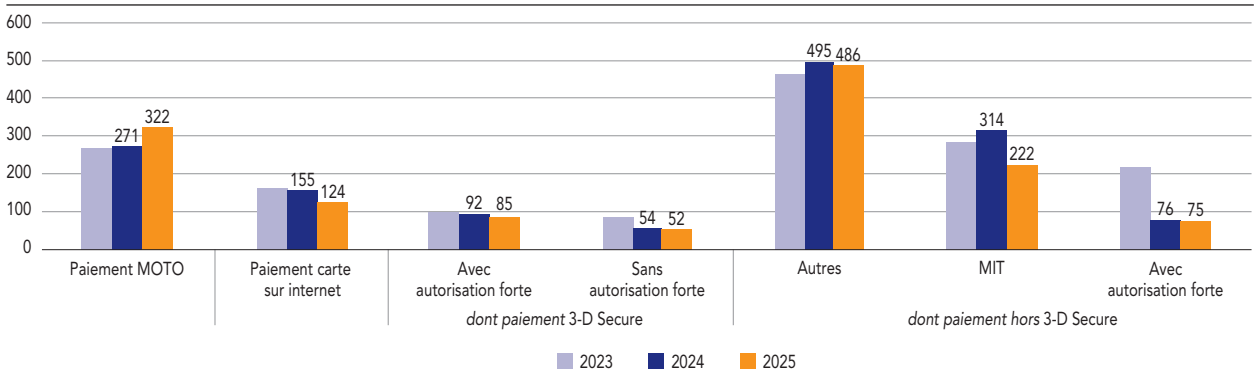
La limite de vélocité est fixée à 500 euros depuis juin 2024, excepté pour certains secteurs d'activité dûment identifiés. L'Observatoire a demandé au Comité de pilotage de progressivement lever ces exemptions sectorielles de façon à aboutir à une limite de vélocité uniforme de 500 euros pour l'ensemble des secteurs d'ici la fin de l'année 2026. En parallèle, l'Observatoire recommande l'usage de procédés sécurisés pour la transmission par téléphone du numéro de la carte (saisie directe sur le clavier ou serveur vocal interactif). De plus, il soutient le développement d'une solution d'authentification des paiements initiés par téléphone (*Telephone Order,* TO). Les réseaux de paiement par carte ont défini des spécifications en début d'année 2026. Ainsi, à partir du second semestre 2026, cette nouvelle solution d'authentification commencera à être déployée. Concrètement, une authentification forte du paiement, généralement sur l'application mobile bancaire, pourra être demandée pour tout paiement pour lequel le numéro de la carte est communiqué par téléphone.

Axe 2 : sur les paiements par carte sur internet hors *3-D Secure*

La limite de vélocité est fixée à 0,01 euro depuis janvier 2026 pour les paiements pour lesquels le PSP acquéreur est situé au sein de l'Espace économique européen (EEE). L'Observatoire recommande désormais d'appliquer des limites de vélocité sur les paiements internationaux par carte. L'horizon de mise en application est différencié selon les régions du monde pour tenir compte de leur niveau de maturité concernant les procédures *3-D Secure*.

Un troisième axe de travail se profile dans le plan d'action du Comité de pilotage. Il consistera pour l'Observatoire à surveiller, dans les mois et années à venir, le renforcement de la sécurité des paiements par carte initiés par les commerçants (*merchant initiated transactions*, MIT). Cette action est en lien avec la recommandation n° 2 *bis* du plan de sécurisation. Il s'agit d'accroître la transparence des informations liées au mandat dans les fenêtres d'authentification *3-D Secure*, lorsque le consommateur approuve le mandat de prélèvement par carte. Cet axe vise aussi à mettre à disposition du consommateur, dans ses outils de banque en ligne, des outils de visualisation et de gestion des différents mandats qu'il a signés. Les acteurs industriels de la carte ont d'ores et déjà engagé des réflexions qui feront l'objet d'un suivi de la part du Comité de pilotage.

Fraude sur les cartes émises par les PSP français (en euros pour 100 000 euros de paiement)



Note : MIT, *merchant initiated transaction*, paiement initié par le commerçant ; MOTO, *mail order, telephone order*, paiements par courrier ou par téléphone.

Source : Observatoire de la sécurité des moyens de paiement.

2.2.3 Effets du plan de l'Observatoire

Les statistiques de fraude 2025 confirment que les paiements par carte à distance restent beaucoup plus exposés à la fraude que les paiements de proximité. En effet, parmi les transactions par carte, si les paiements à distance ne représentent que 28 % des montants échangés, ils représentent 78 % des montants de fraude. Les canaux les plus exposés à la fraude restent i) les paiements MOTO, ii) les paiements sur internet sans authentification forte qui ne recourent pas au protocole *3-D Secure* et iii) les MIT. Le taux de fraude de ces trois catégories de paiement est trois à cinq fois plus élevé que celui des autres paiements par carte à distance. L'implication de l'Observatoire pour mieux sécuriser les paiements par carte à distance reste donc primordiale.

Cela étant rappelé, les résultats positifs du plan de sécurisation de l'Observatoire sont déjà manifestes dans les statistiques de fraude 2025.

Les paiements dits « MOTO »

D'une part, les flux MOTO (*mail order, telephone order*, paiements par carte initiés par courrier ou par téléphone) baissent en volume comme en valeur, avec un recul de 12 % en volume entre 2024 et 2025 (contre 1 % entre 2023 et 2024) et de 21 % en valeur (contre 6 % entre 2023 et 2024). Cette diminution est probablement sous-tendue par un plus fort recours aux solutions de paiement alternatives (paiement par carte sur internet ou virement, voire paiement de proximité), conformément aux recommandations de l'Observatoire.

D'autre part, les montants de fraude sur les flux MOTO ont baissé de 7 % pour atteindre 37,7 millions d'euros en 2024 (contre 40,4 millions d'euros en 2024). Cette diminution étant toutefois moins forte que celle des flux, cela se traduit mécaniquement par une hausse du taux de fraude. La poursuite du plan de sécurisation devrait néanmoins permettre d'aboutir, à terme, à une baisse du taux de fraude. L'examen plus approfondi des données montre que la fraude baisse plus rapidement sur les transactions MOTO nationales (– 13% en valeur entre 2024 et 2025) que sur les paiements MOTO européens et internationaux. Par conséquent, un complément du plan d'action visant à mieux sécuriser les MOTO internationaux pourra être examiné par le Comité de pilotage à l'avenir.

Les paiements internet hors *3-D Secure*

Le taux de fraude sur les paiements par carte internet, ainsi que sur l'ensemble de ses canaux d'initiation associés, recule de 20 % entre 2024 et 2025, passant de 0,155 % à 0,124 %. Cette diminution est le résultat de la baisse i) du taux de fraude sur les paiements MIT (– 21 %), ii) du taux de fraude sur les paiements *3-D Secure* avec authentification forte (– 9 %) et iii) de la proportion de paiements hors *3-D Secure* (– 22 %), c'est-à-dire les paiements non authentifiés en excluant les paiements MIT.

Les paiements de type MIT sont quant à eux en progression (+ 12 % en volume, + 14 % en valeur), alors que dans le même temps la fraude associée reflue nettement (– 17 % en volume, – 21 % en valeur). Mécaniquement, le taux de fraude recule de 21 %. Les mesures de sécurisation des MIT ne sont pas encore généralisées. Cependant, le travail mené sous l'égide de l'Observatoire avec quelques commerçants classés prioritaires, car affichant des taux de fraude importants sur leurs transactions MIT, a pu porter ses premiers fruits. Néanmoins, une part encore élevée de la fraude sur ces paiements pourrait être due à des litiges commerciaux. Par exemple, les consommateurs contestent

10 Vélocité = montant cumulé des achats / carte / commerçant / 24 heures glissante.

avoir souscrit un abonnement et signalent les transactions comme étant frauduleuses auprès de leur PSP. En règle générale, ce dernier rembourse le client après avoir émis une demande de rétrofacturation (*chargeback*) auprès du commerçant concerné. Dans le cadre actuel, les dispositifs de rétrofacturation ne permettent toutefois pas d'identifier de manière satisfaisante les contestations abusives.

2.2.4 État du déploiement des recommandations et perspectives pour 2027

Les paiements MOTO

Tout d'abord, le dialogue se poursuit avec la dizaine de commerçants prioritaires (recommandation n° 3 *bis*), appartenant à des secteurs exemptés mais dont l'exposition à la fraude est régulièrement supérieure à la moyenne de la Place. Chaque commerçant prioritaire a été invité à fournir un plan d'action visant à réduire autant que possible ses flux MOTO au profit de canaux plus sécurisés et à sécuriser les flux MOTO restants. Une fois validé, chaque plan d'action est suivi par l'Observatoire jusqu'à son terme.

Ensuite, la limite de vélocité a été abaissée à 500 euros dès juin 2024 à l'exception d'une liste réduite de secteurs d'activité. D'ici la fin de l'année 2026, cette limite de 500 euros sera applicable à l'ensemble des secteurs [11]. Seul celui de la vente sur catalogue (MCC [12], 5965) pour les achats réalisés par courrier uniquement (code ERT [13] 22 dans la nomenclature du Groupement des Cartes Bancaires) continuera de bénéficier d'une exemption. En effet, l'absence de solution d'authentification pour les paiements par carte initiés sur support papier nécessite cette dérogation. Les paiements initiés par téléphone (*Telephone Order*, TO) mais ayant bénéficié d'une authentification par le protocole *3-D Secure* seront également exemptés de cette limite de vélocité.

Par conséquent, l'ensemble des acteurs est très fortement invité par l'Observatoire à participer au déploiement de la solution d'authentification des paiements par téléphone (émetteurs, acquéreurs, prestataires d'acceptation et bien sûr commerçants). L'objectif est de garantir le bon fonctionnement de cette solution et son déploiement à partir du second semestre 2026 *(cf. recommandation n° 5)*. Les spécifications ont déjà été définies par le réseau Cartes Bancaires CB et sont compatibles avec les réseaux Visa et Mastercard. Les commerçants acceptant des paiements par téléphone, en particulier ceux pour lesquels les transactions peuvent dépasser 500 euros, doivent interroger leurs prestataires bancaires et monétiques pour connaître les jalons de mise en œuvre de cette solution. Ils pourront ainsi anticiper les développements à conduire en amont.

La réussite du déploiement de la solution d'authentification des paiements par téléphone est une priorité stratégique de l'Observatoire en 2026 et 2027. Cette solution pourrait permettre à la France d'être pionnière dans la sécurisation de ces transactions qui n'ont pas bénéficié jusqu'ici des effets positifs de l'authentification forte. À l'avenir, lorsque cette solution sera suffisamment déployée et qu'elle aura prouvé son efficacité en matière de lutte contre la fraude et aussi d'accessibilité pour les usagers, le Comité de pilotage travaillera à progressivement abaisser la limite de vélocité en-deçà de 500 euros pour les transactions MOTO qui ne transiteraient pas par *3-D Secure*.

Les paiements internet hors *3-D Secure*

En premier lieu, à l'instar des paiements MOTO, le Comité de pilotage a continué d'assurer le suivi des commerçants identifiés comme prioritaires pour les paiements MIT (recommandations n° 3 *ter*). Le suivi de leur plan d'action continuera en 2027.

En parallèle, la limite de vélocité sur les paiements par carte hors *3-D Secure* a progressivement été abaissée, par paliers successifs pour atteindre 0,01 euro depuis janvier 2026 (recommandation n° 3). Le plan de l'Observatoire ne couvrait initialement pas les paiements internationaux auprès de commerçants et de PSP acquéreurs situés en dehors de l'espace économique européen (EEE). Dorénavant, cette limite de vélocité a été étendue aux commerçants et acquéreurs situés :

- dans les pays européens n'appartenant pas à l'EEE (par exemple le Royaume-Uni ou la Suisse), et dans la zone monétaire du franc Pacifique, dont les écosystèmes de paiement sont rôdés au protocole *3-D Secure*, avec un seuil de 1,01 euro depuis mars 2026 ;
- dans la zone Afrique et Moyen-Orient, pour laquelle la limite de vélocité est de 100 euros depuis juillet 2026 ;
- dans la zone Asie, Amérique du Nord et Sud, Océanie et Pacifique, pour laquelle la limite de vélocité est de 500 euros depuis septembre 2026.

Chaque pays a été rattaché à une zone géographique et associé à un calendrier de déploiement repris dans le plan de l'Observatoire publié sur son site internet *(cf. recommandation n° 3* quater *et annexe 5)*.

Enfin, les PSP émetteurs notent une amélioration substantielle du niveau de conformité des MIT, qui présentent de plus en plus des références de chaînage valide. Néanmoins, certains commerçants relèvent encore des problèmes de performance générale ou de couverture de cas d'usage complexes.

Par ailleurs, d'ici la fin de l'année 2026, l'ensemble des grands groupes bancaires français permettra aux commerçants d'afficher dans la fenêtre *3-D Secure* une information enrichie sur le contexte d'un paiement récurrent (périodicité, date de fin, montant d'échéance unitaire, montant à la souscription en cas de période d'essai, etc.). Cette meilleure transparence sur les caractéristiques des mandats de MIT facilitera leur validation par les consommateurs. Les établissements bancaires ont aussi lancé une réflexion pour mettre à disposition, dans les interfaces de banque en ligne, des outils de visualisation et de gestion des abonnements souscrits par carte.

Ainsi, en 2027, l'Observatoire va s'attacher : i) au renforcement de la transparence des mandats de MIT dans les fenêtres d'authentification *3D-Secure* avec une meilleure information du client sur les termes et effets du mandat ; ii) au suivi de la mise en place des outils de gestion de ces mandats depuis les interfaces de banque en ligne, et enfin iii) à l'accompagnement du marché français dans la mise en œuvre de ces nouveaux outils. Conjugués aux outils d'identification des terminaux utilisés par les consommateurs, ces outils devraient permettre aux PSP émetteurs de mieux distinguer les fraudes des litiges commerciaux dans le traitement des contestations comme dans les reportings réglementaires. Ils devraient ainsi contribuer à réduire le niveau de fraude mesuré sur les transactions MIT.

11 La procédure permettant des dérogations individuelles reste valable. Certains commerçants peuvent ainsi accepter des paiements MOTO sans limite de vélocité, à condition d'avoir correctement démontré la sécurisation de leurs flux (cf. annexe 3 du plan de sécurisation).

12 MCC : *Merchant Category Code*, code de catégorie de commerçant.

13 ERT : environnement réglementaire et technique.

T2 Vue synthétique de la mise en œuvre des recommandations de l'Observatoire sur les paiements par carte à distance hors *3-D Secure*

Recommandation	Niveau de réalisation
Recommandation n° 1 : Limitation des paiements MOTO et MIT aux seuls cas d'usage où le recours à un autre mode de paiement n'est pas possible	Les paiements MOTO sont en baisse en 2025 sur les cartes émises par des PSP français (– 12 % en volume et – 21 % en valeur). Les paiements MIT sont en augmentation (+ 14 % en volume et + 12 % en valeur), ce qui est cohérent avec les développements des usages numériques.
Recommandation n° 2 : Chaînage valide des MIT	Amélioration substantielle du niveau de conformité des MIT, présentant des références de chaînage valide.
Recommandation n° 2 *bis* : Sécurisation des MIT	Réflexions en cours sur les outils à mettre en place pour répondre à la recommandation.
Recommandation n° 3 : Limite de vélocité et mise en place d'un mécanisme de *soft decline*	Limite de vélocité fixée à 500 euros sur les paiements MOTO (avec une levée progressive des exemptions sectorielles jusqu'à la fin de l'année 2026) et à 0,01 euro sur les paiements internet hors *3D-Secure.*
Recommandation n° 3 *bis* : Mesures spécifiques applicables aux commerçants identifiés comme prioritaires pour la réduction de la fraude sur le MOTO	Suivi jusqu'à leur terme des plans d'actions soumis par les commerçants.
Recommandation n° 3 *ter* : Mesures spécifiques applicables aux commerçants identifiés comme prioritaires pour la réduction de la fraude sur les paiements MIT	Suivi jusqu'à leur terme des plans d'actions soumis par les commerçants.
Recommandation n° 3 *quater* sur les transactions dites « *one-leg* » : Limite de vélocité pour les transactions internet hors 3D-Secure avec un PSP acquéreur établi en dehors de l'espace économique européen (EEE)	La baisse des seuils est en cours et se poursuivra jusqu'à la fin de l'année 2026.
Recommandation n° 4 : Sécurisation des données de paiement pour les paiements MOTO	Rappels réguliers à l'ensemble des acteurs de l'écosystème. La mise en œuvre de cette recommandation est également surveillée au moment de l'instruction des demandes individuelles de dérogation aux limites de vélocité.
Recommandation n° 5 : Expérimentation de l'authentification des paiements MOTO	Mise en œuvre généralisée envisagée à partir du second semestre 2026.

MOTO : *mail order*, *telephone order*, paiement par carte initié par courrier ou par téléphone ; MIT : *merchant initiated transactions*, transaction initiée par le marchand ; PSP : prestataires de services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

2.3 Suivi des autres actions et recommandations de l'Observatoire

2.3.1 Recommandations de l'Observatoire contre la fraude au chèque

Dix recommandations de l'Observatoire sur la sécurité des paiements par chèque ont été publiées dans son rapport annuel 2020. Certaines mesures ont très vite montré leur efficacité à l'image des dispositifs de prévention et de surveillance mis en place par les banques pour renforcer le contrôle des chèques à l'encaissement (par exemple la temporisation du crédit en compte en cas de remise de chèque d'un montant inhabituel).

Si la moitié de ces recommandations a pu être clôturée en raison de leur bonne application, cinq d'entre elles continuent à faire l'objet d'un suivi par l'Observatoire en vue d'assurer leur bon déploiement au cours des années 2026 et 2027.

2.3.1.1 Protection du chéquier lors de son acheminement au client (recommandation n° 4)

Pour lutter plus efficacement contre le vol de chéquiers pendant la phase d'acheminement chez le client, l'Observatoire a appelé les établissements bancaires à i) privilégier le retrait en agence (qui ne doit pas occasionner de frais supplémentaire pour le client), ii) sécuriser par tout moyen l'acheminement des chéquiers s'il se fait par voie postale jusqu'à ce que le chéquier soit entre les mains du client et iii) adopter en ce domaine un dispositif de vigilance permanente assurant une réaction rapide. **Bien que l'Observatoire ait appelé chacun à privilégier le retrait du chéquier en agence, il ne s'est pas opposé aux modalités de l'envoi postal du chéquier sous réserve que celui-ci soit sécurisé et tracé.**

À cet effet, chaque groupe bancaire a établi, à la demande de la Banque de France, un plan d'action formulant les décisions prises en vue de respecter les recommandations de l'Observatoire.

L'Observatoire effectuera un suivi rapproché auprès des groupes bancaires pour lesquels les mesures ne sont pas totalement déployées à ce stade.

2.3.1.2 Simplification des procédures de mise en opposition pour perte ou vol de chèques ou chéquiers (recommandation n° 5)

Afin de simplifier concrètement les procédures de mise en opposition, l'Observatoire a demandé aux établissements bancaires de laisser la possibilité au client de mettre un chéquier/chèque en opposition directement en ligne, par le biais des outils numériques dont dispose la banque. L'Observatoire a précisé que ces outils doivent permettre aux clients de déclarer et de confirmer l'opposition de bout en bout. En outre, l'Observatoire a demandé que les dispositifs de mise en opposition s'appuyant sur des supports non numériques soient également fluides et rapides.

Dans ce cadre et à l'instar de la recommandation n° 4, chaque groupe bancaire a remis son plan d'action de mise en œuvre de cette mesure. Pour la plupart des groupes bancaires, la mesure est d'ores et déjà déployée. En revanche, deux groupes bancaires observent un délai de mise en œuvre plus long, ramenant l'échéance à début 2027. L'Observatoire réalisera un suivi des groupes bancaires pour lesquels les mesures ne sont pas totalement déployées à ce stade.

T3 Plan d'action défini par l'Observatoire en matière d'acheminement des chéquiers

Demandes de l'Observatoire	État de la mise en œuvre de la recommandation
Laisser de manière explicite le choix du mode de réception d'un chéquier au client.	**La recommandation est effective dans tous les groupes bancaires, à l'exception d'un groupe qui ne laisse pas le choix du mode de réception dans la mesure où les chéquiers sont tous envoyés en lettre suivie.**
Lorsque le client fait le choix de recevoir son chéquier par courrier postal, l'établissement bancaire procède à : i) l'envoi d'un premier message au client annonçant l'envoi du chéquier, ii) l'envoi d'un second message informant que le chéquier devrait être arrivé à destination.	i) La recommandation est effective dans l'ensemble des groupes bancaires. ii) La recommandation est en cours de mise en œuvre sur une période allant de juin à décembre 2026.
Le canal emprunté pour envoyer ces messages doit être adapté à chaque profil de clients.	La recommandation est en cours de mise œuvre sur une période allant de juin à décembre 2026 et déjà effective dans un groupe bancaire.

Source : Observatoire de la sécurité des moyens de paiement.

2.3.1.3 Évolutions législatives relatives au Fichier national des chèques irréguliers (FNCI)

Dans une perspective de renforcement de la prévention de la fraude et de maîtrise des risques opérationnels, l'Observatoire avait appelé les pouvoirs publics à faire évoluer la réglementation régissant le fonctionnement du FNCI. L'objectif était de diversifier les possibilités d'accès en consultation de ce fichier et d'enrichir son contenu. La loi n° 20251058 du 6 novembre 2025 visant à renforcer la lutte contre la fraude bancaire a permis de répondre à ces attentes, permettant de contribuer à la mise en œuvre de trois recommandations de l'Observatoire.

a) Amélioration des contrôles de la banque du remettant contre les remises frauduleuses (recommandation n° 2)

L'article L131-86 [14] du Code monétaire et financier a élargi la consultation du FNCI aux banques. En effet, il permet désormais aux banques, lorsqu'elles reçoivent des remises de chèques de leurs clients, de consulter le FNCI. Cette consultation était précédemment réservée aux clients recevant des chèques en paiement. Cet accès permet aux établissements bancaires de disposer d'un outil opérationnel supplémentaire pour détecter, dès la remise et lors des traitements, les chèques qui ont fait l'objet d'une opposition pour perte ou vol. Cette possibilité contribue à renforcer l'efficacité des contrôles dans les processus d'encaissement, en particulier pour les remises à risque ou atypiques, et à améliorer la réactivité des dispositifs de lutte contre la fraude.

À ce stade, l'offre de service Vérifiance [15] dédiée aux banques, ouverte depuis le 4 mars 2026, est en phase de tests auprès de trois groupes bancaires. Deux autres groupes bancaires ont sollicité un test en conditions réelles. Ainsi, la Banque de France s'attend à une augmentation du nombre de consultations du FNCI en amont de l'encaissement d'un chèque.

b) Soutenir le développement des contrôles du côté de l'établissement tiré (recommandation n° 3)

La modification de l'article L.13184 [16] du Code monétaire et financier a permis d'élargir la liste des cas d'irrégularité devant être signalés à la Banque de France dans le cadre du FNCI. Cette liste s'étend désormais aux cas de rejet pour falsification ou contrefaçon de chèque, ainsi qu'aux situations dans lesquelles le banquier émetteur du chèque a connaissance de telles fraudes. Cela renforce ainsi le poids du FNCI en matière de lutte contre la fraude matérielle au chèque.

Cette obligation prévoit d'informer la Banque de France dans les meilleurs délais, ce qui répond aux attentes de l'Observatoire en matière de réactivité de ce dispositif. Cette orientation contribue à limiter les risques de réutilisation frauduleuse de chèques ou de formules contrefaites et renforce l'efficacité préventive du FNCI. Ainsi, la Banque de France a d'ores et déjà observé une augmentation de 7,83 % du volume annuel des déclarations de faux chèques, passant de 5 300 déclarations en 2024 à 5 715 en 2025, alors que la loi n'est entrée en vigueur qu'en novembre 2025.

c) Offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du FNCI (recommandation n° 6)

Pour ouvrir la consultation du FNCI au plus grand nombre, la Banque de France a mis en place, dans le cadre du service Vérifiance, une modalité de consultation du FNCI, appelée « mandataire spécifique ». Celle-ci vise à élargir la consultation du FNCI aux bénéficiaires au-delà des acteurs professionnels, et donc notamment aux particuliers et aux associations.

2.3.1.4 Harmonisation des éléments de sécurité identifiés dans les formules de chèques (recommandation n° 7)

Afin de mieux lutter contre la falsification et la contrefaçon de chèque, la Banque de France a conduit un examen comparatif des exemplaires de spécimen de chèque des principaux établissements bancaires, afin d'identifier les éléments de sécurité présents dans les formules de chèque en circulation.

Cette démarche vise *in fine* à promouvoir l'adoption des meilleures pratiques de sécurisation des chèques, renforçant ainsi leur résistance à la contrefaçon. Elle doit s'accompagner d'une communication proactive sur ces éléments de sécurisation auprès du grand public et des acteurs du système de paiement par chèque, afin de leur permettre de détecter plus aisément les tentatives de fraude par contrefaçon.

14 L'article L. 131-86 du Code monétaire et financier dispose, depuis la loi n° 2025-1058 du 6 novembre 2025 – art. 4 que « *La Banque de France assure l'information de toute personne qui, lors de la remise d'un chèque pour le paiement d'un bien ou d'un service, souhaite vérifier la régularité, au regard du présent chapitre, de l'émission de celui-ci. / **Elle assure également l'information du banquier qui, lors de la présentation du chèque au paiement, souhaite vérifier la régularité, au regard du présent chapitre, de l'émission de ce chèque**. / L'origine de ces demandes d'information donne lieu à enregistrement.* »

15 Service officiel de la Banque de France qui permet aux bénéficiaires de chèques de consulter le FNCI.

16 L'article L. 131-84 du Code monétaire et financier dispose, depuis la loi n° 2025-1058 du 6 novembre 2025, article 3 que « *Le tiré qui a refusé le paiement d'un chèque pour défaut de provision suffisante, qui a clôturé un compte sur lequel des formules de chèque ont été délivrées, qui a enregistré une opposition pour perte ou vol de chèques ou de formules de chèque, qui a rejeté un chèque pour falsification ou contrefaçon ou qui a pris connaissance de la falsification ou de la contrefaçon de chèques ou de formules de chèque en avise, dans les meilleurs délais, la Banque de France. / Un décret précise les modalités, les conditions et les délais dans lesquels le tiré avise la Banque de France.* »

T4 Vue synthétique de la mise en œuvre des dix recommandations de l'Observatoire sur la fraude au chèque *(émises dans le rapport annuel 2020)*

Recommandation	Niveau de réalisation
Recommandation n° 1 : Révision de la collecte statistique de la Banque de France pour améliorer la connaissance des phénomènes de fraude au chèque	Réalisée.
Recommandation n° 2 : Améliorer les contrôles de la banque du remettant contre les remises frauduleuses	Possibilité au banquier remettant de consulter le FNCI selon sa politique de risque. Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France.
Recommandation n° 3 : Soutenir le développement des contrôles du côté de l'établissement tiré	Signalement au FNCI des cas de chèques contrefaits et falsifiés qui sont rejetés. Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France.
Recommandation n° 4 : Protéger les chèques du vol dans leur acheminement chez le client	En cours de mise en œuvre par les plans d'action, sous la responsabilité de chaque établissement et sous la supervision de la Banque de France.
Recommandation n° 5 : Simplifier les procédures de mise en opposition pour perte ou vol	En cours de mise en œuvre, sous la responsabilité de chaque établissement et sous la supervision de la Banque de France.
Recommandation n° 6 : Offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du Fichier national des chèques irréguliers (FNCI)	i) Déploiement en cours d'une offre dite « de mandataire spécifique » mise en place par le service Vérifiance-FNCI-Banque de France ; ii) Développement par les acteurs privés, les banques et les sociétés spécialisées dans la sécurité du chèque, d'outils de vérification des chèques avant acceptation embarquant la consultation du service Vérifiance-FNCI Banque de France. Cette vérification est dorénavant possible pour les banquiers présentateurs de chèques (article L. 131-86 du Code monétaire et financier).
Recommandation n° 7 : Renforcer la surveillance de la Banque de France sur la résistance physique des formules de chèques à la falsification et la contrefaçon	Réalisée.
Recommandation n° 8 : Assurer l'efficacité du service Vérifiance-FNCI-Banque de France contre la contrefaçon de chèque	Réalisée.
Recommandation n° 9 : Structurer durablement la coopération entre les acteurs dans la lutte contre la fraude et soutenir l'action des forces de l'ordre	Réalisée.
Recommandation n° 10 : Soutenir, par un plan de communication, la vigilance des utilisateurs dans l'usage du chèque	Réalisée.

Note : FNCI, Fichier national des chèques irréguliers.

Source : Observatoire de la sécurité des moyens de paiement.

2.3.2 Recommandations concernant la fraude aux paiements SEPA

Dans le cadre des travaux réalisés en 2024, l'Observatoire a formulé des recommandations à l'attention des secteurs public et privé, ainsi que des utilisateurs des services de paiement. Ces recommandations sont rappelées dans le tableau 5 *infra*. Le lancement en mai 2026 du fichier national des comptes bancaires signalés pour risque de fraude (FNC-RF) permet de répondre à la première recommandation.

CRÉATION DU FICHIER NATIONAL DES COMPTES BANCAIRES SIGNALÉS POUR RISQUE DE FRAUDE (FNC-RF)

Chaque prestataire de services de paiement utilise ses systèmes de détection de la fraude afin de protéger ses clients, mais jusqu'à présent, aucun partage d'information n'était possible en raison du secret bancaire. La loi contre la fraude bancaire du 6 novembre 2025, par l'article L. 521-6-1 du Code monétaire financier instituant le FNC-RF, permet aux prestataires de services de paiement de partager des événements de fraude se rapportant à des comptes de paiement et de dépôt. Il s'agit même d'une obligation réglementaire s'imposant à l'ensemble des prestataires de services de paiement établis en France, à l'exception des prestataires de services d'information sur les comptes et des établissements de paiement fournissant exclusivement un service d'initiation de paiement.

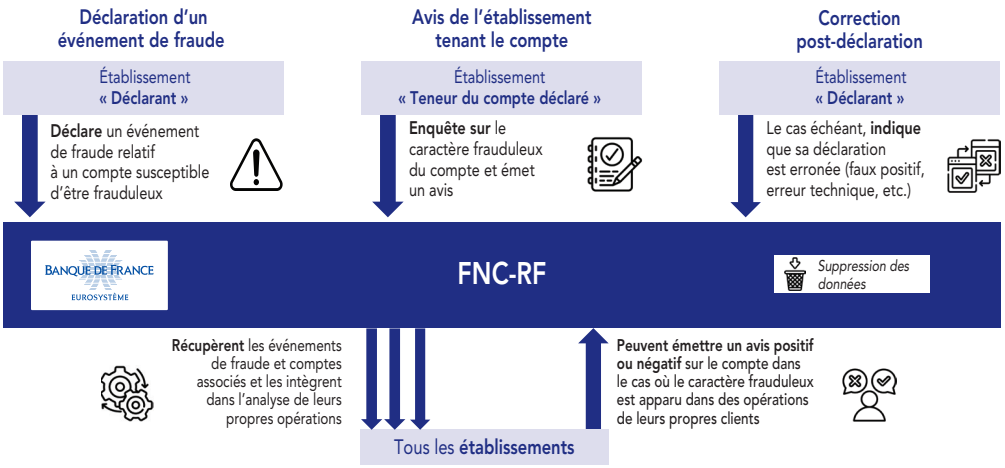
L'événement de fraude ainsi partagé comprend l'identifiant du compte (IBAN) et également les éléments permettant de caractériser la fraude, tels que la méthode utilisée par le fraudeur, la catégorie de fraude, le canal utilisé pour réaliser l'opération, etc.

Le FNC-RF, administré par la Banque de France, renforce ainsi l'efficacité des dispositifs internes de lutte contre la fraude de l'ensemble de l'écosystème.

Les futurs rapports annuels de l'OSMP présenteront des indicateurs permettant d'apprécier la performance de ce fichier, comme cela est prévu à l'article L. 141-4 du Code monétaire et financier.

Les choix techniques retenus dans le cadre de la mise en place de ce fichier visent en outre à optimiser son interopérabilité avec le futur dispositif européen de partage prévu à l'article 83 du futur règlement sur les paiements attachés à la révision de la deuxième directive européenne sur les services de paiement (DSP2).

Les fichiers de partage d'information entre des acteurs clés des paiements jouent un rôle essentiel dans la lutte contre la fraude et matérialisent la notion de bien commun attachée à la lutte contre la fraude. À cet égard, la loi du 25 juin 2026 relative à la lutte contre les fraudes sociales et fiscales a ouvert la consultation du FNC-RF aux sociétés de financement et à certaines administrations pour les aider à mieux lutter contre les types de fraude les concernant.



T5 Recommandations de l'Observatoire relatives aux virements et prélèvements SEPA *(émises dans le rapport annuel 2023)*

Recommandations	Destinataires
Faire évoluer le cadre réglementaire dans le but de permettre un partage entre établissements des données relatives aux fraudes détectées sur les virements et prélèvements.	Pouvoirs publics
Alerter le public sur les risques liés aux techniques de manipulation directe de l'utilisateur de services de paiement et l'y sensibiliser. Dans un contexte de sophistication des techniques d'ingénierie sociale par les fraudeurs, l'utilisateur de services de paiement est devenu une cible privilégiée.	Prestataires de services de paiement Pouvoirs publics Utilisateurs des services de paiement, qu'ils soient professionnels ou issus du grand public
Mettre en œuvre les bonnes pratiques suivantes lors de la réalisation d'un virement, d'autant plus s'il s'agit d'un virement instantané : • N'effectuez un virement que lorsque vous êtes certains de l'identité du bénéficiaire et de son IBAN. • Utilisez les services bancaires pour vérifier la concordance entre l'IBAN et l'identité du bénéficiaire. • En cas de doute ou d'incohérence, réalisez un contre-appel vers le bénéficiaire pour confirmer l'exactitude de ses coordonnées bancaires ou de son identité, en particulier si le prétendu bénéficiaire vous a communiqué un changement récent. • Ne réalisez jamais d'opération sous la pression et dans la précipitation, notamment lorsque l'opération est réalisée à la demande d'une personne se faisant passer pour votre conseiller ou pour un collaborateur du service des fraudes. • Pour réaliser un virement, privilégiez l'usage de l'espace de banque à distance, les solutions d'initiation de paiement ou les déplacements en agence bancaire. • Tout au long du processus de paiement, prêtez attention aux informations et avertissements relatifs à l'opération qui sont affichés par votre prestataire de services de paiement.	Utilisateurs des services de paiement, qu'ils soient professionnels ou issus du grand public
Rappeler les principes de fonctionnement du prélèvement bancaire et les risques associés. Ces actions de sensibilisation devraient en particulier décrire le rôle du créancier, du débiteur et de leurs prestataires de services de paiement respectifs dans la gestion du mandat de prélèvement, ainsi que les mesures de protection dont bénéficie le débiteur et les règles de vigilance qu'il doit appliquer. Notamment : • La vérification régulière des extraits de compte et la consultation des messages transmis par sa banque, et la nécessité de réagir au plus tôt en cas d'anomalie constatée. • La mise à disposition, par la banque du débiteur, de moyens de consultation des créanciers actifs prélevant son compte. • La possibilité d'indiquer les créanciers non autorisés à prélever son compte, ou à l'inverse, de limiter les créanciers autorisés à le faire, sous réserve d'une gestion rigoureuse de ces listes. • La possibilité de révoquer un mandat de prélèvement auprès de sa banque. • La possibilité de contester une opération de prélèvement (sans révocation du mandat associé) auprès de sa banque, étant rappelé les délais réglementaires durant lesquels il peut obtenir un remboursement auprès de sa banque : 8 semaines de façon inconditionnelle pour un prélèvement autorisé, 13 mois pour un prélèvement réalisé sans consentement (non autorisé). • La possibilité de bloquer toute opération de prélèvement sur un compte (cette option peut être utile en cas de compte secondaire, de compte en gestion extinctive, ou encore de compte uniquement utilisé pour recevoir et émettre des virements).	Prestataires de services de paiement Pouvoirs publics Utilisateurs des services de paiement, qu'ils soient professionnels ou issus du grand public
Protéger aussi rigoureusement que possible les données personnelles, et notamment les coordonnées bancaires (IBAN etc.), que les utilisateurs ont en leur possession dans leurs systèmes d'information et équipements informatiques, compte tenu des usages frauduleux pouvant survenir en cas de fuite de données.	Créanciers (entreprises, associations, administrations) Grand public

Note : IBAN – *international bank account numbers*, numéros de compte bancaire internationaux.

Source : Observatoire de la sécurité des moyens de paiement.

2.3.3 Recommandations en matière d'authentification forte des paiements par carte

En matière d'authentification forte des paiements par carte, l'Observatoire a publié ses recommandations dans son rapport annuel 2022. Celles-ci sont rappelées dans les tableaux T6 et T7.

T6 Principes généraux applicables à toutes les exemptions à l'authentification forte hors TRA *(formulés dans le rapport annuel 2022)*

Recommandations	Destinataires
Caractère non obligatoire et disponibilité de l'exemption Bien que les exemptions ne présentent pas de caractère obligatoire, les prestataires de services de paiement (PSP) sont invités à les mettre en œuvre dès lors qu'ils sont en capacité technique de le faire et que les conditions d'application définies dans les RTS sont respectées.	Prestataires de services de paiement
Responsabilité du prestataire de services de paiement du payeur en matière de sécurité Le PSP du payeur conserve en toutes circonstances la faculté de requérir une authentification forte de son utilisateur dès lors que son appréciation du niveau de risque de l'opération le justifie, quand bien même l'opération remplit les critères d'éligibilité à une exemption (*Questions and Answers* – Q&A – n° 4034 et 4480 de l'ABE).	Prestataires de services de paiement
Égalité de traitement entre prestataires de services de paiement À niveau de risque jugé équivalent, le PSP du payeur veille à répondre de façon équitable aux demandes d'exemption indépendamment de l'identité du PSP du bénéficiaire.	Prestataires de services de paiement

Note : TRA (*transaction risk analysis*), transactions à faible niveau de risque visées à l'article 18 des RTS (*regulatory technical standards*), normes techniques de réglementation émises par l'Autorité bancaire européenne (ABE).

Source : Observatoire de la sécurité des moyens de paiement.

T7 Principes spécifiques applicables à l'exemption TRA *(formulés dans le rapport annuel 2022)*

Recommandations	Destinataires
Respect du taux de fraude de référence par le PSP requérant l'exemption Les RTS prévoient qu'un prestataire de services de paiement (PSP) ne peut recourir à l'exemption TRA que si les deux conditions suivantes sont remplies : • il a déployé un mécanisme de contrôle des opérations en temps réel, intégrant les facteurs d'analyse spécifiés dans la réglementation dans une note de risque attribuée à chaque opération individuelle (article 18 des RTS, *Questions and Answers – Q&A – n° 4127*) ; • et si son taux de fraude pour le type d'opération concernée est suffisamment maîtrisé. Les taux de fraude de référence pour accéder à l'exemption TRA sont définis en annexe des RTS.	Prestataires de services de paiement
Taux de fraude à prendre en compte dans le cas des paiements par carte sur internet Dans le cas des transactions par carte sur internet, l'exemption TRA peut être requise par le PSP émetteur (TRA émetteur) ou par le PSP acquéreur (TRA acquéreur). Seul le taux de fraude de référence du PSP demandant le recours à l'exemption TRA doit être pris en considération (Q&A n° 4034 de l'ABE).	Prestataires de services de paiement
Responsabilité en cas de fraude En cas de fraude sur une transaction ayant bénéficié de l'exemption TRA, la réglementation dispose que la responsabilité financière est supportée par le PSP à l'origine de la demande de TRA [a].	Prestataires de services de paiement
Calcul des taux de fraude pour les paiements par carte L'Observatoire invite les PSP fournissant des services d'émission et d'acquisition à calculer des taux de fraude dissociés pour ces deux activités, et à considérer uniquement le taux de fraude relatif à leur rôle dans une transaction donnée.	Prestataires de services de paiement

a) Références : articles 73 et 74 de la deuxième directive européenne sur les services de paiement (DSP2), complétés par Q&A 4042 de l'Autorité bancaire européenne (ABE).

T7 Principes spécifiques applicables à l'exemption TRA (suite)

Recommandations	Destinataires
Suspension du droit d'usage de l'exemption TRA et notification à la Banque de France Conformément à l'article 20 des RTS, les PSP doivent informer immédiatement la Banque de France si : • leur taux de fraude, calculé pour les besoins de la TRA, dépasse l'un des taux de référence fixés par la réglementation, limitant ainsi leur capacité d'usage de l'exemption TRA ; • leur taux de fraude est au contraire redevenu conforme à l'un des taux de référence, libérant de nouveau leur capacité d'usage de l'exemption TRA.	Prestataires de services de paiement

Note : TRA (*transaction risk analysis*), transactions à faible niveau de risque visées à l'article 18 des RTS (*regulatory technical standards*), normes techniques de réglementation émises par l'ABE.

Source : Observatoire de la sécurité des moyens de paiement.

2.3.4 Recommandations issues des travaux de veille technologique de l'Observatoire

Dans le cadre de ses travaux de veille annuels, l'Observatoire adresse des recommandations à l'attention des acteurs de marché et des utilisateurs. Les principales recommandations émises au cours des dernières années sont reprises dans cette section. Pour disposer de l'étude de veille dans son exhaustivité, le lecteur est invité à se référer directement au rapport annuel correspondant.

T8 Recommandations relatives à l'usage de l'intelligence artificielle dans le cadre de la lutte contre la fraude *(rapport annuel 2024)*

Recommandations	Destinataires
Explorer à des fins de lutte contre la fraude l'apport de modules d'intelligence artificielle (IA) pour les modèles de contrôle et de notation des opérations de paiement	Tous les professionnels du secteur des paiements
Optimiser le périmètre de données utilisées dans les modèles de contrôle et de notation des opérations de paiement	Tous les professionnels du secteur des paiements
Instaurer un pilotage des modèles de contrôle et de notation des opérations de paiement reposant sur l'IA	Tous les professionnels du secteur des paiements

Source : Observatoire de la sécurité des moyens de paiement.

T9 Recommandations relatives à l'informatique quantique et la sécurité des systèmes de paiement par carte bancaire *(rapport annuel 2023)*

Recommandations	Destinataires
Inventorier les différents dispositifs de sécurité des systèmes d'information, et évaluer les vulnérabilités notamment par rapport aux standards actuels et au risque quantique.	Établissements de paiement Acteurs des systèmes de paiement
Hiérarchiser les données selon leur degré de sensibilité.	Établissements de paiement et Acteurs des systèmes de paiement
Expérimenter l'implémentation d'algorithmes asymétriques basée sur des systèmes hybrides et crypto-agiles.	Établissements de paiement Acteurs des systèmes de paiement
Constituer une feuille de route au niveau de chaque acteur de la chaîne de paiement.	Établissements de paiement Acteurs des systèmes de paiement
Sensibiliser les autorités de standardisation qui définissent la sécurité des protocoles de paiement afin d'arrêter des jalons et des choix en matière d'hybridation et de crypto-agilité.	Autorités de standardisation
Œuvrer à la création d'un groupe de travail pérenne de haut niveau, idéalement à l'échelle européenne, regroupant notamment les grandes institutions de paiement, les autorités publiques de supervision et de standardisation.	Groupe de travail européen

Source : Observatoire de la sécurité des moyens de paiement.

T10 Recommandations de l'Observatoire relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette *(rapport annuel 2022)*

Recommandations	Destinataires
Obtenir les certifications techniques nécessaires avant l'expérimentation ou le lancement commercial d'une solution d'acceptation SoftPOS.	Fournisseurs de solutions d'acceptation sur *smartphone* ou tablette
Sélectionner les environnements de déploiement en mettant en balance les avantages et les inconvénients en matière de sécurité par rapport aux terminaux de paiement traditionnels, et privilégier son utilisation dans les cas où le paiement par carte serait temporairement inaccessible.	Fournisseurs de solutions d'acceptation sur *smartphone* ou tablette
Mettre en place un programme d'actions et de contrôles destiné à assurer la sécurité dans le temps de ces équipements.	Fournisseurs de solutions d'acceptation sur *smartphone* ou tablette
Accompagner et former activement les commerçants utilisateurs d'applications SoftPOS aux enjeux de sécurité associés à ces équipements.	Fournisseurs de solutions d'acceptation sur *smartphone* ou tablette
Rester en veille active sur les failles des protocoles de communication et des équipements réseaux pour effectuer dès que possible les maintenances correctives sur les applications SoftPOS.	Fournisseurs de solutions d'acceptation sur *smartphone* ou tablette
Considérer l'équipement sur lequel est installée l'application SoftPOS comme un équipement aussi sensible qu'un terminal de paiement traditionnel et lui appliquer les mêmes principes de sécurité et de vigilance.	Commerçants
Appliquer les principes de sécurité applicables à tout *smartphone*.	Commerçants
Si la solution n'est pas accessible pour les personnes en situation de déficience visuelle, notamment en raison des écrans tactiles et des claviers virtuels, prévoir une solution alternative adaptée à ces utilisateurs.	Commerçants
Appliquer les règles de sécurité applicables à tout paiement par carte : garder en main votre carte et composer votre code PIN à l'abri de tout regard indiscret.	Consommateurs
Rester attentif à l'environnement dans lequel la transaction se fait et, en cas de doute, demander au commerçant de payer par un autre moyen (autre terminal ou autre moyen de paiement).	Consommateurs

Source : Observatoire de la sécurité des moyens de paiement.

T11 Recommandations de l'Observatoire relatives à l'identité numérique et la sécurité des paiements *(rapport annuel 2021)*

Recommandations	Destinataires
Recourir, dans le cadre des règles applicables en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT), à des moyens d'identification électronique de niveau substantiel ou élevé au sens du règlement (UE) n° 910/2014, à des services de confiance qualifiés et plus généralement à des services respectant les exigences du référentiel établi par l'Agence nationale de la sécurité des systèmes d'information (Anssi) applicables aux prestataires de vérification d'identité à distance.	Prestataires de services de paiement
Recourir à des moyens d'identification électroniques de niveau substantiel ou à des solutions d'identité numérique apportant un niveau de sécurité équivalent pour authentifier leurs utilisateurs pour l'accès aux espaces clients ou pour certaines opérations comme les demandes de carte SIM chez les opérateurs téléphoniques.	Fournisseurs et commerçants
Recourir aux moyens d'identification électronique de niveau substantiel ou élevé et aux services de confiance reconnus au sens de l'eIDAS, de type signature électronique avancée ou qualifiée, pour authentifier plus fortement leurs utilisateurs ou leurs contreparties au moment de certaines opérations sensibles (communication ou réception de nouvelles coordonnées bancaires, signature d'un mandat de prélèvement).	Administrations et entreprises
Utiliser, lorsque cela est possible, des solutions d'identité numérique sécurisées, par exemple celles certifiées de niveau substantiel ou élevé, à même de sécuriser leurs usages en ligne auprès des administrations comme des entreprises, et limiter ainsi les risques de divulgation de leurs données personnelles d'identité et de leurs données bancaires.	Utilisateurs

Source : Observatoire de la sécurité des moyens de paiement.

T12 Recommandations de l'Observatoire relatives à la sécurité des paiements en temps réel *(rapport annuel 2020)*

Recommandations	Destinataires
Mettre en œuvre, dans les conditions fixées par la DSP2, l'authentification forte des utilisateurs pour l'autorisation des paiements en temps réel et pour toute opération sensible périphérique (ajout d'un bénéficiaire, changement de coordonnées, etc.).	Prestataires de services de paiement (émetteurs)
Améliorer en continu les outils de prévention de la fraude en temps réel, notamment au moyen de technologies fondées sur l'apprentissage automatique, pour améliorer la performance des systèmes d'analyse de risques déployés.	Prestataires de services de paiement (émetteurs et receveurs)
Faire usage si nécessaire des mesures de paramétrage des droits, de types plafonds et limitations, pour limiter les préjudices d'un développement incontrôlé de la fraude.	Prestataires de services de paiement (émetteurs)
Identifier les opérations atypiques en réception, notamment quand celles-ci précèdent d'autres opérations en sortie.	Prestataires de services de paiement (receveurs)
Prêter une attention particulière, avant de valider l'ordre de paiement, à l'origine de la demande et l'identité de l'interlocuteur, et vérifier les coordonnées bancaires du bénéficiaire.	Utilisateurs
Saisir des données bancaires exclusivement sur des sites internet ou des applications mobiles réputés fiables et de confiance ; privilégier les sites et applications référencés et s'y connecter directement en considérant avec la plus grande prudence les liens reçus par des moyens de communication peu sécurisés, tels que les SMS et courriels.	Utilisateurs
Avertir, aussi rapidement que possible après l'exécution du paiement, son établissement bancaire de toute opération suspecte non autorisée ou frauduleuse.	Utilisateurs
Soutenir la vigilance des utilisateurs par la mise à disposition d'outils de confirmation du bénéficiaire et d'information active et en temps réel des opérations réalisées sur leur compte.	Prestataires de services de paiement

Source : Observatoire de la sécurité des moyens de paiement.

T13 Recommandations de l'Observatoire relatives à la sécurité des données de paiement *(rapport annuel 2019)*

Recommandations	Destinataires
Recourir, dans les conditions fixées par la DSP2 (notamment tous les quatre-vingt-dix jours pour la consultation de comptes), à l'authentification forte des utilisateurs pour l'accès aux services de paiement et à toute donnée sensible.	Prestataires de services de paiement
Mettre en place des dispositifs de détection des connexions suspectes.	Prestataires de services de paiement
Garder secrets tous les éléments qui servent à effectuer des paiements ; pour la carte, cette vigilance ne doit pas se limiter au seul code confidentiel, mais à l'ensemble des données présentes sur la carte et qui permettent de payer un achat sur Internet (numéro de carte, nom du titulaire, date d'expiration et cryptogramme) ; par ailleurs, le code confidentiel ne doit jamais être communiqué à un tiers ni stocké sur un support digital.	Utilisateurs
Saisir des données bancaires exclusivement sur des sites internet ou des applications mobiles réputés fiables et de confiance / privilégier les sites et applications référencés et s'y connecter directement, en considérant avec la plus grande prudence les liens reçus par des moyens de communication peu sécurisés tels que les SMS et courriels.	Utilisateurs
Dans le cas particulier de l'accès aux services de paiement, n'utiliser que des applications de confiance, notamment celles publiées par son fournisseur de services de paiement ou dont le fournisseur est dûment autorisé en France pour la prestation de services de paiement (c'est-à-dire présent dans l'annuaire Regafi ou dans le registre de l'Autorité bancaire européenne).	Utilisateurs
S'informer régulièrement sur les risques numériques et leurs évolutions au moyen, par exemple, du site du gouvernement *www.cybermalveillance.gouv.fr*	Utilisateurs

Note : DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T14 Recommandations de l'Observatoire relatives à la sécurité des paiements par mobile *(rapport annuel 2018)*

Recommandations	Destinataires
Mettre en œuvre des mécanismes fiables pour le stockage sécurisé des informations confidentielles dans la solution mobile (données sensibles de paiement, données d'identité, données d'authentification ou biométriques).	Prestataires de services de paiement et leurs prestataires techniques
Mettre en œuvre un mécanisme d'authentification forte de l'utilisateur au moment de l'enrôlement de son moyen de paiement dans l'application de paiement.	Prestataires de services de paiement
Mettre à disposition des utilisateurs les mises à jour correctives des solutions mobiles dès lors qu'une faille de sécurité de nature à altérer l'intégrité, la confidentialité ou la disponibilité du système ou des données est identifiée.	Fournisseurs de systèmes d'exploitation ou d'applications, fabricants de *smartphones*
Donner aux utilisateurs un niveau suffisant de visibilité sur les mesures de sécurité intégrées dans leurs applications tout en insistant sur le besoin de déployer des contre-mesures effectives pour lutter contre l'usage non autorisé de ces applications.	Prestataires de services de paiement
Évaluer régulièrement le niveau de sécurité des solutions de paiement par téléphone mobile.	Prestataires de services de paiement
Mettre à jour régulièrement le système d'exploitation de son téléphone mobile.	Utilisateurs
Choisir de manière non triviale et changer régulièrement les codes confidentiels, mots de passe et toute autre donnée personnelle utilisée pour les procédés d'authentification sur son *smartphone*, ou tout du moins pour ses applications de paiement.	Utilisateurs
Activer, si le système d'exploitation le permet, l'option d'effacement à distance des données en cas de perte ou de vol de son téléphone mobile.	Utilisateurs
N'utiliser que des applications de confiance, notamment celles recommandées par ses fournisseurs de services de paiement.	Utilisateurs
Éviter autant que possible de réaliser des transactions de paiement sur son téléphone mobile lorsque le canal de communication n'est pas fiable (par exemple connexion wifi publique non sécurisée).	Utilisateurs

Source : Observatoire de la sécurité des moyens de paiement.

3

LA SÉCURITÉ DES PAIEMENTS PAR CRYPTO-ACTIF

3.1 Introduction

L'émergence de nouvelles technologies, comme les technologies des registres distribués [1] (DLT, *Distributed ledger technologies*), a permis le développement de nouveaux types d'actifs financiers. Parmi eux figurent les « crypto-actifs » qui peuvent être échangés entre acteurs économiques et servir de support pour régler des transactions [2] de détail et des transactions financières sans recourir, en principe, aux instruments de paiement scripturaux ou fiduciaires, ni aux infrastructures de marché traditionnelles. Ces actifs constituent ainsi la pierre angulaire de la « finance décentralisée » (DeFi, *decentralised finance*), qui vise à s'affranchir des canaux centralisés traditionnels de la finance et des paiements. Cette décentralisation signifie que le contrôle des transactions, les décisions et les validations sont opérés par un réseau de participants, selon des mécanismes définis par le réseau sous-jacent, sans autorité centrale unique.

Les crypto-actifs sont définis comme des représentations numériques d'une valeur ou d'un droit, pouvant être transférées et stockées de manière électronique, au moyen d'une DLT, comme la chaîne de blocs (*blockchain*), ou d'une technologie similaire. Leur émission et leur distribution sont régulées dans l'Union européenne par le règlement européen MiCA [3]. Pour la suite de cette étude, on entend deux types d'actifs :

- les crypto-actifs dits de « première génération », comme le Bitcoin ou l'Ether, qui ne sont adossés à aucune réserve d'actifs et connaissent une forte volatilité de leur valeur, liée à la rencontre de l'offre et de la demande, par rapport aux monnaies ayant cours légal ;
- les crypto-actifs dits de « deuxième génération », les « *stablecoins* », apparus pour tenter de remédier à cette volatilité, qui sont souvent adossés à un actif financier traditionnel (devise, matière première, titre, etc.) ou à un panier d'actifs (indice boursier, etc.). Lorsqu'ils sont conçus pour être utilisés comme actifs de règlement, ils sont en règle générale adossés à une monnaie ayant cours légal, avec une parité de 1:1. Au regard du règlement MiCA et des précisions apportées par l'Autorité bancaire européenne (ABE), ils sont alors qualifiés de « jetons de monnaie électronique » [4] (EMT, *e-money tokens*) et intègrent la qualification d'unités de monnaie électronique [5] en matière d'encadrement réglementaire (notamment la deuxième directive européenne sur les services de paiement – DSP2 – et la deuxième directive sur la monnaie électronique – DME2 [6]).

3.1.1 Du point de vue des infrastructures

Concernant leur fonctionnement, les transactions sur crypto-actifs sont enregistrées dans une chaîne de blocs [7], et sont distribuées par un réseau généralement public et décentralisé. Celui-ci a pour objectifs de regrouper, de sécuriser et d'horodater les transactions par le biais de moyens cryptographiques, afin de garantir leur traçabilité et leur intégrité. Ces technologies, prises individuellement, présentent parfois des similitudes à celles utilisées pour sécuriser des paiements classiques. Toutefois, leur association à la technologie de chaîne de blocs permet un fonctionnement entièrement décentralisé, sans tiers de confiance chargé d'assurer une tenue de compte de référence. En effet, chaque participant, ou « nœud », à la chaîne de blocs détient une copie du registre des transactions identique à celle des autres participants, rendant les tentatives de falsification plus complexes.

1 « Registre distribué » : répertoire d'informations qui conserve un enregistrement des transactions et qui est partagé et synchronisé au sein d'un ensemble de nœuds de réseau DLT, au moyen d'un mécanisme de consensus (article 3 du règlement européen MiCA, *Markets in Crypto-Asset Regulation*).

2 Les usages des crypto-actifs à des fins de règlement pour l'achat d'autres crypto-actifs (y compris les crypto-actifs uniques et non fongibles ou les actifs réels représentés sous la forme de jetons) sont exclus du périmètre de l'étude.

3 Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés des crypto-actifs.

4 EMT : « *e-money token* » émis par un établissement de monnaie électronique (EME) ou de crédit (EC).

5 Article L. 315-1 du Code monétaire et financier (CMF I. et II. : « La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique […] et les unités de monnaie électronique sont dites unités de valeur ».

6 Directive européenne (UE) 2015/2366 relative aux services de paiement (DSP2), et directive 2009/110/CE sur la monnaie électronique (DME2).

7 Pour en savoir plus : « La *blockchain* », Banque de France, ABC de l'Économie, *L'Éco en Bref*.

3.1.2 Du point de vue des acteurs

En pratique, l'accès direct à la chaîne de blocs requiert des compétences et des moyens informatiques difficilement accessibles pour les utilisateurs traditionnels de paiement de détail, qu'il s'agisse de commerçants ou de particuliers. En conséquence, la mise en œuvre du paiement de détail par crypto-actif repose sur le recours à des intermédiaires spécialisés. Ces derniers délèguent ensuite l'exécution des échanges d'unités de crypto-actifs à travers la chaîne de blocs.

Tout au long du parcours de paiement par crypto-actif, divers acteurs interviennent en effet pour faciliter la réalisation du paiement, depuis l'utilisateur final jusqu'au commerçant acceptant ce mode de règlement. Ainsi, afin de relier les diverses parties prenantes aux paiements par crypto-actif, peuvent intervenir des acteurs comme les émetteurs de crypto-actifs, les plateformes d'échange [8] et les institutions bancaires, qui ont notamment la charge de reverser au commerçant le montant de la transaction en euros.

3.1.3 Des ponts avec le secteur des paiements « traditionnels » existent

Dans la quasi-totalité des cas, le commerçant préfère recevoir son paiement en monnaie ayant cours légal, c'est-à-dire en euros, ce qui nécessite une conversion préalable des crypto-actifs qui sont utilisés par le payeur avant que le produit de cette conversion ne soit reversé au commerçant. Pour ce faire, différents parcours sont possibles, selon le type de paiement par crypto-actif : QR code [9], carte de paiement ou portefeuille de crypto-actifs. Cette conversion implique une association de services sur crypto-actifs et de services de paiement traditionnels.

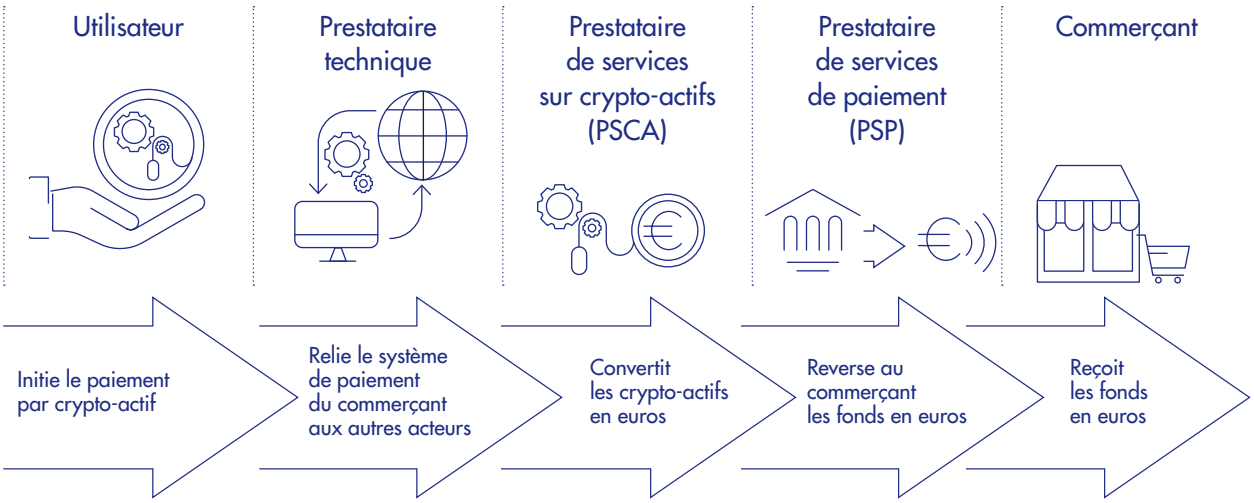
3.1.4 Les objectifs de cette étude

Dans le cadre du mandat de l'Observatoire, la présente étude se concentre sur l'analyse de la sécurité des paiements de détail par crypto-actif en France.

Les autres risques liés [10] à la détention ou à l'usage de crypto-actifs (risques de marché, de crédit, de liquidité ou encore de blanchiment de capitaux) ne sont donc pas évoqués dans le cadre de cette étude, mais doivent néanmoins être pris en considération par les acteurs qui souhaitent détenir ou échanger des crypto-actifs, ou plus largement, offrir des services sur crypto-actifs. De même, ce rapport ne se concentrera pas sur les aspects strictement juridiques des paiements par crypto-actif [11], ni sur les aspects fiscaux liés à de tels paiements.

Cette étude vise ainsi à dresser, pour la France, un panorama des solutions de paiement par crypto-actif à la suite de l'entrée en application du règlement européen MiCA, et à identifier les enjeux de sécurité propres aux paiements par crypto-actif. L'Observatoire émet, dans ce cadre, des recommandations en la matière.

S1 PANORAMA DES ACTEURS POUR UN PAIEMENT PAR CRYPTO-ACTIF



Source : Observatoire de la sécurité des moyens de paiement.

3.2 La typologie des paiements par crypto-actif

Les crypto-actifs de première génération (à l'instar du Bitcoin) peuvent être techniquement utilisés dans le cadre de paiements. Dans les faits toutefois, ils ne sont pas adaptés aux paiements du quotidien en raison de la volatilité de leur valeur, ainsi que des frais et délais associés à chaque transaction. C'est pourquoi l'analyse ci-après se concentre principalement sur les cas d'usage de paiement par *stablecoins*, tout en englobant, à la marge, certains cas d'usage de paiement par crypto-actif de première génération. En effet, dès lors que le commerçant préfère, en pratique, être réglé en euros, l'usage de *stablecoins* permet notamment une limitation du risque de change et de volatilité par rapport aux autres crypto-actifs lors de la conversion en monnaie ayant cours légal.

Il est à noter, de façon préliminaire, que **les crypto-actifs sont très peu utilisés dans les paiements de détail à ce jour sur le territoire français**. En effet, moins de 3 % [12] des Français indiquaient, en 2023, avoir déjà utilisé des crypto-actifs à des fins de paiement. *A fortiori*, le nombre de commerces de détail référencés acceptant directement le paiement par crypto-actif en France en 2025 est très faible. Par exemple pour le Bitcoin, il existe environ 300 accepteurs pour un total de 300 000 points de vente, ce qui représente seulement 0,1 % des points de vente totaux.

En outre, les crypto-actifs, dont les *stablecoins*, sont utilisés pour réaliser des opérations d'achat et de vente sur d'autres crypto-actifs, mais ils ne servent en pratique que très marginalement à l'achat de biens et de services traditionnels. En dehors des paiements de détail réalisés en France, on observe néanmoins le développement de l'utilisation des *stablecoins*, en particulier ceux régulés par MiCA. Ils sont essentiellement utilisés pour des transactions sur des marchés financiers, pour des paiements transfrontaliers entre professionnels et pour de la gestion de trésorerie, y compris à l'échelle de groupes.

3.2.1 Les paiements de proximité

D'un point de vue pratique, les paiements au point de vente par crypto-actif s'effectuent en s'appuyant sur des instruments similaires à ceux mis à disposition pour les paiements traditionnels. L'**initiation du paiement** passe ainsi, soit par le terminal de paiement électronique (TPE) du commerçant, qui génère un QR code comportant les informations relatives à la transaction, soit par la carte de paiement du client, qu'il s'agisse de la carte en elle-même ou qu'elle soit intégrée dans son mobile. Dans tous les cas, la solution d'**acceptation du paiement** par crypto-actif peut, quant à elle, être intégrée au système de caisse, ou alors être émise sur un support tel qu'une tablette ou un téléphone, utilisés comme solution d'encaissement mobile (*SoftPos*).

Dans le cas du paiement par QR code au point de vente, le client scanne, en premier lieu, le QR code généré par le TPE du commerçant. Selon les possibilités offertes par le commerçant, il choisit alors i) sa plateforme d'échange, ii) son portefeuille de crypto-actifs (s'il en dispose de plusieurs), puis iii) le crypto-actif avec lequel il souhaite payer. À l'étape suivante, le payeur valide l'opération auprès de la plateforme d'échange ou de l'émetteur d'EMT, qui la transmet ensuite au réseau de la chaîne de blocs. Enfin, la transaction est confirmée et la vente finalisée. S'ensuit une phase de conversion qui est neutre pour le payeur en matière de parcours client, pendant laquelle le paiement transite par une passerelle de paiement, chargée d'établir le lien entre les crypto-actifs et les canaux bancaires traditionnels (SEPA, etc.). La plateforme d'échange, ou l'émetteur d'EMT, convertit les crypto-actifs en monnaie ayant cours légal, et le montant en euros est ensuite reversé au commerçant par un prestataire de services de paiement.

Dans le cas du paiement par carte bancaire de proximité, le paiement passe par la mise en contact de la carte, aussi bien physique que virtuelle, avec un terminal de paiement. La carte est généralement préalimentée en crypto-actifs ou connectée à un portefeuille de crypto-actifs. Plusieurs options existent dans le choix du crypto-actif à utiliser pour le paiement. En principe, un choix par défaut est effectué par l'utilisateur pour les opérations à venir. Mais le choix peut basculer de façon automatique vers

8 Ces plateformes d'échange ont pour rôle de convertir les crypto-actifs présents sur le portefeuille de crypto-actifs (*wallet*) de l'utilisateur.

9 Le paiement par QR (*Quick Response*) code correspond à une solution de paiement numérique qui consiste, pour un payeur, à scanner un code bidimensionnel avec son téléphone afin d'initier la transaction.

10 « Crypto-actifs : l'AMF appuie l'appel à la prudence lancée par l'ESMA à destination des investisseurs individuels », AMF (18 décembre 2024). Pour rappel, les crypto-actifs sont très risqués car leur protection est faible de manière générale, et sont généralement moins encadrés que la plupart des autres types d'actifs, avec des acteurs parfois non régulés.

11 *Rapport sur l'évolution de la notion juridique de monnaie*, Haut Comité Juridique de Place (HCJP), juin 2025.

12 « Quel avenir pour le monde des crypto-actifs ? », Banque de France, 17 octobre 2024.

un autre actif lorsque le solde de crypto-actifs utilisés par défaut ne couvre pas la totalité du paiement. La conversion en monnaie ayant cours légal a ensuite lieu par le biais des passerelles de paiement sur une plateforme d'échange ou un autre prestaire de services sur crypto-actifs (PSCA), de façon identique au paiement par QR code. Enfin, la transaction s'effectue par l'intermédiaire des réseaux traditionnels de paiement par carte, jusqu'à réception des fonds par le commerçant, par l'intermédiaire de son prestataire de services de paiement (PSP).

Pour ces deux types de solutions de paiement par crypto-actif au point de vente, une connexion internet est le plus souvent nécessaire pour valider l'opération. Toutefois, selon le support [13] de paiement utilisé, il est parfois possible de payer hors-ligne, c'est-à-dire sans connexion internet directe, en utilisant la technologie NFC [14] ou par QR code.

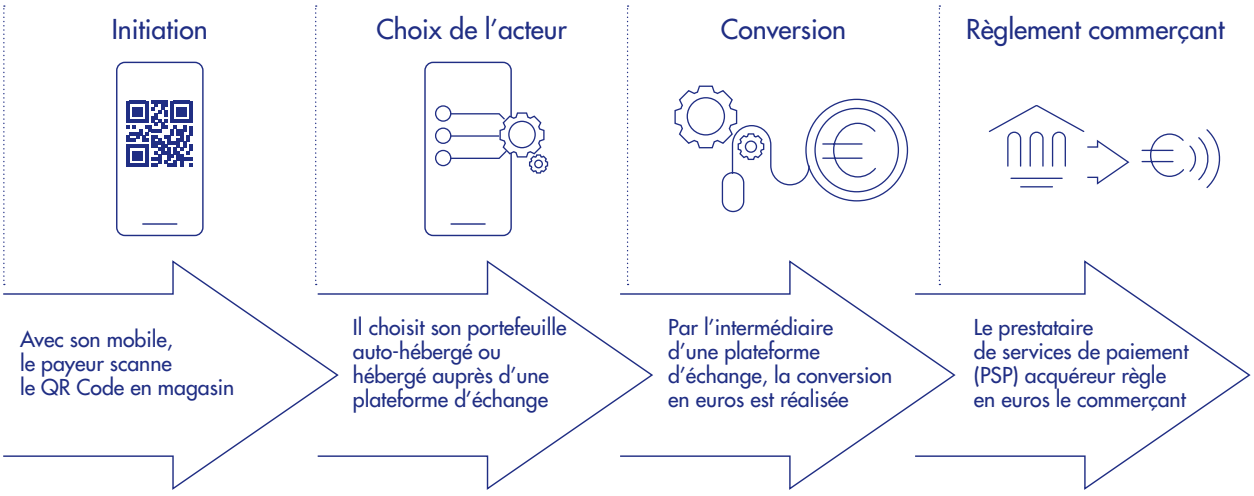
3.2.2 Les paiements à distance

Le paiement à distance par crypto-actif peut s'effectuer comme un paiement en *e-commerce* par un moyen de paiement classique (tel que la carte, le virement, ou à partir d'un compte de monnaie électronique), soit en se rendant sur le site du commerçant, soit à partir d'un lien de paiement généré par le commerçant. La possibilité de payer par crypto-actif apparaît alors au moment de choisir le moyen de paiement, au côté des autres moyens de paiement possibles. Ensuite, le paiement se déroule comme décrit précédemment, avec le choix de l'actif dans le portefeuille électronique, la réalisation de la transaction, puis la conversion pour régler le commerçant en monnaie ayant cours légal.

3.2.3 Les paiements de portefeuille à portefeuille

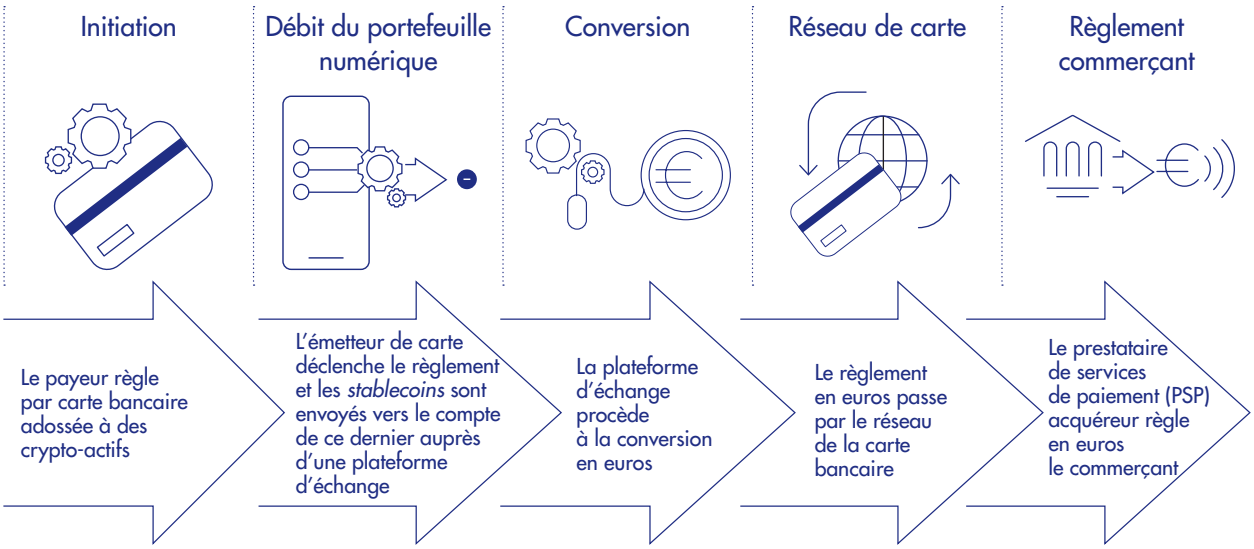
Une alternative existe, avec un usage très rare, lorsque l'utilisateur et le commerçant disposent tous les deux d'un portefeuille de crypto-actifs. Le paiement se fait alors par crypto-actif, directement d'un portefeuille à un autre, sans conversion en monnaie ayant cours légal. Ce cas de figure est quasi inexistant en France et concerne aussi bien les paiements à distance que ceux de proximité. Les risques sont accrus pour l'utilisateur dans le cas d'un paiement réalisé directement de portefeuille à portefeuille, lorsque les portefeuilles sont autohébergés (portefeuilles *non-custodial*) [15], ou d'un paiement par des crypto-actifs autres que des EMT.

S2 FLUX DE PAIEMENT DE PROXIMITÉ PAR QR CODE



Source : Observatoire de la sécurité des moyens de paiement.

S3 FLUX DE PAIEMENT DE PROXIMITÉ PAR CARTE BANCAIRE



Source : Observatoire de la sécurité des moyens de paiement.

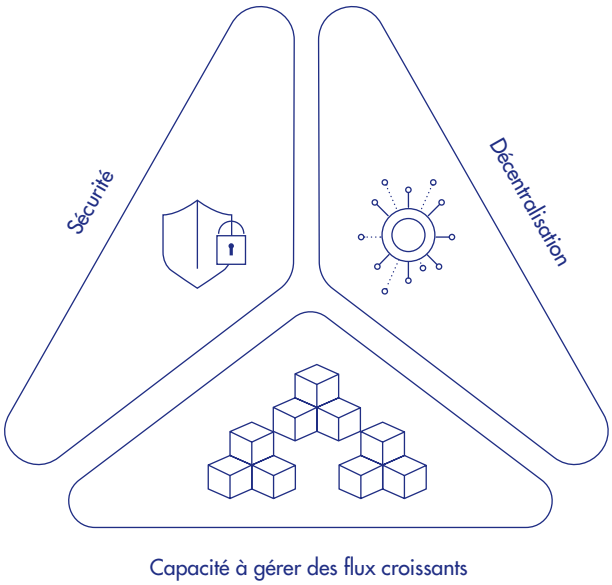
3.3 Le fonctionnement technique sous-jacent

Le principe de la chaîne de blocs réside en une infrastructure informatique implémentant des protocoles techniques, qui permettent le fonctionnement de l'ensemble du système.

Il existe deux grandes catégories de chaînes de blocs, déterminées par le mode de participation : permissionnée (souvent privée) et non permissionnée (souvent publique). Sur le plan technique, la méthode de fonctionnement est identique pour les deux catégories. Ce qui les distingue sont leurs accès. En matière de chaîne de blocs privée, les opérations ne sont visibles que par les participants ayant la permission d'y accéder. L'accès est donc limité et par conséquent la transparence partielle. *A contrario*, lorsque la chaîne de blocs est publique, les opérations sont visibles par tous et réputées immuables, avec des frais de réseau parfois élevés.

En phase de conception d'une chaîne de blocs, les principaux objectifs recherchés sont i) la sécurité du réseau, ii) sa décentralisation (contrôle effectué par plusieurs acteurs) et iii) sa scalabilité (capacité à faire un grand nombre de transactions, plus rapidement et à moindres frais). Ces objectifs sont difficilement conciliables, ce qui constitue une forme de trilemme. Le fonctionnement des chaînes de blocs a donc évolué au cours des dernières années pour trouver un équilibre optimal, en fonction des usages et des attentes du marché.

S4 TRILEMME DE LA CHAÎNE DE BLOCS



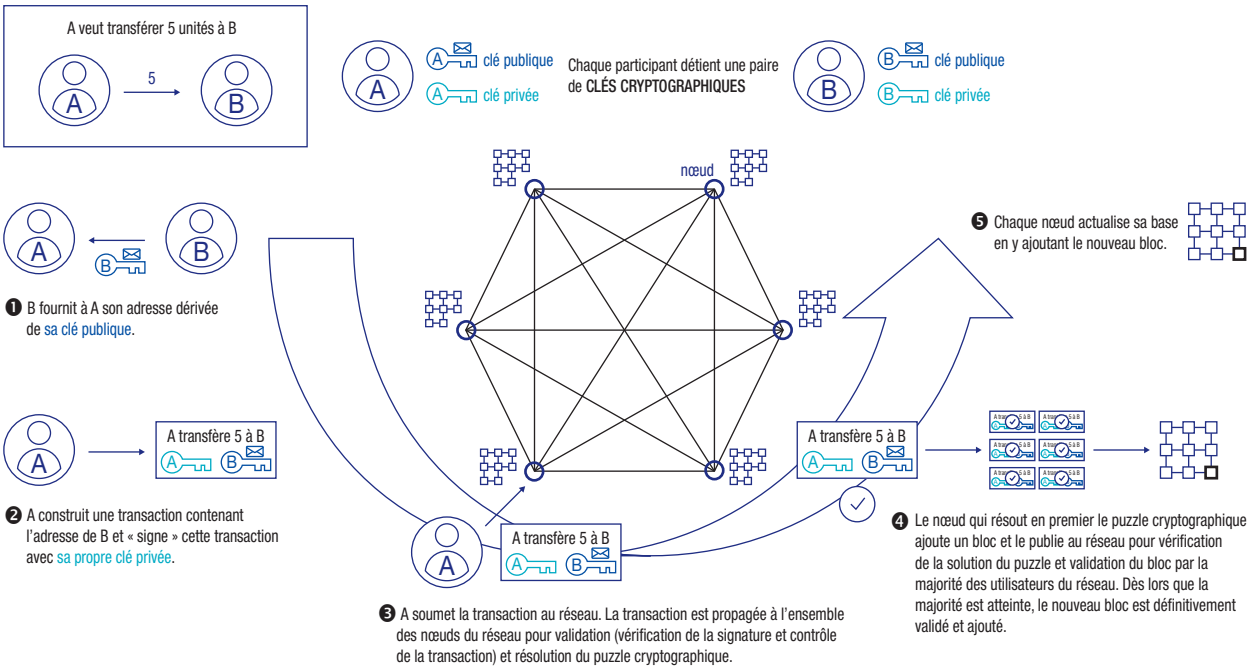
Source : Observatoire de la sécurité des moyens de paiement.

13 Portefeuille « *self-custody* », portefeuille matériel (*hardwallet*) ou cartes de paiement spécifiques.

14 « *Near Field Communication* » : technologie permettant un partage de données à très courte portée entre des appareils compatibles.

15 Dans ce cas, les clés privées sont stockées localement sur l'appareil.

S5 VALIDATION D'UNE TRANSACTION DANS UNE CHAÎNE DE BLOCS À PREUVE DE TRAVAIL



Source : Banque de France (ABC de l'Économie, *L'Éco en Bref*, « La *blockchain* »).

3.3.1 Les chaînes de blocs natives

À l'origine, la chaîne de blocs repose sur une première couche, dite « couche 1 », qui permet d'enregistrer des transactions directement sur la chaîne (*on-chain*). Elle garantit la sécurité et la décentralisation du processus par des mécanismes de consensus [16]. Ces derniers consistent, pour un réseau de nœuds [17], à valider les transactions, sans l'intervention d'une autorité centrale, en utilisant différents protocoles [18]. Cette chaîne de blocs dite « d'infrastructure » a des fonctionnalités de sécurité, gouvernance, consensus et exécution.

La structure de ce sous-jacent technologique se décompose principalement en trois volets :

- **le réseau**, qui s'apparente à plusieurs ordinateurs ou serveurs – nœuds –, qui exécutent un algorithme afin de sécuriser le système en recevant les transactions, les validant selon les règles du protocole utilisé et stockant les blocs ;
- **les blocs**, qui comprennent un ensemble de transactions, dont le nombre peut varier selon la chaîne utilisée ;
- et **une chaîne**, qui relie les blocs de bout en bout en utilisant des moyens cryptographiques [19], à travers un hachage. Ce hachage consiste en une empreinte digitale non modifiable, permettant de sécuriser la transaction. En pratique, les données contenues dans le bloc précédent sont chiffrées, et ainsi figées.

Le délai d'exécution peut s'avérer long et coûteux en fonction de plusieurs facteurs :

- le nombre d'ordinateurs en charge de valider l'opération. Selon le réseau et le nombre de validateurs actifs, le traitement des transactions peut être plus ou moins rapide ;
- les frais. Les transactions avec des frais de réseau plus importants sont priorisées par les « nœuds », car c'est par ce biais que les validateurs de ces nœuds sont rémunérés. Ces frais sont plus communément appelés « frais de gaz » (« *gas fee* », soit les frais de réseau).

- la congestion du réseau. Le nombre de nœuds [20] actifs étant fixe, si les transactions s'accumulent, elles peuvent être mises en attente avant de disposer d'un nouveau bloc qui pourra les contenir.

⇨ Pour des opérations de faible montant, les frais de réseau ne sont pas négligeables et la transaction peut mettre une dizaine de minutes à être validée, voire parfois davantage, avec un risque de congestion du réseau. Pour ces raisons, les paiements par crypto-actif reposant sur la couche 1 ne semblent pas adaptés à la réalisation d'achats de biens ou de services au quotidien, et ne sont donc pas – ou très rarement – utilisés comme tels. Cette complexité technique explique notamment l'utilisation marginale, voire quasi inexistante, des crypto-actifs au sens strict parmi les solutions de paiement proposées par les professionnels en France. Ces actifs sont ainsi presque exclusivement utilisés comme actifs spéculatifs à des fins d'investissement.

3.3.2 Les chaînes de blocs spécifiques

L'introduction d'une couche supplémentaire de blocs, dite « couche 2 », vise à accélérer et à améliorer les performances de l'ensemble de la chaîne de blocs. Pour ce faire, les transactions sont traitées en dehors de la chaîne de blocs principale (*off-chain*), puis validées dans la couche 1. Les transactions sont ainsi agrégées et traitées en masse, ce qui permet de gérer un plus grand nombre de transactions et de réduire les coûts associés.

Cette couche 2 est en constante évolution au gré de l'innovation et plusieurs modèles existent à l'heure actuelle. Par exemple, le protocole « *rollup* optimiste » part du postulat que les transactions sont valides en l'absence de preuve de fraude par les mécanismes de détection. Le séquenceur, composant opérationnel du *rollup*, va collecter, ordonner et exécuter plusieurs opérations en dehors de la chaîne de blocs. Il traite donc plus rapidement les transactions, et réduit ainsi les frais. Les transactions sont, par ce moyen, regroupées en lot [21]. Dans ce cas, un résumé de l'ensemble des transactions est publié sur la couche 1 et les transactions ne sont pas vérifiées immédiatement sur cette couche 1. Une vérification détaillée peut avoir lieu, *a posteriori*, pendant la période de contestation en cas de fraude. Sur la chaîne de blocs de couche 2, des « contrats intelligents » (*smart contracts* [22]) applicatifs vont permettre de traiter toutes les étapes et, sur la chaîne de base en couche 1, des contrats intelligents de contrôle vont ensuite permettre d'assurer la sécurité. Une autre méthode, utilisée par le « *ZK rollup* [23] » (*zero-knowledge rollup*), consiste à sécuriser davantage les opérations en générant des preuves cryptographiques pour les garantir. Ces preuves sont ainsi enregistrées sur la couche 1 sans révéler les détails des transactions.

Très récemment, une « couche 3 » a également émergé. Il s'agit d'une couche applicative améliorant l'interopérabilité entre couches. La couche 3 vise ainsi à connecter les couches 1 et 2 de la chaîne de blocs avec les applications et services inhérents, sans l'intervention d'un tiers.

Ces couches supplémentaires qui viennent s'ajouter à la chaîne de blocs d'origine jouent un rôle essentiel dans le développement de ces nouvelles technologies. Elles garantissent la possibilité d'accroissement de l'écosystème et l'interaction de ses composantes.

⇨ L'interopérabilité constitue en effet un enjeu intrinsèque des aspects technologiques. Chaque réseau de chaîne de blocs dispose de ses propres standards, ce qui rend ainsi nécessaire l'utilisation de passerelles et génère donc un premier point de vulnérabilité potentiel sur la chaîne de paiement.

16 Processus défini en amont, par lequel la transaction s'effectue.

17 Réseau composé de machines/ordinateurs qui contribuent au stockage, à la validation/vérification et à l'échange d'informations sur les transactions.

18 Preuve de travail (*proof of work*) ou preuve d'enjeu (*proof of stake*).

19 La sécurité cryptographique est intégrée dans le protocole de la chaîne de blocs, de sorte que l'utilisateur final dispose d'une clé privée pour signer la transaction. La vérification de la signature s'effectue de façon décentralisée, avec une clé publique.

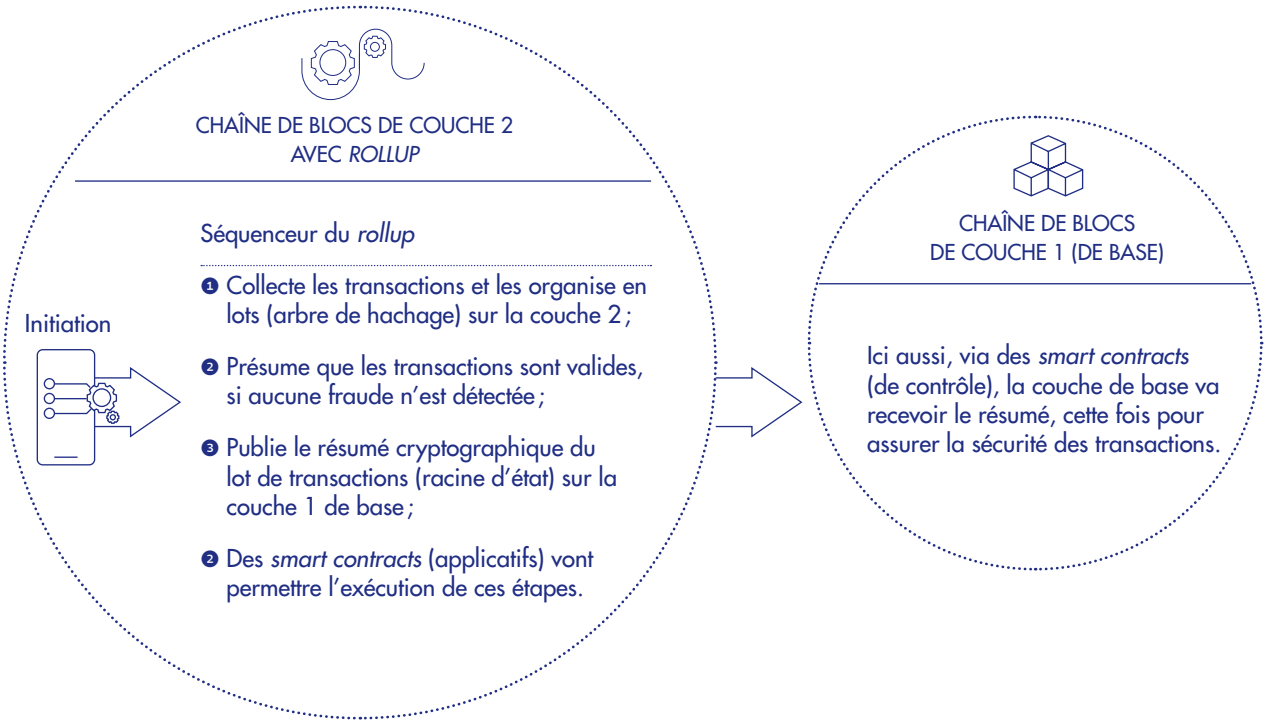
20 Par exemple, le nombre de nœuds pour les principaux réseaux : jusqu'à 2 500 pour Bitcoin, 1 400 pour Ethereum, 5 000 pour Solana ou 2 000 pour Polygon.

21 Elles sont regroupées et organisées selon un « arbre de hachage » (ou arbre de *Merkle*). Il s'agit d'une structure de données utilisée en cryptographie pour réduire les quantités de données qui doivent être conservées dans une chaîne de blocs à des fins de vérification. Le hachage de la racine résume toutes les données contenues individuellement dans chaque transaction traitée au sein du même lot.

22 Programme autonome déployé sur une chaîne de blocs, qui exécute automatiquement des règles prédéfinies.

23 Rapport sur la finance décentralisée, *Decentralised Finance (DeFi)*, *European Union Blockchain Observatory and forum* (Observatoire et Forum de la blockchain de l'Union européenne), 24 mai 2022 : *« Un* Zero-Knowledge (ZK) rollup *est une solution de mise à l'échelle qui exécute les transactions hors chaîne, puis publie sur la couche 1 une preuve cryptographique de validité (*Zero-Knowledge Proof*). Cette preuve garantit la conformité des transactions sans divulguer leurs données, ce qui réduit la quantité d'informations à publier sur la* blockchain *principale »*.

S6 ILLUSTRATION DU « *ROLLUP* », PROTOCOLE D'UNE CHAÎNE DE BLOCS DE COUCHE 2



Source : Observatoire de la sécurité des moyens de paiement.

3.4 Les enjeux de sécurité

Les risques auxquels sont exposés les paiements par crypto-actif sont de deux ordres : i) les risques « classiques », affectant l'utilisation des moyens de paiement traditionnels, et ii) les risques plus spécifiquement attachés à l'utilisation des crypto-actifs, qui ont trait aux caractéristiques techniques inhérentes à ces nouveaux actifs de règlement.

3.4.1 Les risques dits « classiques »

Bien qu'il ne s'agisse pas d'une caractéristique propre aux paiements par crypto-actif, il est essentiel de souligner, à titre liminaire, que les arnaques et fraudes en ligne qui utilisent les crypto-actifs comme supports se sont accrues. Elles doivent donc constituer un point d'attention majeur pour les utilisateurs potentiels.

De façon générale, lorsque le paiement par crypto-actif est réalisé avec une carte de paiement classique, l'utilisateur est exposé aux risques attachés à une transaction par carte. En matière de sécurité, les normes ISO [24] avec des champs cryptographiquement protégés sont souvent utilisées. De plus, les données de paiement sont chiffrées par l'utilisation d'algorithmes de chiffrement symétrique (AES – *Advanced Encryption Standard*) et asymétrique (RSA – du nom des initiales de ses trois inventeurs). Parallèlement, la chaîne de traitement du paiement est certifiée par la norme de sécurité des données de l'industrie des cartes de paiement PCI-DSS (*Payment Card Industry – Data Security Standard*). Cependant, les chiffrements actuels ne sont pas tous post-quantiques et peuvent ainsi présenter une vulnérabilité face aux attaques.

⇨ Mettre en place des démarches d'adaptation au chiffrement post-quantique s'avère donc nécessaire, conformément aux recommandations [25] déjà édictées par l'Observatoire afin de prévenir ce risque de résilience opérationnelle.

De même, l'utilisation du QR code peut également constituer une faille, notamment car les fraudeurs peuvent le falsifier (*quishing*). Dans ce cas, le fraudeur remplace le QR code du commerçant par le sien afin de recevoir les paiements à la place du commerçant. Ce procédé

a déjà été observé dans le cadre de l'utilisation de ce mécanisme d'initiation de paiement. En effet, certains commerçants mettent à disposition de leur clientèle un QR code statique, qui constitue un facteur de risque, car ce type de QR code n'est pas limité dans le temps et peut donc être plus facilement falsifiable.

⇨ Le QR code dynamique, quant à lui, possède une durée limitée et permet ainsi de réduire le risque de fraude associé à ce mécanisme.

De manière générale, la multiplicité des acteurs intervenant dans le processus de paiement par crypto-actif, tel que décrit précédemment, affecte la fluidité de l'acte de paiement (et prolonge donc sa durée). De surcroît, cette multitude d'intervenants compromet la résilience de la chaîne des paiements, en introduisant autant de points de vulnérabilité potentiels.

En outre, ces solutions de paiement présentent une résilience moindre que les paiements scripturaux classiques. Par exemple, une panne récente chez un important fournisseur *cloud*[26] a provoqué des interruptions dans les services de plusieurs acteurs de la sphère des crypto-actifs. Ce dysfonctionnement a concerné l'accès aux réseaux de chaînes de blocs, aux interfaces de programmation d'application (API – *Application Programming Interface*) de paiement et aux portefeuilles électroniques des utilisateurs. La capacité de résilience repose également sur les choix d'hébergement. La concentration vers un nombre limité de fournisseurs de services critiques – c'est-à-dire qui peuvent influer sur la sécurité et la performance du dispositif – peut effectivement soulever des difficultés lorsque la réplication des données est effectuée auprès de deux sites appartenant à un même fournisseur *cloud*.

⇨ Le renforcement du Plan d'Urgence et de Poursuite des Activités (PUPA) est donc une nécessité face aux éventuels risques de résilience opérationnelle, qui sont largement accrus par l'utilisation de crypto-actifs comme moyens de paiement et par la multiplicité des acteurs qui interviennent lors de ces parcours de paiement.

3.4.2 À ces risques dits « classiques », s'ajoutent de nouveaux risques spécifiques à l'utilisation des crypto-actifs

3.4.2.1 Le risque de sécurité des chaînes de blocs

Les chaînes de blocs reposent sur des principes de cryptographie, de décentralisation et de consensus, qui visent à assurer leur sécurité de manière intrinsèque. Ces principes natifs ne sont pour autant pas infaillibles, à plus forte raison dans le contexte actuel d'accumulation des couches, qui a pour objectif d'optimiser le fonctionnement des chaînes de blocs.

La sécurité des chaînes de blocs dépend donc fortement de la robustesse des infrastructures techniques et des protocoles sous-jacents. La fiabilité des nœuds, la résilience des fournisseurs *cloud*, la sécurité des API et la sécurité des « contrats intelligents » sont autant de facteurs critiques à prendre en compte.

⇨ Dans ce contexte, une évaluation rigoureuse de la solidité opérationnelle des composants techniques est indispensable pour garantir la sécurité des paiements par crypto-actif.

3.4.2.2 Le risque de perte/vol de clés privées et de fuites de données

Il existe différentes sortes de portefeuilles de crypto-actifs. Les deux principaux sont le portefeuille physique (*hard wallet*) et le portefeuille numérique (*hot wallet* ou *software wallet*). Le premier dispose de clés privées stockées sur un support, comme une clé USB ou une puce sécurisée. Le second possède des clés privées stockées sur un appareil connecté à internet, lorsqu'il s'agit d'un portefeuille autohébergé, ou en ligne sur un serveur distant, pour tout portefeuille hébergé (portefeuille *custodial*)[27]. Des clés asymétriques sont ainsi utilisées pour sécuriser les portefeuilles numériques avec, d'une part, la clé privée pour signer la transaction et, d'autre part, la clé publique pour recevoir les fonds. Par conséquent, pour un achat, l'utilisateur final de la chaîne de blocs va disposer d'une clé privée pour signer la transaction sur son portefeuille numérique, tandis que la clé publique – assimilable à l'identité bancaire d'un compte classique – consiste en l'adresse de réception des fonds. Cette clé publique peut, par exemple, être communiquée par le biais du QR code présenté par le commerçant au client.

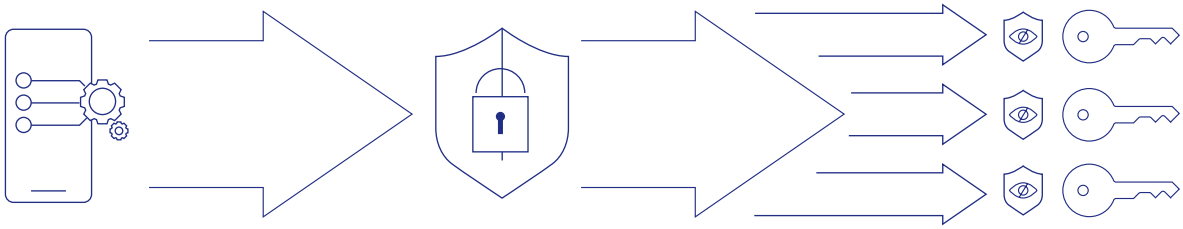
24 Normes définies par l'Organisation internationale de normalisation (ISO) et s'appliquant aux produits et aux services.

25 Chapitre 3 (pages 73-90) du *Rapport annuel de l'OSMP 2023* : « L'informatique quantique et la sécurité des systèmes de paiement par carte bancaire ».

26 Prestataire de services informatiques (hébergement d'infrastructure, de données, etc.).

27 Les clés privées sont conservées sur les serveurs d'un tiers comme une plateforme d'échange.

S7 PORTEFEUILLE QUI UTILISE LA MÉTHODE DE CALCUL MULTIPARTITE SÉCURISÉ (MPC – MULTI-PARTY COMPUTATION)



Source : Observatoire de la sécurité des moyens de paiement.

⇨ Les clés privées, qu'elles soient stockées sur un portefeuille physique ou numérique, constituent des données sensibles de paiement à protéger. Elles doivent donc être sécurisées afin d'éviter la perte irréversible d'accès aux crypto-actifs ou une compromission susceptible de permettre à un tiers malveillant de réaliser des opérations non autorisées. Cette sécurisation consiste notamment en des mises à jour régulières des appareils et moyens de stockage des clés privées vers les versions actualisées, ainsi qu'en la protection contre les connexions non sécurisées, comme les réseaux publics non sécurisés, en utilisant par exemple un réseau privé virtuel (VPN – *Virtual Private Network*).

Par ailleurs, les techniques de fraude pour obtenir les clés privées, qui donnent accès au portefeuille de crypto-actifs et permettent donc de réaliser des paiements, sont semblables à celles utilisées pour les paiements traditionnels : *phishing*, *smishing*, faux sites, etc.

⇨ Des versions plus sécurisées existent cependant, comme les portefeuilles intégrant soit des protocoles multisignatures soit la méthode de calcul multipartite sécurisé (MPC – *multi-party computation*). Plus adapté aux paiements de détail, le portefeuille utilisant la méthode MPC est une solution cryptographique dans laquelle la clé privée n'est pas présente sous sa forme complète en un seul endroit. Elle est fragmentée par des protocoles de calcul multipartite entre le payeur, le fournisseur de services et, potentiellement, un tiers de confiance. Par conséquent, la compromission de la clé privée devient plus difficile.

3.4.2.3 Les risques afférents aux « contrats intelligents » (*smart contracts*)

Un autre point de vulnérabilité potentiel réside dans le fait que les paiements par crypto-actif s'effectuent le plus souvent via des automates exécuteurs de clauses prédéfinies au niveau des chaînes de blocs, dits « contrats intelligents ». Concrètement, il s'agit de codes informatiques dans un langage de programmation spécifique à la chaîne de blocs utilisée. L'objectif est de définir, en amont, les conditions d'exécution des opérations, qu'il s'agisse d'émission d'unités de crypto-actifs ou de transactions, et d'encadrer les rôles et fonctions des parties prenantes. Par exemple, ces contrats intelligents permettent de conditionner l'exécution d'un paiement à la réalisation d'une condition externe, comme l'approvisionnement du compte ou l'autorisation d'un transfert, et de planifier des transactions récurrentes à exécuter. Or, le « contrat intelligent » peut être modifié lors d'une attaque externe qui utilise les méthodes classiques des attaques informatiques, par exemple, ou d'une fraude interne. Celle-ci est réalisable par une personne ayant une capacité d'action au sein d'une entité exploitant le contrat intelligent. Une fois ce contrat modifié, le fraudeur peut alors commettre une grande variété de fraudes : obtenir un accès à des portefeuilles d'actifs, réaliser des paiements frauduleux, etc.

L'OWASP – *Open Web Application Security Project* –, organisation internationale à but non lucratif dédiée à la sécurité des applications web, a ainsi procédé à une identification des dix plus importantes vulnérabilités des « contrats intelligents », dont elle tire plusieurs recommandations en matière de sécurité [28].

Illustration des principales vulnérabilités des « contrats intelligents »

1. L'attaque de « réentrance » : elle peut donner lieu à un détournement de fonds par un fraudeur, qui réussit à exécuter plusieurs fois une fonction du programme avant la mise à jour du « contrat intelligent », pour que l'opération apparaisse comme effectuée (cas du piratage « PenPie Hack » en 2024).
2. Défaillance du contrôle d'accès : le fraudeur réussit à entrer dans des fonctions du programme qui ne devraient être accessibles qu'à l'administrateur, comme les remboursements, afin de détourner des fonds (attaque de Bybit en février 2025).
3. Faille de la vérification de dépassement lors du calcul de liquidité : faille dans le contrat intelligent qui permet au pirate informatique de tromper le programme en lui faisant croire qu'il ajoute plus de liquidités qu'en réalité. À cause de cette manipulation, le contrat calcule des prix faussés, ce qui autorise l'attaquant à retirer plus d'actifs qu'il n'en a réellement apporté (attaque contre Cetus en mai 2025).

La sécurité des « contrats intelligents » est donc un enjeu essentiel. Les acteurs ont ainsi mis en place de bonnes pratiques, comme l'audit de ces « contrats intelligents » par un tiers indépendant. Certains auditeurs indépendants sont qualifiés « prestataires d'audit de la sécurité des systèmes d'information » (Passi) par l'Agence nationale de la sécurité des systèmes d'information (Anssi) [29], ce qui garantit leur expertise en matière de cybersécurité.

⇨ Par ailleurs, l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) ont publié le *Rapport d'un groupe de travail sur la certification des « contrats intelligents »*. Des pistes de réflexion y sont mises en lumière pour orienter i) la définition de standards de certification des « contrats *intelligents* », avec les grands principes de sécurité que ces derniers pourraient comprendre, ii) l'utilisation des méthodes d'audit existantes dans le cadre de cette certification, les organismes et moyens susceptibles de les mettre en œuvre, et iii) des pistes réglementaires qui pourraient intégrer un éventuel schéma de certification.

3.4.2.4 La surveillance en temps réel des couches 1 et 2

Outre les risques attachés à la chaîne de blocs primaire (couche 1), les traitements réalisés au sein de la couche 2 doivent également être surveillés, en tant que circuits externes à la chaîne de blocs primaire dont le résultat est ensuite déversé dans celle-ci. Le pont entre la couche 1 et la couche 2 peut également présenter un point de vulnérabilité.

⇨ Il est donc nécessaire d'exercer une surveillance en temps réel des paiements par crypto-actif, au même titre que les paiements traditionnels. L'objectif est de lutter efficacement contre la fraude en assurant une sécurité opérationnelle pour contrer les attaques et détecter les opérations frauduleuses.

3.5 Les enjeux de conformité

3.5.1 Les enjeux liés à la sécurité du parcours de paiement

Les solutions de paiement par crypto-actif doivent répondre à des obligations réglementaires en matière de sécurité du parcours de paiement, sur lesquelles s'appuie cette étude, tout autre aspect réglementaire en étant exclu. L'application des règles issues de la deuxième directive européenne sur les services de paiement (DSP2) est ainsi obligatoire pour les crypto-actifs, qualifiés de « jetons de monnaie électronique » (EMT) et donc assimilés à des fonds. En revanche, leur application n'est pas strictement obligatoire pour les solutions de paiement reposant sur des crypto-actifs qui ne sont pas qualifiés de fonds. Il s'agit notamment des crypto-actifs de première génération ou des « jetons se référant à un ou plusieurs actifs » (ART – *asset-referenced tokens*). En conséquence, certains acteurs non régulés proposent des solutions de paiement par des crypto-actifs autres que les EMT régulés, qui présentent donc un risque non négligeable pour les utilisateurs.

⇨ En s'appuyant sur le principe « *même activité, mêmes risques* », il est recommandé que ces règles soient observées par tous les acteurs, régulés ou non, pour leurs solutions de paiement reposant sur des crypto-actifs, quelle que soit la qualification juridique du crypto-actif. Cela concerne notamment les exigences en matière d'authentification forte des transactions.

28 Sur le site OWASP Smart Contract Security.

29 Référentiels d'exigences pour la qualification – Référentiel Passi.

Les règles de sécurité issues de la DSP2 s'appliquent aux crypto-actifs qualifiés de jetons de monnaie électronique, en particulier celles sur l'authentification forte [30] pour les paiements en ligne, le code confidentiel pour les opérations par carte supérieures à 50 euros ou encore la biométrie pour les transactions mobiles. Au-delà du paiement, les PSCA doivent également s'assurer de l'authentification forte de l'utilisateur final. Celle-ci permet de sécuriser l'accès au portefeuille de crypto-actifs ou la réalisation d'opérations sensibles (modification de mot de passe ou d'IBAN, enregistrement d'un nouvel appareil de confiance, etc.).

⇨ À cet égard, la révision en cours menée sur le paquet législatif DSP3/PSR et ses éventuelles implications réglementaires pour les acteurs concernés sur la chaîne des paiements par crypto-actif devront être suivies attentivement. En effet, il convient de garantir la bonne conformité de l'ensemble des acteurs du secteur aux exigences de sécurité mises en place par les cadres coordonnés DSP et MiCA, à travers l'articulation des statuts de PSP et PSCA notamment.

À ce titre, sur demande de la Commission européenne, l'ABE a publié, en juin 2025, un avis soulignant, en particulier, la nécessité du respect de certaines dispositions de la DSP2. Parmi elles se trouvent l'authentification forte du payeur pour l'accès aux portefeuilles de crypto-actifs ou encore le signalement des fraudes aux paiements. L'objectif est d'assurer, par ce moyen, un niveau de protection des consommateurs élevé, quels que soient les moyens de paiement utilisés (jetons de monnaie électronique ou fonds « traditionnels »). L'ABE rappelle également que les consommateurs et les autres acteurs du marché doivent être protégés de manière adéquate et avoir un degré élevé de confiance dans la stabilité du marché et la fiabilité des opérations de paiement, afin de permettre des paiements de détail efficaces et sûrs.

3.5.2 Les enjeux liés à la sécurité du système de paiement

Le règlement européen DORA (*Digital Operational Resilience Act*) relatif à la cyber-résilience du secteur financier impose aux PSCA les mêmes obligations qu'aux PSP en matière de cybersécurité, ainsi que la mise en place de tests et procédures pour encadrer et protéger les systèmes d'information. Néanmoins, à ce stade, l'infrastructure de chaîne de blocs n'étant pas réglementée, l'utilisation d'une nouvelle chaîne de blocs par l'émetteur de crypto-actifs n'est pas encadrée et peut donc susciter des problématiques de sécurité. Toute nouvelle utilisation doit ainsi être portée à la connaissance des autorités et des détenteurs de crypto-actifs dans le cadre du livre blanc (*whitepaper*) rédigé par l'émetteur et requis par le règlement MiCA.

⇨ En ce sens, l'analyse des risques, intégrant notamment un audit, en amont, et un audit régulier des chaînes de blocs, en aval, compte tenu des éventuelles nouvelles fonctionnalités ajoutées, sont de bonnes pratiques supplémentaires à encourager pour sécuriser dans le temps une infrastructure de chaîne de blocs.

Ces enjeux de résilience concernent également les infrastructures existantes. Les PSCA doivent donc se conformer aux exigences des règlements MiCA et DORA et, notamment, mettre en place des politiques de gestion opérationnelle des risques informatiques.

3.5.3 Les enjeux liés à la sécurité des acteurs et des actifs du paiement

Au-delà des aspects de sécurité, l'acceptation des paiements par crypto-actif implique pour les professionnels – commerçants ou prestataires techniques intégrant la solution de paiement – de recourir à un prestataire tiers dûment agréé.

⇨ L'acteur en charge de l'exécution de la transaction et de la conversion des crypto-actifs en monnaie ayant cours légal doit nécessairement être agréé en tant que PSCA (auprès de l'AMF s'il est établi en France) [31]. L'acteur qui procède au versement en euros sur les comptes du commerçant doit être agréé comme PSP ou autorisé en tant qu'agent de PSP (auprès de l'ACPR s'il est établi en France).

De la même manière, les crypto-actifs proposés par les acteurs doivent être conformes aux exigences réglementaires. À cet égard, les commerçants et leurs prestataires doivent sélectionner les actifs avant de les accepter pour paiement et strictement refuser ceux non conformes à la réglementation.

⇨ À ce titre, plusieurs autorités de marché, dont l'AMF [32], appellent à un cadre européen renforcé des marchés de crypto-actifs (ajustement potentiel du règlement MiCA). Elles sollicitent la prise en compte d'enjeux, en particulier, de renforcement des règles pour les plateformes opérant hors de l'Union européenne, un meilleur encadrement des plateformes face au

risque cyber, et une supervision directe par l'Autorité européenne des marchés financiers (AEMF) pour les PSCA significatifs. L'objectif est d'assurer une application uniforme des règles pour les acteurs européens.

30 Les règles européennes sur l'authentification forte sont notamment précisées dans un acte délégué de la DSP2 : le règlement (UE) n° 2018/389 détaillant les transactions assujetties.

31 L'émission de jetons de monnaie électronique est réservée aux établissements de crédit (EC) et aux établissements de monnaie électronique (EME). La fourniture de services sur crypto-actifs, dont la liste est définie à l'article 3 du règlement MiCA, est réservée aux prestataires de services sur crypto-actifs (PSCA).

32 AMF, 15 septembre 2025 : « Les autorités de marché française, autrichienne et italienne appellent à un cadre européen renforcé des marchés de crypto-actifs ».

RECOMMANDATIONS

L'Observatoire rappelle, en premier lieu, que les crypto-actifs présentent de nombreux risques (volatilité, liquidité, défaillance, blanchiment des capitaux et financement du terrorisme, frais transactionnels élevés, etc.), qui ne relèvent pas des strictes problématiques de sécurité adressées au travers des recommandations ci-après. Ils nécessitent une vigilance renforcée de la part de leurs utilisateurs et des autorités compétentes.

À la suite de cette étude de veille, l'OSMP émet les recommandations suivantes concernant la sécurité des solutions de paiement par crypto-actif dans le cadre de l'achat de biens et services au quotidien :

RECOMMANDATIONS À L'ATTENTION DES CONSOMMATEURS ET COMMERÇANTS

Recommandation n° 1
Faire preuve de vigilance pour repérer les tentatives d'escroquerie

L'Observatoire recommande aux utilisateurs intéressés par des solutions de paiement par crypto-actif de vérifier les autorisations réglementaires des fournisseurs et des crypto-actifs utilisés. Les crypto-actifs non autorisés dans l'Union européenne doivent être refusés.

L'Observatoire rappelle également ses recommandations générales de sécurité : ne pas réagir face aux contacts non sollicités, ne pas cliquer sur des liens sponsorisés, mais se rendre par ses propres moyens sur le site internet, ne jamais valider d'opérations dont on n'est pas à l'origine, etc.

Les autorisations réglementaires peuvent être vérifiées sur le site de l'Autorité européenne des marchés financiers (AEMF) pour les prestataires de services sur crypto-actifs (PSCA), et sur le site de l'Autorité bancaire européenne (ABE) pour les prestataires de services de paiement (PSP). Les listes noires [33] de l'ACPR et de l'AMF permettent également d'identifier des fournisseurs étant en exercice illégal d'activité.

Recommandation n° 2
Veiller à sécuriser ses données sensibles de paiement

L'Observatoire recommande aux utilisateurs finaux de solutions de paiement par crypto-actif de protéger leurs clés privées stockées, selon le type de portefeuille (physique ou numérique) [34] :

- en conservant l'appareil dans un endroit sécurisé, en n'enregistrant pas la phrase de récupération en ligne, et en s'assurant d'avoir un mot de passe robuste ;
- en s'authentifiant fortement à la plateforme d'échange ou au fournisseur de portefeuilles autohébergés ;
- en cas de demande par téléphone ou par courriel par un tiers, en ne communiquant jamais ses informations sensibles de paiement ;
- en mettant à jour régulièrement les appareils et moyens de stockage des clés privées vers les versions actualisées plus sécurisées de ces appareils et moyens de stockage ;
- en se protégeant contre les connexions non sécurisées, comme les réseaux publics non sécurisés, et en utilisant une connexion internet sécurisée et un réseau privé virtuel (VPN) visant à protéger les données sur internet et permettant de naviguer anonymement.

Recommandation n° 3
Privilégier les paiements par des actifs régulés tels que les jetons de monnaie électronique

L'Observatoire recommande aux utilisateurs et commerçants intéressés par ces solutions de privilégier des crypto-actifs émis par des acteurs régis par le règlement MiCA, tels que les jetons de monnaie électronique, pour les paiements du quotidien, afin de bénéficier de la sécurité attachée au régime réglementaire encadrant ces actifs.

Recommandation n° 4
Pour les commerçants, privilégier l'utilisation de QR codes dynamiques

Les QR codes statiques mis à disposition de la clientèle présentent un risque de fraude (fraude au *quishing*). Par conséquent, les QR codes statiques pour les systèmes de caisse ne disposant pas d'affichage numérique semblent moins sécurisés.

RECOMMANDATIONS À L'ATTENTION DES ACTEURS DU MARCHÉ DES PAIEMENTS PAR CRYPTO-ACTIF

L'Observatoire renvoie, en premier lieu, aux **propositions [35] publiées en 2025 par le « Groupe de travail sur la certification**

des *smart contracts* », sous l'égide du Forum Fintech ACPR-AMF, en matière d'audits, de gouvernance et de réglementation des contrats intelligents (*smart contracts*).

L'Observatoire renvoie également les prestataires de solutions de paiement par crypto-actif à ses recommandations de 2023 pour anticiper les risques quantiques (inventorier les dispositifs de sécurité, tester des algorithmes post-quantiques, et établir une feuille de route pour anticiper les risques liés à l'informatique quantique)[36].

Recommandation n° 5

Garantir un niveau de protection équivalent, par les acteurs régulés ou non, en mettant en œuvre les règles d'authentification forte au sens de la DSP2 pour toutes les solutions de paiement par crypto-actif, y compris les crypto-actifs autres que les EMT

Les paiements par crypto-actif nécessitent l'intervention de multiples acteurs. En suivant strictement les principes de sécurité issus de la deuxième directive européenne sur les services de paiement (DSP2), l'Observatoire rappelle qu'il est essentiel d'authentifier fortement le processus de paiement (accès au compte ou au portefeuille, initiation d'un paiement à distance, opérations sensibles comme le changement de mot de passe, d'IBAN ou d'appareil de confiance).

A fortiori, il est important d'appliquer ces règles à l'ensemble des acteurs proposant des solutions de paiement par crypto-actif, qu'ils soient régulés ou non, compte tenu des actifs proposés (EMT et autres crypto-actifs) pour les opérations de paiement par carte adossée à des crypto-actifs ou par portefeuille de crypto-actifs, ainsi que la protection des données sensibles de paiement.

Recommandation n° 6

Assurer un niveau de surveillance en temps réel des paiements par crypto-actif équivalent à celui mis en œuvre dans le cadre des paiements traditionnels

L'Observatoire invite les acteurs de la chaîne des paiements par crypto-actif à assurer un degré de surveillance de ces paiements équivalent à celui appliqué aux paiements traditionnels (par l'évaluation du niveau de risque individuel de chaque transaction notamment), afin de lutter efficacement contre la fraude.

Recommandation n° 7

Privilégier l'utilisation de portefeuilles intégrant la méthode MPC de gestion des clés privées

Le portefeuille utilisant la technologie de calcul MPC est un mécanisme qui permet de renforcer significativement la sécurité opérationnelle des paiements par crypto-actif. L'utilisation d'une telle méthode intégrée à un portefeuille permet donc d'éviter la vulnérabilité liée à l'utilisation de portefeuilles classiques.

Recommandation n° 8

Avant de faire appel à une nouvelle chaîne de blocs, il est nécessaire de procéder à une analyse de risques. Cette surveillance doit également s'opérer dans la durée, notamment lorsque la chaîne de blocs évolue.

Afin de s'assurer de la sécurité de l'infrastructure, l'Observatoire recommande aux émetteurs de crypto-actifs souhaitant faire appel à une nouvelle chaîne de blocs dans le cadre de leurs activités, d'effectuer, en amont, une analyse des risques, et de s'assurer que la chaîne présente un haut degré de sécurité. Il est également important d'auditer régulièrement la chaîne de blocs, car celle-ci est vouée à évoluer dans le temps au gré des mises à jour fonctionnelles. Ces analyses doivent naturellement étendre leur périmètre aux processus externes à la chaîne de blocs, qui visent à en améliorer le fonctionnement.

33 Assurance Banque Épargne Infoservice : « Listes noires des autorités ».

34 Plateforme MesServicesCyber, Anssi, « Recommandations relatives à l'authentification multifacteur et aux mots de passe ».

35 Ces propositions visent en premier lieu les activités décentralisées, mais peuvent aussi s'appliquer plus largement aux activités centralisées.

36 Rapport annuel de l'OSMP 2023, chapitre 3 (pages 73-90) : « L'informatique quantique et la sécurité des systèmes de paiement par carte bancaire ».

ANNEXES

A1	Conseils de prudence pour l'utilisation des moyens de paiement	73
A2	Missions et organisation de l'Observatoire	86
A3	Liste nominative des membres de l'Observatoire	88
A4	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux	91
A5	Dossier statistique sur l'usage et la fraude aux moyens de paiement	101

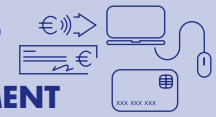
A1 CONSEILS DE PRUDENCE POUR L'UTILISATION DES MOYENS DE PAIEMENT

Face à l'ingéniosité des fraudeurs, les utilisateurs des moyens de paiement scripturaux (carte, chèque, virement et prélèvement) doivent faire preuve de vigilance. À l'initiative de l'Observatoire, six fiches ont été élaborées pour exposer les principaux types de fraude rencontrés et proposer quelques conseils pour s'en prémunir. Cette annexe liste également les réflexes pour savoir réagir en cas de fraude.

PREMIÈRE PARTIE – PRÉVENIR LA FRAUDE

FICHE 1

CONSEILS APPLICABLES À L'ENSEMBLE DES MOYENS DE PAIEMENT

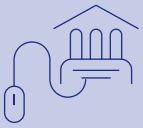


▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

- Conservez vos moyens de paiement auprès de vous ou en lieu sûr.
- Ne communiquez à personne, pas même à votre banque (elle n'en fera jamais la demande) vos identifiants, mots de passe et codes confidentiels associés à vos moyens de paiement.
- Ne cliquez jamais sur un lien envoyé par courriel ou SMS provenant d'un expéditeur inconnu. En cas de doute, prenez contact avec votre conseiller bancaire par votre canal de communication habituel.
- Vérifiez régulièrement et attentivement le relevé de vos opérations sur votre compte en banque afin de signaler rapidement à votre banque toute opération dont vous ne seriez pas à l'origine ou qui vous apparaîtrait douteuse.
- Consultez et suivez les consignes de sécurité publiées par votre banque.
- Assurez-vous que votre banque dispose de vos coordonnées pour vous contacter rapidement en cas d'opérations douteuses.

FICHE 2

CONNEXION À L'ESPACE DE BANQUE EN LIGNE



▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

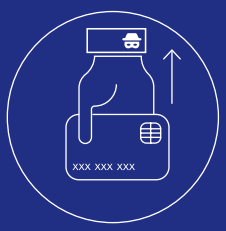
- Pour accéder à votre banque en ligne, choisissez un navigateur internet connu, un moteur de recherche de confiance et pour les accès sur *smartphone* téléchargez l'application bancaire sur les magasins officiels d'applications.
- N'accédez pas à votre banque en ligne depuis un ordinateur public ou lorsque vous êtes connecté à un réseau wifi public.
- N'accédez jamais à votre banque en ligne depuis un lien fourni par courriel ou SMS. Saisissez toujours l'adresse internet exacte fournie par votre banque, éventuellement enregistrée dans vos favoris.
- Sur internet, vérifiez la présence du « S » dans HTTPS (s signifiant *secure*) situé devant l'adresse du site et la présence de l'icône d'une clé ou d'un cadenas dans la barre d'état du navigateur.
- Choisissez un code d'accès suffisamment complexe, qui ne doit être utilisé que pour l'accès à votre banque en ligne, et ne l'enregistrez nulle part ailleurs sur votre ordinateur ou votre téléphone.

FICHE 3

CONSEILS APPLICABLES AUX PAIEMENTS PAR CARTE

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Campagnes de *phishing* et *smishing*

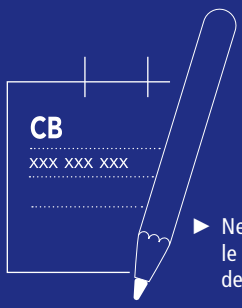


Vol de carte

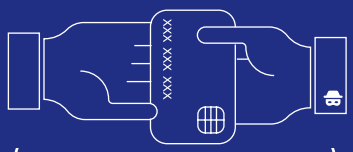
Manipulation psychosociale

Usurpation d'identité du client auprès de l'opérateur mobile

CONSEILS À DESTINATION DES UTILISATEURS



- Ne stockez pas le numéro de votre carte



- Ne confiez jamais votre carte à un tiers

- Vérifiez la présence du « https:// » devant l'adresse d'un site internet

- Ne jamais fournir vos données de carte après avoir cliqué sur un lien reçu par un SMS ou un courriel

PRINCIPAUX CAS DE FRAUDE À LA CARTE RENCONTRÉS

- **CAMPAGNES D'HAMEÇONNAGE** par courriel, SMS, messagerie en ligne ou sur les réseaux sociaux : il s'agit de techniques à partir de messages non sollicités invitant à cliquer sur un lien renvoyant vers un faux site (celui d'une banque en ligne, d'une administration ou d'un marchand en ligne) où il est demandé à l'internaute de communiquer ses données de carte. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide (paiement d'une facture sous peine de la suspension d'un service, régularisation d'une interdiction bancaire ou encore mise à jour sécuritaire).

- **VOL DE LA CARTE** (cambriolage, vol à la tire ou à l'arrachée, détournement de courrier postaux, etc.) ou des données de la carte (par exemple : attaque informatique de bases de données mal sécurisées, suivie d'actions de revente de ces données sur l'internet clandestin).

- **MANIPULATION PSYCHOSOCIALE** pour convaincre l'utilisateur de donner ses codes confidentiels, de réaliser l'authentification forte, voire de remettre volontairement sa carte. Par exemple, dans la fraude au faux conseiller bancaire, l'escroc contacte par téléphone sa victime en se faisant passer pour sa banque sous le prétexte de vouloir l'aider à arrêter une opération frauduleuse en cours. Parfois, l'escroc lui propose même l'intervention d'un coursier à son domicile pour récupérer sa carte dans le but d'accélérer le processus de remplacement de la carte soit disant piratée.

- **USURPATION D'IDENTITÉ** auprès de l'opérateur téléphonique de la victime pour effectuer à son insu un renouvellement de carte SIM : une fois la nouvelle carte SIM activée (physique ou virtuelle) par le fraudeur, celui-ci est en mesure de recevoir tous les appels et SMS à destination du numéro de mobile du client, y compris ceux de la banque, ce qui lui permet de s'authentifier à l'insu du client.

Respectez les délais et veillez à transmettre une information exhaustive à votre banque, au médiateur ou votre avocat, de la même manière que vous le feriez pour les forces de l'ordre.

▷ CONSEILS À DESTINATION DES UTILISATEURS DE CARTE DE PAIEMENT

- Soyez attentif à chaque fois que vous utilisez votre carte de paiement (vérification du montant à payer, authenticité du terminal, etc.) et ne confiez jamais votre carte à un tiers.
- Ne stockez pas le numéro de votre carte, et *a fortiori* votre code confidentiel, sur quelque support que ce soit (votre ordinateur, votre navigateur, un papier dans votre portefeuille ou sac à main, etc.).
- Ne fournissez jamais vos données de carte après avoir cliqué sur un lien reçu par SMS ou par courriel.
- Sécurisez si possible l'accès à l'espace client de votre opérateur téléphonique par une authentification forte ou au minimum par un mot de passe complexe et spécifique.
- Soyez extrêmement sélectif et vigilant avant d'enregistrer votre numéro de carte dans l'espace client d'un commerçant en ligne. Au moindre doute sur la fiabilité ou la sécurité informatique du commerçant, refusez d'enregistrer votre numéro de carte.
- Votre solution d'authentification forte doit être autant protégée que le code confidentiel de votre carte bancaire. Ne communiquez jamais vos informations personnelles permettant de vous authentifier fortement et ne validez jamais les opérations de paiement dont vous n'êtes pas l'initiateur.

▼ En pratique

1 • **Contactez le service réclamation** de votre banque à l'adresse qui figure sur votre relevé de compte ou sur le site internet de votre banque.

2 • Si vous n'êtes pas satisfait par la réponse de votre banque, **soumettez, sans délai, votre litige au médiateur** désigné par votre banque à partir de 15 jours (jusqu'à 35 jours maximum en cas de situation exceptionnelle notifiée par une réponse d'attente de votre banque) après votre première demande [1] et dans un délai d'un an [2].

3 • À tout moment, **vous pouvez engager une action en justice**, après le rejet de votre contestation initiale.

1 Article L. 133-45 du Code monétaire et financier et Recommandations 2024-R-02 du 2 juillet 2024 de l'Autorité de contrôle prudentiel et de résolution (ACPR) sur le traitement des réclamations.

2 Article L. 612-2 du Code de la consommation.

FICHE 4

CONSEILS APPLICABLES AUX VIREMENTS

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Ingénierie sociale

Logiciels malveillants

Campagnes
de *phishing* et *smishing*

CONSEILS À DESTINATION DES UTILISATEURS

- Vérifiez les coordonnées bancaires avec les services de vérification du bénéficiaire et soyez attentifs en l'absence de concordance exacte

- Mettez à jour vos systèmes d'exploitation et antivirus

- N'authentifiez que les opérations dont vous êtes à l'origine

PRINCIPAUX CAS DE FRAUDE AU VIREMENT RENCONTRÉS

▼ LES MANIPULATIONS PAR INGÉNIERIE SOCIALE

- **LA FRAUDE AU PRÉSIDENT :** le fraudeur usurpe l'identité d'un haut responsable de l'entreprise pour obtenir d'un collaborateur la réalisation, de manière confidentielle, d'un virement urgent à destination d'un nouveau compte.

- **LA FRAUDE AUX COORDONNÉES BANCAIRES :** le fraudeur usurpe l'identité d'un fournisseur, bailleur ou autre créancier, et prétexte auprès du client, locataire ou débiteur, un changement de coordonnées bancaires aux fins de détourner le paiement des factures ou loyers. Le fraudeur envoie les nouvelles coordonnées bancaires par courrier électronique ou postale, revêtant le format d'un courrier en bonne et due forme du créancier.

- **LA FRAUDE AU FAUX TECHNICIEN OU CONSEILLER BANCAIRE :** le fraudeur usurpe l'identité d'un banquier et prétexte des tests de sécurité ou bien la détection d'une opération atypique sur le compte du destinataire dans le but de récupérer des informations permettant au fraudeur d'opérer des virements frauduleux ou encore de procéder à l'installation de logiciels malveillants.

▼ LES ATTAQUES INFORMATIQUES

- **LOGICIELS MALVEILLANTS (OU *MALWARES*) :** logiciels malveillants (tels que les troyens, les spammeurs, les virus, etc.) qui s'installent sur l'ordinateur d'une entreprise ou d'un particulier à son insu lors de l'ouverture d'un courriel frauduleux, de la navigation sur des sites infectés ou encore lors de la connexion de périphériques infectés (clé USB par exemple) pour récupérer les données bancaires transitant par l'ordinateur ou le téléphone du client.

- **HAMEÇONNAGE (OU *PHISHING*) :** technique permettant de collecter les données bancaires à partir de courriels non sollicités invitant leurs destinataires à cliquer sur un lien renvoyant vers un faux site de banque en ligne. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide, comme par exemple la régularisation d'une interdiction bancaire ou encore une mise à jour sécuritaire.

▷ CONSEILS À DESTINATION DE TOUS LES ÉMETTEURS DE VIREMENT

- Suivez les consignes de sécurité pour accéder à votre banque en ligne *(cf. fiche n° 2).*
- N'ajoutez comme bénéficiaire sur votre espace de banque en ligne que les personnes de confiance dont vous avez vérifié les coordonnées bancaires, le cas échéant par le biais d'un contre-appel.
- Saisissez des noms complets et exacts pour tous les bénéficiaires. À l'aide des services de vérification du bénéficiaire, soyez attentifs aux alertes de non-concordance avant de valider un virement. En cas de doute, vérifiez les coordonnées bancaires saisies par le biais d'un contre-appel auprès du bénéficiaire.
- Mettez à jour régulièrement vos systèmes d'exploitation et déployez-y des antivirus.
- N'authentifiez que les opérations dont vous êtes à l'origine.

▷ CONSEILS À DESTINATION DES ENTREPRISES

- Vérifiez, en tant que salarié, l'identité et la légitimité de toute personne demandant des informations ou la réalisation d'une opération inhabituelle.
- Soyez particulièrement vigilant en cas de changement de coordonnées bancaires d'un fournisseur, le cas échéant en procédant à un contre-appel.
- Dissociez, dans la mesure du possible, la saisie et la validation des ordres de paiement, en les confiant à des personnes distinctes et en privilégiant les procédures automatisées et électroniques.
- Étudiez les services proposés par votre banque pour limiter les risques comme la fixation de limites (par opération, par bénéficiaire, par jour ou par pays) ou des services de vérification des coordonnées bancaires des clients et fournisseurs.
- Déployez un programme de sécurité informatique de façon à lutter contre les *malwares* ou les attaques informatiques externes.
- Sensibilisez et formez régulièrement vos collaborateurs aux risques de fraude (ingénierie sociale, cyber-risques, etc.), y compris ceux relatifs à l'intelligence artificielle.

FICHE 5

CONSEILS APPLICABLES AUX PRÉLÈVEMENTS

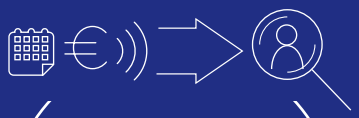
PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Émission illégitime d'ordres de prélèvement

Usurpation d'IBAN

Entente frauduleuse entre le créancier et le débiteur

CONSEILS À DESTINATION DES UTILISATEURS



- Lors de la réception d'un mandat de prélèvement, vérifiez les informations relatives au créancier

- Soyez vigilant sur la communication de votre IBAN

- Surveillez attentivement et régulièrement les opérations par prélèvement débitées sur votre compte

PRINCIPAUX CAS DE FRAUDE AU PRÉLÈVEMENT RENCONTRÉS

- **ÉMISSION ILLÉGITIME D'ORDRES DE PRÉLÈVEMENT (FAUX PRÉLÈVEMENTS)** : le créancier fraudeur s'enregistre en tant qu'émetteur de prélèvements auprès d'un prestataire de services de paiement et émet massivement des prélèvements vers des IBAN (*international bank account numbers*) qu'il a obtenus illégalement et sans aucune autorisation.

- **USURPATION D'IBAN** pour la souscription de services (détournement) : le débiteur fraudeur communique à son créancier les coordonnées bancaires d'un tiers lors de la signature du mandat de prélèvement et bénéficie ainsi du service, sans avoir à en honorer les règlements prévus.

- **ENTENTE FRAUDULEUSE ENTRE CRÉANCIER ET DÉBITEUR :** un créancier fraudeur émet des prélèvements sur un compte détenu par un débiteur complice de façon régulière et en augmentant progressivement les montants. Un peu avant la fin de la période de rétractation légale (de treize mois après le paiement du prélèvement), le débiteur conteste les prélèvements qui ont été débités sur son compte, au motif qu'il n'a pas signé de mandat de prélèvement correspondant. Au moment des rejets des prélèvements, le solde du compte du créancier fraudeur ne permet plus le remboursement des opérations contestées car les fonds ont été préalablement transférés vers un compte complice.

▷ CONSEILS À DESTINATION DE TOUS LES DÉBITEURS

- Lors de la réception d'un mandat de prélèvement, vérifiez que les informations relatives au créancier sont cohérentes avec vos engagements contractuels et conservez précieusement ces informations.

- Pensez à vérifier régulièrement sur votre espace de banque en ligne la liste des créanciers prélevant sur votre compte, et le cas échéant, mettez à jour la liste des créanciers autorisés (appelée aussi « liste blanche ») ou interdits (appelée aussi « liste noire »).

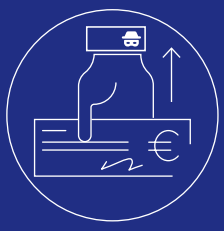
- Faites preuve de vigilance sur la communication de votre IBAN en la réservant à vos créanciers de confiance.

- Surveillez attentivement et régulièrement les opérations par prélèvement débitées sur votre compte et en cas de fraude contestez sans délai l'opération de prélèvement. Le remboursement des prélèvements est sans condition dans un délai de huit semaines, indépendamment de l'existence ou non d'un mandat de prélèvement.

FICHE 6

CONSEILS APPLICABLES AUX CHÈQUES

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS



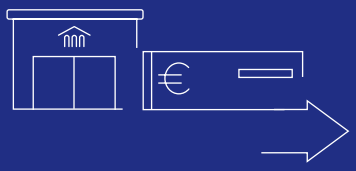
Vol de chèque(s) ou chèquier

Falsification d'un chèque

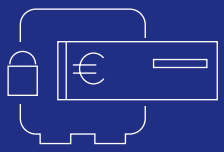
Contrefaçon d'un chèque

Fraude à la « mule »

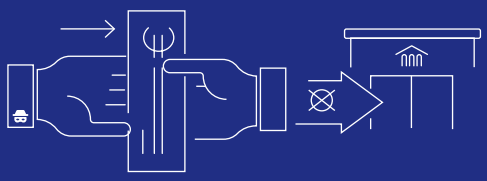
CONSEILS À DESTINATION DES UTILISATEURS



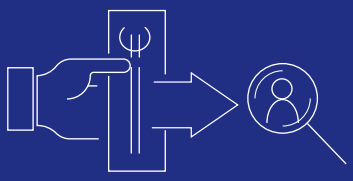
▶ Privilégiez la remise de chéquiers en agence



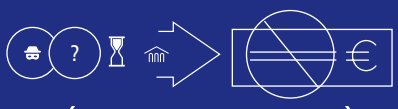
▶ Conservez votre chéquier en sécurité



▶ N'acceptez jamais d'encaisser des chèques pour le compte d'autrui



▶ Restez vigilant lorsque vous acceptez un chèque



▶ Soyez réactif dans la mise en opposition des chéquiers perdus ou volés

PRINCIPAUX CAS DE FRAUDE AU CHÈQUE RENCONTRÉS

▼ ORIGINE DES CHÈQUES FRAUDULEUX

- Vol de chéquiers dans les circuits de distribution (transporteurs, circuits postaux, etc.) ou chez le client (cambriolage, vol à la tire ou à l'arraché, etc.).
- Interception frauduleuse d'un chèque régulièrement émis puis falsifié par grattage, gommage ou effacement (modification du bénéficiaire ou du montant) ou directement encaissé sans modification sur un compte n'appartenant pas au bénéficiaire légitime.
- Contrefaçon de chèque, en créant un faux chèque de toutes pièces, parfois émis sur une fausse banque, mais le plus souvent sur une banque existante.

▼ UTILISATION DES CHÈQUES FRAUDULEUX

- Remise de chèques frauduleux à des bénéficiaires légitimes contre la remise de biens et de services (commerçants, sociétés de location, etc.)
- Processus de « cavalerie » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement d'un décaissement des fonds par virement, retrait ou paiement par carte. Ces remises de chèques peuvent se faire soit directement par le biais de comptes frauduleusement ouverts sous une fausse identité ou une identité usurpée (par exemple, les comptes de professionnels et d'entrepreneurs bénéficiant de mécanismes de crédit en compte immédiat des chèques remis à l'encaissement), soit indirectement par le biais d'une tierce personne, souvent un particulier, qui accepte, contre promesse de rémunération ou dans un contexte de chantage affectif, d'encaisser les chèques frauduleux (fraude à la « mule »).

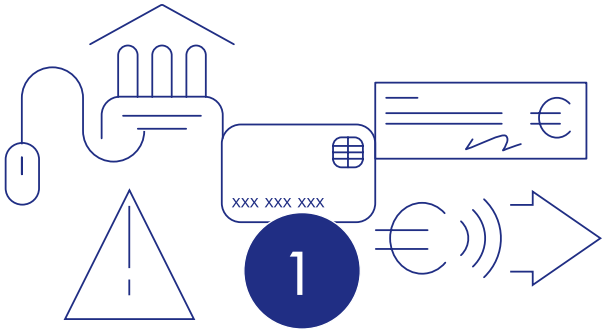
▷ CONSEILS À DESTINATION DE TOUS LES UTILISATEURS DE CHÈQUES

- Privilégiez dans la mesure du possible la remise de chéquiers en agence et en cas d'envoi par voie postale, soyez très attentifs à sa réception et faites opposition aussitôt que le délai est anormalement long.
- Conservez votre chéquier en sécurité et remplissez votre chèque avec soin, à l'encre noire, en remplissant l'ensemble des mentions obligatoires et en traçant des traits horizontaux pour ne laisser aucun espace.
- N'acceptez jamais et sous aucun prétexte d'encaisser des chèques pour le compte d'autrui, notamment quand cela se fait dans des situations d'urgence ou contre des promesses d'argent.
- Restez vigilant quand il s'agit d'accepter et d'encaisser un chèque, y compris un chèque de banque. N'acceptez jamais un chèque qui ne correspond pas à ce qui a été convenu, notamment en cas de trop perçu.
- Faites preuve d'une très grande réactivité dans la mise en opposition des chéquiers perdus ou volés, ou des chèques non reçus par leur bénéficiaire.

▷ CONSEILS À DESTINATION DES COMMERÇANTS

- Ne perdez pas de temps avant d'encaisser un chèque, car un chèque qui traîne est un risque inutile de perte ou de vol.
- Demandez une ou deux pièces d'identité au payeur pour vérifier la cohérence du chèque remis avec son identité (article L. 131-15 du Code monétaire et financier).
- Dans tous les cas, faites un examen physique approfondi du chèque. Il s'agit de vérifier la cohérence des données du chèque et la présence des éléments de sécurité (par exemple, microlettres visibles à la loupe sur les lignes du chèque, encres fluorescentes visibles sous une lampe à ultraviolets, qualité des motifs imprimés, etc.).
- Souscrivez à des services de consultation du Fichier national des chèques irréguliers (FNCI) de la Banque de France, comme Vérifiance, service officiel de prévention des chèques impayés, y compris les chèques volés, perdus ou contrefaits.

DEUXIÈME PARTIE – RÉAGIR EN CAS DE FRAUDE



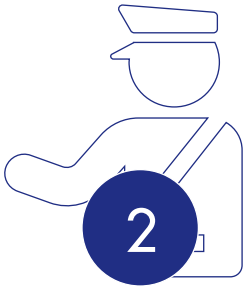
FAIRE OPPOSITION

- **Faites immédiatement opposition** dès que vous constatez la perte, le vol, le détournement ou toute utilisation non autorisée de votre moyen de paiement ou des données qui y sont liées. Cette opposition permet de bloquer le moyen de paiement, évitant ainsi par la suite toute opération frauduleuse. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée. Dans certains cas, cette réactivité peut permettre à la banque d'arrêter la tentative de fraude ou d'initier auprès de la banque destinataire une procédure d'annulation de l'opération.

▼ En pratique

- **Appelez le numéro indiqué par votre établissement financier.** À défaut, pour la carte **appelez le 0 892 705 705**, *service facturé 0,34 €/mn + prix d'un appel (en France métropolitaine).*

Une opposition tardive peut vous priver du remboursement par la banque de tout ou partie des opérations contestées.



SIGNALER LA FRAUDE AUPRÈS DES FORCES DE L'ORDRE

- **Il est recommandé de systématiquement signaler les cas de fraude aux moyens de paiement aux forces de l'ordre,** en privilégiant la démarche sur la plateforme Perceval [3] pour les fraudes à la carte bancaire sur internet.

- **Un dépôt de plainte de l'utilisateur ne peut pas être exigé par le prestataire de services de paiement comme action préalable indispensable à l'instruction de sa demande de remboursement.**

Toutefois, l'utilisateur peut aussi porter plainte auprès d'un commissariat de police ou d'une unité de gendarmerie en cas de vol de son moyen de paiement et en cas d'utilisation frauduleuse de celui-ci ou des données qui lui sont liées. Afin de gagner du temps lors du rendez-vous, une pré-plainte en ligne est possible.

Ces signalements et dépôts de plainte permettent aux forces de l'ordre de disposer des éléments pour mener leurs enquêtes.

La transmission d'une information exhaustive est nécessaire à l'instruction du dossier, mais aussi à l'identification des auteurs et à la mise en œuvre de poursuites pénales à leur encontre. Elle est également indispensable pour enrichir de façon vertueuse les avis de mise en garde à l'attention des consommateurs et contribuer ainsi à la sensibilisation des utilisateurs de services de paiement. Il est donc important de faire ces démarches pour contribuer à la lutte contre la fraude.

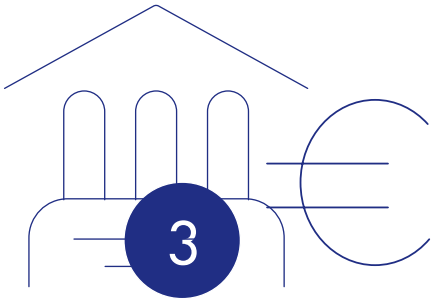
.../...

3 Perceval – Plateforme électronique de recueil de coordonnées bancaires.

▼ En pratique

- Allez sur la **plateforme en ligne Perceval** pour les signalements relatifs à une fraude à la carte de paiement sur internet ;
- Dans les autres cas, rendez-vous dans **un commissariat de police ou dans une unité de gendarmerie** pour signaler les cas de fraude, après avoir déposé une pré-plainte en ligne sur *www.pre-plainte-en-ligne.gouv.fr.*

Lors de vos déclarations auprès des forces de l'ordre, **faites preuve de la plus grande transparence dans la description des faits relatifs à la fraude**.



CONTACTER VOTRE BANQUE POUR POTENTIELLEMENT OBTENIR UN REMBOURSEMENT

Une fois la mise en opposition de votre moyen de paiement réalisée et le signalement aux forces de l'ordre effectué, **contactez votre banque pour contester les opérations de paiement frauduleuses** et obtenir potentiellement un remboursement de la part de votre établissement de paiement. Réunissez l'ensemble des éléments dont vous disposez pour faciliter l'instruction de votre dossier par la banque. Au-delà de votre dossier, cette transparence permet aussi à la banque d'améliorer ses outils de lutte contre la fraude et la pertinence de ses campagnes de sensibilisation.

▼ En pratique

- **Suivez la procédure de contestation indiquée par votre banque sur votre espace de banque en ligne ou contactez votre agence ou conseiller bancaire.**

La transmission d'une information exhaustive est nécessaire à l'instruction du dossier. Les utilisateurs veillent à fournir l'ensemble des éléments dont ils disposent concernant la fraude dont ils ont été victimes, notamment sur :

- **la nature et le contexte de l'opération :**
  - niveau de connaissance du bénéficiaire,
  - procédés techniques ou manipulatoires que le fraudeur est supposé avoir mobilisés,
  - instrument et terminaux utilisés pour l'opération de paiement,
  - messages ou appels reçus,
  - actions réalisées sous le coup d'une manipulation par le fraudeur, etc. ;
- **les actions entreprises une fois la fraude découverte :**
  - blocage de l'instrument,
  - démarche Perceval (transmettre le récépissé),
  - dépôt de plainte auprès des forces de l'ordre notamment lorsque la démarche Perceval n'est pas applicable, etc.

Lorsque vous contestez une ou plusieurs opérations de paiement, votre banque doit procéder dans le délai d'un jour ouvré à une première analyse en examinant les paramètres techniques associés à l'opération, les modalités de l'authentification forte mise en œuvre et les éléments de contexte dont elle dispose.

Votre banque procédera alors sans délai au remboursement [4] de cette ou de ces opération(s) de paiement contestée(s) sauf si :

- elle dispose de bonnes raisons de soupçonner une fraude de votre part ;
- elle dispose de suffisamment de preuves pour considérer que vous avez autorisé les opérations contestées ou que vous avez été gravement négligent.

Votre banque peut poursuivre si nécessaire les investigations dans un délai n'excédant pas 30 jours, sauf situation exceptionnelle. Dans le cas où votre banque a procédé au remboursement des fonds immédiatement, elle doit vous informer de l'éventualité d'une reprise de fonds ultérieure. De la même manière, votre banque doit vous informer de sa décision de ne pas rembourser les opérations contestées en communiquant le motif ainsi qu'en y joignant, le cas échéant, les éléments qui la justifient.

▼ En pratique

Plusieurs scénarios peuvent se produire :

1 • Votre banque vous rembourse immédiatement sans qu'elle n'ait besoin de mener une investigation complémentaire.

2 • Votre banque vous rembourse sous réserve d'une potentielle reprise de fonds ultérieure, au plus tard dans un délai de 30 jours, une fois l'investigation complémentaire terminée.

3 • Votre banque refuse immédiatement ou dans un délai de 30 jours de vous rembourser.

Votre banque doit impérativement :

- **prendre contact avec vous :**
  - dans un délai d'un jour ouvré pour procéder au remboursement définitif des opérations que vous avez contestées,
  - dans un délai d'un jour ouvré pour vous informer d'investigations complémentaires qui pourraient conduire à une reprise de fonds ultérieure dans un délai de 30 jours,
  - à tout moment, mais dans un délai n'excédant pas 30 jours, pour **vous informer** de sa décision de ne pas vous rembourser et **du motif de ce refus en joignant les éléments qui justifient sa décision.**
- en cas de refus de remboursement, **vous communiquer les modalités suivant lesquelles une réclamation peut être déposée.**

En cas de réponse insatisfaisante de la part de votre banque, vous pouvez vous tourner vers le service de réclamation de votre prestataire de paiement. L'adresse figure sur votre relevé de compte ou sur le site internet de votre banque. Lors de votre réclamation écrite, veillez à faire preuve de la plus grande transparence dans la description des faits relatifs à la fraude comme lors de la première contestation. Joignez une copie des pièces justificatives et résumez les démarches entreprises auprès de votre banque (compte rendu du rendez-vous, copie des échanges, etc.).

Le service dédié aux réclamations vous apportera une réponse qualitative et motivée le plus rapidement possible et, en tout état de cause, dans un délai n'excédant pas 15 jours pour les paiements réalisés par carte, virement ou prélèvement (jusqu'à 35 jours maximum en cas de situation exceptionnelle notifiée par une réponse d'attente de votre banque) et deux mois pour les chèques [5].

Vous pouvez, immédiatement et gratuitement, soumettre votre litige au médiateur de la consommation désigné par votre banque, en cas de réponse insatisfaisante ou en l'absence de réponse à partir des délais susmentionnés et ce pendant la période d'un an à compter de la date de votre première demande [6].

La médiation intervient dans un délai de 90 jours maximum à compter de la réception de l'exhaustivité des éléments relatifs à la fraude dont vous disposez. Vous êtes libre d'accepter ou de refuser la solution proposée par le médiateur. L'acceptation de la proposition du médiateur par les deux parties met fin au différend.

Enfin, **vous pouvez engager une action en justice,** à tout moment après le rejet de votre contestation initiale.

▼ En pratique

1 • **Contactez le service réclamation** de votre banque à l'adresse qui figure sur votre relevé de compte ou sur le site internet de votre banque.

2 • Si vous n'êtes pas satisfait par la réponse de votre banque, **soumettez sans délai votre litige au médiateur** désigné par votre banque ou en l'absence de réponse à partir de 15 jours pour les paiements réalisés par carte, virement ou prélèvement (jusqu'à 35 jours maximum en cas de situation exceptionnelle notifiée par une réponse d'attente de votre banque) et deux mois pour les chèques et dans un délai d'un an.

3 • À tout moment, **vous pouvez engager une action en justice**, après le rejet de votre contestation initiale.

Respectez les délais et veillez à transmettre une information exhaustive aux services de réclamation et de médiation, de la même manière que pour les forces de l'ordre.

4 Articles L. 133-18 et L. 133-19 du Code monétaire et financier.

5 Article L. 133-45 du Code monétaire et financier et Recommandations 2024-R-02 du 2 juillet 2024 de l'Autorité de contrôle prudentiel et de résolution (ACPR) sur le traitement des réclamations.

6 Article L. 612-2 du Code de la consommation.

A2 MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

Les missions, la composition et les modalités de fonctionnement de l'Observatoire de la sécurité des moyens de paiement sont précisées par les articles L. 141-4, R. 141-1, R. 141-2 et R. 142-22 à R. 142-27 du Code monétaire et financier.

PÉRIMÈTRE CONCERNÉ

L'Observatoire de la sécurité des moyens de paiement couvre l'ensemble des moyens de paiement scripturaux. Ce périmètre résulte de l'évolution législative apportée par l'article 65 de la loi n° 2016-1691 du 9 décembre 2016, qui a élargi la mission de l'Observatoire de la sécurité des cartes de paiement à tous les instruments de paiement autres que les espèces.

Selon l'article L. 311-3 du Code monétaire et financier, un moyen de paiement s'entend comme tout instrument qui permet à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé. Les moyens de paiement couverts par l'Observatoire sont les suivants :

- **Le virement** est fourni par le prestataire de services de paiement qui détient le compte de paiement du payeur et qui consiste à créditer, sur la base d'une instruction du payeur, le compte de paiement d'un bénéficiaire par une opération ou une série d'opérations de paiement réalisées à partir du compte de paiement du payeur.

- **Le prélèvement** vise à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur.

- **La carte de paiement** est une catégorie d'instrument de paiement offrant à son titulaire les fonctions de retrait ou de transfert de fonds. On distingue différentes typologies de cartes :
  - Les cartes de débit sont des cartes associées à un compte de paiement permettant à son titulaire d'effectuer des paiements ou retraits qui seront débités selon un délai fixé par le contrat de délivrance de la carte ;
  - Les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai. L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;
  - Les cartes commerciales, délivrées à des entreprises, à des organismes publics ou à des personnes physiques exerçant une activité indépendante, ont une utilisation limitée aux frais professionnels, les paiements effectués au moyen de ce type de cartes étant directement facturés au compte de l'entreprise, de l'organisme public ou de la personne physique exerçant une activité indépendante.

- **La monnaie électronique** constitue une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise (par les établissements de crédit ou les établissements de monnaie électronique) contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

- **Le chèque** consiste en un écrit par lequel une personne, appelée tireur, donne l'ordre à un établissement de crédit, appelé tiré, de payer à vue une certaine somme à son ordre ou à une tierce personne, appelée bénéficiaire.

- **Les effets de commerce** sont des titres négociables qui constatent au profit du porteur une créance de somme d'argent et servent à son paiement. Parmi ces titres on distingue la lettre de change et le billet à ordre.

- **La transmission de fonds** est un service de paiement pour lequel les fonds sont reçus de la part d'un payeur, sans création de compte de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant correspondant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, et/ou pour lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci.

ATTRIBUTIONS

Conformément aux articles L. 141-4 et R. 141-1 du Code monétaire et financier, les attributions de l'Observatoire de la sécurité des moyens de paiement sont de trois ordres :

- Il assure le suivi de la mise en œuvre des mesures adoptées par les émetteurs, les commerçants et les entreprises pour renforcer la sécurité des moyens de paiement ;
- Il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de moyens de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents moyens de paiement scripturaux ;
- Il assure une veille technologique en matière de moyens de paiement scripturaux, avec pour objet de proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des moyens de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

Les propositions de l'Observatoire pour analyser et lutter contre les atteintes à la sécurité des moyens de paiement sont émises sous la forme de recommandations. En outre, le ministre chargé de l'Économie et des Finances peut, aux termes de l'article R. 141-2 du Code monétaire et financier, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

COMPOSITION

L'article R. 142-22 du Code monétaire et financier détermine la composition de l'Observatoire. Conformément à ce texte, l'Observatoire comprend :

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel et de résolution ou son représentant ;
- un représentant de la Commission nationale de l'informatique et des libertés ;
- huit représentants des émetteurs de moyens de paiement ;
- sept représentants des opérateurs de systèmes de paiement ;
- cinq représentants des consommateurs ;
- huit représentants des commerçants et des entreprises dans les domaines, notamment, du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;
- deux représentants des opérateurs de communications électroniques ;
- deux représentants d'associations de personnes en situation de handicap ;
- deux personnalités qualifiées en raison de leur compétence.

La liste nominative des membres de l'Observatoire figure en annexe 3.

Les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans. Leur mandat est renouvelable.

Le président est désigné parmi ces membres par le ministre chargé de l'Économie et des Finances. Son mandat est de trois ans, renouvelable. Monsieur Denis Beau, premier sous-gouverneur de la Banque de France, en est l'actuel président.

MODALITÉS DE FONCTIONNEMENT

Conformément à l'article R. 142-23 et suivants du Code monétaire et financier, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté un règlement intérieur qui précise les conditions de son fonctionnement.

Le secrétariat de l'Observatoire, assuré par la Banque de France, est chargé de l'organisation et du suivi des séances, de la centralisation des informations nécessaires à l'établissement des statistiques de la fraude sur les moyens de paiement, de la collecte et de la mise à disposition des membres des informations nécessaires au suivi des mesures de sécurité adoptées et à la veille technologique en matière de moyens de paiement. Le secrétariat prépare également le rapport annuel de l'Observatoire, remis chaque année au ministre chargé de l'Économie et des Finances et transmis au Parlement.

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'Économie et des Finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat.

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat sont tenus au secret professionnel par l'article R. 142-25 du Code monétaire et financier, et doivent donc conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. À cette fin, l'Observatoire a inscrit dans son règlement intérieur l'obligation incombant aux membres de s'engager auprès du président à veiller strictement au caractère confidentiel des documents de travail.

A3 LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

En application de l'article R. 142-22 du Code monétaire et financier, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre de l'Économie. Le dernier arrêté de nomination date du 9 juin 2026.

PRÉSIDENT

Denis BEAU
Premier sous-gouverneur de la Banque de France

REPRÉSENTANTS DU PARLEMENT

Nathalie GOULET
Sénatrice

Mélanie THOMIN
Députée

REPRÉSENTANT DU SECRÉTARIAT GÉNÉRAL DE L'AUTORITÉ DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION

- La secrétaire générale ou son représentant :
  Emmanuelle ASSOUAN

REPRÉSENTANTS DES ADMINISTRATIONS

Sur proposition du secrétariat général de la Défense et de la Sécurité nationale :
- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  Raphaël KENIGSBERG

Sur proposition du ministre de l'Économie, de l'Industrie et du Numérique :
- Le directeur général de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse ou son représentant :
  Olivier COROLLEUR
- Le directeur général du Trésor ou son représentant :
  Anselme MIALON
- Le président de l'Institut d'émission des départements d'outre-mer (IEDOM) et directeur général de l'Institut d'émission d'outre-mer (IEOM) :
  Alexandre GAUTIER
- La cheffe de bureau à la direction générale de la concurrence, de la consommation et de la répression des fraudes :
  Marie-Hélène AUFFRET

Sur proposition du garde des Sceaux, ministre de la Justice :
- Le directeur des Affaires criminelles et des Grâces ou son représentant :
  Étienne PERRIN

Sur proposition du ministre de l'Intérieur :
- La sous-directrice de la lutte contre la criminalité financière à la Direction centrale de la police judiciaire (DCPJ) ou son représentant :
  Magali CAILLAT
- Le directeur général de la Gendarmerie nationale ou son représentant :
  Eddy ROUF

Sur proposition de la Commission nationale de l'informatique et des libertés :
- La cheffe du service des Affaires économiques ou son représentant :
  Nacéra BEKHAT

REPRÉSENTANTS DES ÉMETTEURS DE MOYENS DE PAIEMENT

Fanny RODRIGUEZ
Association française des établissements de paiement et de monnaie électronique (Afepame)

Corinne DENAEYER
Association française des sociétés financières (ASF)

Sébastien MARINOT
BNP Paribas

Mireille MERCIER
Office de coordination bancaire et financière (OCBF)

Jean-Paul ALBERT
Société Générale

Évelyne BOTTOLLIER-CURTET
Groupe BPCE

Jérôme RAGUÉNÈS
Fédération bancaire française (FBF)

Marie-Anne LIVI
Crédit Agricole

REPRÉSENTANTS DES OPÉRATEURS DE SYSTÈMES DE PAIEMENT

Sophie MAHUSSIER
American Express France

Barbara SESSA
Mastercard France

Philippe LAULANIE
Groupement des cartes bancaires

Romain BOISSON
Visa Europe France

Régis FOLBAUM
STET

Vincent SIGLIANO
Worldline

Farid ALIYEV
EPI Company

REPRÉSENTANTS DES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES

Romain BONENFANT
Fédération Française des Télécoms

Pierre TROCME
Association française de Multimédia Mobile (AF2M)

REPRÉSENTANTS DES CONSOMMATEURS

Hugues DE CHAMPS
Confédération nationale des associations familiales catholiques (CNAFC)

Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN
Union nationale des associations familiales (Unaf)

Hervé MONDANGE
Association Force ouvrière consommateurs (Afoc)

Philippe ROSAIRE
Association pour l'information et la défense des consommateurs salariés CGT (INDECOSA-CGT)

REPRÉSENTANTS DES COMMERÇANTS ET DES ENTREPRISES

Bernard COHEN-HADAD
Confédération des petites et moyennes entreprises (CPME)

Émilie TISON
Confédération du commerce de gros et international
Mouvement des entreprises de France (MEDEF)

Florence SEGUREL
Association française des trésoriers d'entreprise (AFTE)

Myriam BOURGEOT
Mercatel

Philippe JOGUET
Fédération du commerce et de la distribution (FCD)

Jean-François BRUNET
Conseil du commerce de France (CdCF)

Hugo JUBLAN
Fédération du e-commerce et de la vente à distance (Fevad)

Edwige BECKER
Chambre de commerce et d'industrie de région Paris – Île-de-France (CCIP)

REPRÉSENTANTS D'ASSOCIATIONS DE PERSONNES EN SITUATION DE HANDICAP

Hamou BOUAKKAZ
Valentin Haüy

Nicolas MERILLE
APF France Handicap

PERSONNALITÉS QUALIFIÉES

Marie-Christine CAFFET
Médiation bancaire

David NACCACHE
École normale supérieure (ENS)

A4 MÉTHODOLOGIE DE MESURE DE LA FRAUDE AUX MOYENS DE PAIEMENT SCRIPTURAUX

CADRE GÉNÉRAL

Définition de la fraude aux moyens de paiement

La définition de la fraude aux moyens de paiement scripturaux, retenue par l'Observatoire, est alignée sur celle de l'Autorité bancaire européenne (ABE) qui est établie dans ses Orientations de 2018 concernant les exigences pour la déclaration de données relatives à la fraude (EBA/GL/2018/05) [1]. La fraude est ainsi définie dans le présent rapport comme **l'utilisation illégitime d'un moyen de paiement ou des données qui lui sont attachées ainsi que tout acte concourant à la préparation ou la réalisation d'une telle utilisation :**

- **ayant pour conséquence un préjudice financier** : pour l'établissement teneur de compte ou émetteur du moyen de paiement, le titulaire du moyen de paiement, le bénéficiaire légitime des fonds (l'accepteur ou créancier), un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ;
- **quel que soit le mode opératoire retenu sur** :
  - les moyens employés pour récupérer, sans motif légitime, les données ou le support du moyen de paiement (vol, détournement du support ou des données, piratage d'un équipement d'acceptation, etc.) ;
  - les modalités d'utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait, en situation de proximité ou à distance, par utilisation physique de l'instrument de paiement ou des données qui lui sont attachées, etc.) ;
  - la zone géographique d'émission ou d'utilisation du moyen de paiement ou des données qui lui sont attachées ;
- **et quelle que soit l'identité du fraudeur** : un tiers, l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

Transactions couvertes

La fraude, ainsi définie, est mesurée par l'Observatoire en comptabilisant l'ensemble des opérations de paiement qui ont donné lieu à une écriture au compte d'au moins une des contreparties de la transaction et qui ont fait l'objet d'un rejet *a posteriori* pour motif de fraude. Ainsi, sont exclues de la fraude les tentatives de fraude, auquel cas la fraude est arrêtée avant exécution de l'opération.

Sont également exclus de la fraude :

- les utilisations irrégulières d'un moyen de paiement du seul fait d'un défaut de provision suffisante ou d'un compte clos se traduisant notamment par un impayé ;
- l'utilisation d'une fausse identité ou d'une identité usurpée pour ouvrir un compte ou obtenir un moyen de paiement en vue de réaliser des paiements ;
- les situations où le titulaire légitime du moyen de paiement autorise un paiement, mais s'oppose au règlement, en détournant les procédures prévues par la loi en formulant une contestation de mauvaise foi, y compris dans le cas de litiges commerciaux (par exemple, cas d'un site en faillite qui ne livre pas les produits commandés ou lorsque l'objet acheté n'est pas conforme à la commande) ;
- les cas d'escroquerie où le payeur effectue un paiement vers un bénéficiaire qui est un escroc ou le complice d'un escroc dans la mesure où le produit ou le service acheté n'existe pas et n'est donc pas livré (par exemple, vente illicite de produits financiers comme des produits d'investissements ou souscription à des crédits).

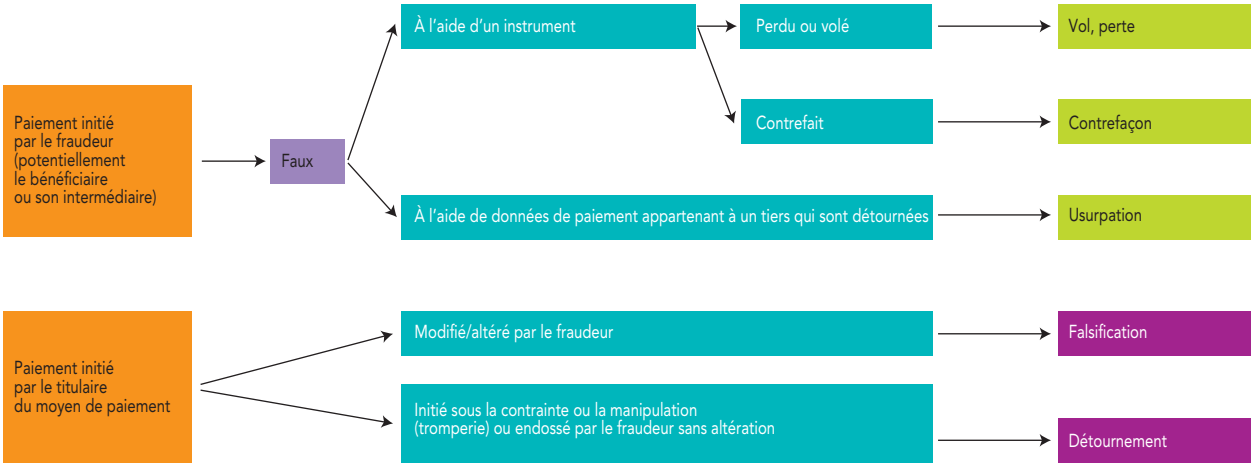
Par ailleurs, l'approche retenue pour évaluer la fraude est celle dite de la « fraude brute » qui consiste à retenir le montant initial des opérations de paiement sans prendre en compte les mesures qui peuvent être prises ultérieurement par les contreparties en vue de réduire le préjudice (par exemple, interruption de la livraison des produits ou de la fourniture de services, accord amiable pour le rééchelonnement du paiement en cas de répudiation abusive du paiement, dommages et intérêts pour donner suite à un recours en justice, etc.).

Origine des données de fraude

Les données de fraude sont collectées par le secrétariat de l'Observatoire auprès de l'ensemble des établissements concernés, selon une approche différenciée par moyen de paiement (cf. ci-après). Compte tenu du caractère confidentiel des données individuelles collectées, seules les statistiques consolidées à l'échelle nationale sont mises à disposition des membres de l'Observatoire et présentées dans son rapport annuel.

1 Ces orientations ont été établies au titre de l'article 96, paragraphe 6, de la deuxième directive européenne concernant les services de paiements dans le marché intérieur (Directive UE 2015/2366 dite « DSP2 »).

Présentation schématique de la typologie de la fraude aux moyens de paiement



Note : Cette présentation schématique est à considérer en complément des guides officiels de la Banque de France relatifs aux collectes statistiques sur la fraude aux moyens de paiement.

Typologie de la fraude aux moyens de paiement

Afin d'analyser la fraude aux moyens de paiement, l'Observatoire a retenu trois principaux types de fraudes, étant précisé que ceux-ci ne s'appliquent pas de la même manière aux différents instruments de paiement :

- **faux** (vol, perte, contrefaçon) : initiation d'un faux ordre de paiement, soit au moyen d'un instrument de paiement physique (carte, chéquier, etc.) qui est volé (lors de son envoi par le prestataire de services de paiement ou après réception par le bénéficiaire légitime), perdu ou contrefait, soit au moyen du détournement de données ou d'identifiants bancaires (usurpation) ;
- **falsification** : altération d'un ordre de paiement régulièrement donné par le titulaire légitime du moyen de paiement, en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.) ;
- **détournement** : transaction initiée par le payeur sous la contrainte ou la manipulation (tromperie), sans altération ou modification d'attribut par le fraudeur.

Ventilation géographique de la fraude aux moyens de paiement

Les fraudes sont ventilées entre les transactions nationales, les transactions européennes et les transactions internationales. Jusqu'en 2020, les transactions européennes prenaient comme référence l'espace SEPA (*Single Euro Payment Area*). Depuis 2021, les transactions européennes prennent comme référence l'Espace économique européen (EEE) de façon à aligner la méthodologie de l'Observatoire sur celle de l'Autorité bancaire européenne (ABE). Le Royaume-Uni fait ainsi partie de l'espace SEPA, mais, depuis le Brexit en 2020, est dorénavant en dehors de l'EEE.

MESURE DE LA FRAUDE À LA CARTE DE PAIEMENT

Transactions couvertes

La fraude à la carte de paiement, telle que mesurée dans le présent rapport, porte sur les transactions de paiement (de proximité et à distance) et de retrait effectuées par carte de paiement et réalisées en France et à l'étranger dès lors que l'une des contreparties de la transaction est considérée comme française : carte émise par un établissement français ou accepteur de la transaction (commerçant ou distributeur automatique de billet/guichet automatique bancaire) situé en France. Aucune distinction n'est faite quant à la nature du réseau d'acceptation (interbancaire [2] ou privatif [3]) ou la catégorie de carte concernée (carte de débit, carte de crédit, carte commerciale ou carte prépayée).

Origine des données de fraude

Les données de fraude à la carte de paiement sont issues des données déclarées par les systèmes de paiement, et non des prestataires de services de paiement. Elles sont spécialement collectées par la Banque de France pour le compte de l'Observatoire auprès :

- du Groupement des cartes bancaires CB, de Mastercard, de Visa Europe, d'American Express, d'UnionPay et de JCB (Japan Credit Bureau) ;
- des principaux émetteurs de cartes privatives actifs en France.

Éléments d'analyse de la fraude

L'analyse de la fraude à la carte de paiement tient compte de plusieurs paramètres : les types de fraudes, les canaux d'initiation de paiement, les zones géographiques d'émission et d'utilisation de la carte ou des données qui lui sont attachées et, pour les paiements à distance, les secteurs d'activité du commerçant et les modalités du paiement sur internet.

2 Le terme « interbancaire » qualifie les systèmes de paiement par carte faisant intervenir plusieurs prestataires de services de paiement émetteurs de cartes et acquéreurs de paiements.

3 Le terme « privatif » qualifie les systèmes de paiement par carte faisant intervenir un seul prestataire de services de paiement, étant à la fois l'émetteur de la carte et l'acquéreur de l'opération.

Typologie de la fraude à la carte de paiement	Forme de la fraude
Carte perdue ou volée	Le fraudeur utilise une carte de paiement à la suite d'une perte ou d'un vol, à l'insu du titulaire légitime.
Carte non parvenue	La carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime. Ce type de fraude se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut difficilement constater qu'un fraudeur est en possession d'une carte lui étant destinée. Dans ce cas de figure, le fraudeur s'attache à exploiter des vulnérabilités dans les procédures d'envoi des cartes.
Carte contrefaite	La contrefaçon d'une carte de paiement consiste soit à modifier les données magnétiques, d'embossage [a)] ou de programmation d'une carte authentique, soit à créer un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou un terminal de paiement de commerçant. Dans les deux cas, le fraudeur s'attache à ce qu'une telle carte supporte les données nécessaires pour tromper le système d'acceptation.
Numéro de carte usurpé	Le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage [b)] » et utilisé en vente à distance – qu'il y ait ou non une manipulation du payeur ayant pour effet d'obtenir ses codes confidentiels ou de réaliser l'authentification forte.
Autre	Tout autre motif de fraude comme l'utilisation d'un numéro de carte cohérent, mais non attribué à un porteur puis utilisé en vente à distance, la modification par le fraudeur d'un ordre de paiement légitime (falsification), etc.

a) Modification de l'impression en relief du numéro de carte.
b) Technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de carte pour générer de tels numéros.

Canal d'utilisation de la carte	Modalités d'utilisation
Paiement de proximité et sur automate	Paiement réalisé au point de vente ou sur automate, y compris le paiement en mode sans contact.
Paiement à distance (hors internet)	Paiement réalisé par courrier, postal ou électronique (courriel), ou par fax/téléphone, souvent qualifié de paiement MOTO par les systèmes de paiement par carte pour « *Mail Order, Telephone Order* ».
Paiement sur internet	Paiement réalisé sur internet (site commerçant ou via application).
Retrait	Retrait d'espèces à un distributeur automatique de billets.

Modalité du paiement sur internet	Description
Paiement 3-D Secure avec authentification forte	Paiement réalisé sur internet au travers de l'infrastructure 3-D Secure avec une authentification forte du porteur.
Paiement hors 3-D Secure avec authentification forte	Paiement réalisé sur internet, en dehors de l'infrastructure 3-D Secure, avec une authentification forte déléguée à un tiers, conformément aux règles d'externalisation applicables dans le cadre de la deuxième directive européenne sur les services de paiement (DSP2), (exemple : portefeuille mobile de type *X-Pay* proposé sous la responsabilité de l'émetteur, délégation de l'authentification forte auprès du commerçant sous la responsabilité de l'émetteur, etc.).
Paiement 3-D Secure sans authentification forte	Paiement réalisé sur internet au travers de l'infrastructure 3-D Secure sans authentification forte du porteur, c'est-à-dire en appliquant une exemption prévue par la réglementation européenne issue de la DSP2 ou en cas d'incident ne permettant pas de la mettre en œuvre. Les authentifications monofacteurs (exemple : SMS OTP – *one time password* – seul) sont également comprises dans cette catégorie.
Paiement non authentifié	Tout paiement réalisé en dehors de l'infrastructure 3-D Secure, recouvrant : • paiement non assujetti aux règles européennes sur l'authentification forte (DSP2) [a], comme le paiement initié par le créancier sur la base d'un accord préexistant entre le payeur et le créancier pour l'effectuer (par exemple : *Merchant Initiated Transaction* – MIT) et le paiement dit « *one-leg* » (l'émetteur ou l'acquéreur du paiement est situé hors de l'Union européenne) ; • paiement assujetti aux règles européennes sur l'authentification forte, mais dont le motif d'exemption à l'authentification forte est formalisé dans le flux d'autorisation ; • paiement assujetti aux règles européennes sur l'authentification forte, mais non conforme.

a) Les règles européennes sur l'authentification forte sont notamment précisées dans un acte délégué de la DSP2 : le règlement (UE) n°2018/389 détaillant pour les transactions assujetties au principe de l'authentification forte les différents motifs d'exemption et les conditions pour les mettre en œuvre.

Zone géographique	Description
Transaction nationale	L'émetteur et l'accepteur sont, tous deux, établis en France [a]. Pour autant, pour les paiements à distance, le fraudeur peut opérer depuis l'étranger.
Transaction européenne sortante	L'émetteur est établi en zone France et l'accepteur est établi à l'étranger dans l'Espace économique européen (EEE).
Transaction internationale sortante	L'émetteur est établi en zone France et l'accepteur est établi à l'étranger en dehors de l'Espace économique européen (hors EEE).
Transaction européenne entrante	L'émetteur est établi à l'étranger dans l'Espace économique européen (EEE) et l'accepteur est établi en zone France.
Transaction internationale entrante	L'émetteur est établi à l'étranger en dehors de l'Espace économique européen (hors EEE) et l'accepteur est établi en zone France.

a) Dans le cadre de cette collecte, le territoire français comprend la France métropolitaine, les départements et les régions d'outre-mer (Guadeloupe, Guyane, Martinique, Réunion, Saint-Pierre-et-Miquelon, Mayotte, Saint-Barthélemy et Saint-Martin) ainsi que la Principauté de Monaco. La Polynésie française, Wallis-et-Futuna et la Nouvelle-Calédonie ne font pas partie de la zone France et ne sont pas membres de l'Union européenne. Les opérations entre la France et ces collectivités sont donc comptabilisées comme des transactions internationales.

Secteur d'activité du commerçant pour les paiements à distance sur internet et hors internet	Description
Alimentation	Épiceries, supermarchés, hypermarchés, etc.
Approvisionnement d'un compte, vente de particulier à particulier	Sites de vente en ligne entre particuliers, etc.
Assurance	Souscription de contrats d'assurance.
Commerce généraliste et semi-généraliste	Textile/habillement, grand magasin généraliste, vente sur catalogue, vente privée, etc.
Équipement de la maison	Vente de produits d'ameublement et de bricolage.
Jeux en ligne	Sites de jeux et de paris en ligne.
Produits techniques et culturels	Matériel et logiciel informatiques, matériel photographique, livre, CD/DVD, etc.
Santé, beauté, hygiène	Vente de produits pharmaceutiques, parapharmaceutiques et cosmétiques.
Services aux particuliers et aux professionnels	Hôtellerie, service de location, billetterie de spectacle, organisme caritatif, matériel de bureau, service de messagerie, etc.
Téléphonie et communication	Matériel et service de télécommunication/téléphonie mobile.
Voyage, transport	Ferroviaire, aérien, maritime.
Divers	Les commerçants ne rentrant dans aucune des catégories susmentionnées.

MESURE DE LA FRAUDE AU VIREMENT

Transactions couvertes

La fraude au virement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement donnés par le débiteur – appelé donneur d'ordre – afin de transférer des fonds de son compte de paiement ou de monnaie électronique vers le compte d'un bénéficiaire tiers. Cette catégorie recouvre à la fois les virements au format SEPA (*SEPA credit transfer*), y compris les virements instantanés (*SEPA credit transfer Inst*), et les virements de clientèle émis via les systèmes de paiement de gros montant (notamment le système Target2 opéré par les banques centrales nationales de l'Eurosystème, ainsi que le système privé paneuropéen Euro1).

Origine des données de fraude

Les données de fraude au virement sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement [4] agréés dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux » de la Banque de France. Les données sont déclarées par les PSP en tant qu'établissement du payeur.

Éléments d'analyse de la fraude

La fraude au virement est analysée à partir des types de fraudes, des zones géographiques d'émission et de destination du virement et des canaux d'initiation utilisés.

4 Établissements autorisés à tenir des comptes de paiement pour le compte de leur clientèle et émettre des moyens de paiement relevant des statuts suivants au sens des réglementations françaises et européennes : i) établissements de crédit ou assimilés (institutions visées à l'article L. 518-1 du Code monétaire et financier), établissements de monnaie électronique et établissements de paiement de droit français ; ii) établissements de crédit, établissements de monnaie électronique et établissements de paiement de droit étranger habilités à intervenir sur le territoire français et établis sur ce dernier (c'est-à-dire présents en France sous la forme de « succursale »).

Typologie de la fraude au virement	Forme de la fraude
Faux	Le fraudeur contrefait un ordre de virement, ou usurpe les identifiants de la banque en ligne du donneur d'ordre légitime afin d'initier un ordre de paiement. Dans ce cas de figure, les identifiants peuvent notamment être obtenus via des procédés de piratage informatique (*phishing*, *malware*, etc.) ou sous la contrainte.
Falsification	Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime.
Détournement	Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.), le titulaire légitime du compte à émettre régulièrement un virement à destination d'un numéro de compte qui n'est pas celui du bénéficiaire légitime du paiement ou qui ne correspond à aucune réalité économique. Par exemple, sont considérés comme répondant à cette définition les cas de « fraude au Président » ou de fraude au changement de coordonnées bancaires.

Zone géographique d'émission et de destination du virement	Description
Virement national	Virement émis depuis un compte tenu en France [a)] vers un compte tenu en France.
Virement européen (virement transfrontalier au sein de l'EEE)	Virement émis depuis un compte tenu en France vers un compte tenu dans un autre pays de l'Espace économique européen (EEE).
Virement international (virement transfrontalier hors de l'EEE)	Virement émis depuis un compte tenu en France vers un compte tenu dans un pays étranger hors de l'Espace économique européen (EEE).

a) Dans le cadre de cette collecte, le territoire français comprend la France métropolitaine, les départements et les régions d'outre-mer (Guadeloupe, Guyane, Martinique, Réunion, Saint-Pierre-et-Miquelon, Mayotte, Saint-Barthélemy et Saint-Martin) ainsi que la Principauté de Monaco. La Polynésie française, Wallis-et-Futuna et la Nouvelle-Calédonie ne font pas partie de la zone France et ne sont pas membres de l'Union européenne. Les opérations entre la France et ces collectivités sont donc comptabilisées comme des transactions internationales.

Canal d'initiation utilisé	Modalités d'utilisation
Voie non électronique (courrier, courriel, téléphone)	Ordre de virement transmis par courrier, formulaire, courriel, télécopie ou téléphone. Ces virements ont en commun la nécessité de saisir de nouveau les instructions de paiement du payeur.
Banque en ligne	Ordre de virement initié par le payeur depuis son espace de banque en ligne (via un navigateur web ou une application mobile de banque en ligne) ou depuis un service d'initiation de paiement en ligne via son espace de banque en ligne.
Virement initié par lot/fichier (canaux télématiques)	Ordre de virement transmis via d'autres canaux électroniques (hors banque en ligne et application de paiement mobile), tels que le système EBICS (*Electronic Banking Internet Communication Standard*, canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque).
Virement électronique initié par canal non distant (GAB, guichet)	Ordre de virement initié au guichet bancaire ou depuis un guichet automatique de banque (GAB).
Prestataire de service d'initiation de paiement	Ordre de virement initié via un prestataire de service d'initiation de paiement (PSIP) à la demande du client.

MESURE DE LA FRAUDE AU PRÉLÈVEMENT

Transactions couvertes

La fraude au prélèvement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement donnés par le créancier à son prestataire de services de paiement afin de débiter le compte d'un débiteur conformément à l'autorisation (ou mandat de prélèvement) donnée par ce dernier. Cette catégorie est constituée des prélèvements au format européen SEPA (*SEPA direct debit – SDD*), et comprend le prélèvement standard (*SDD Core*) et le prélèvement interentreprises (*SDD B2B – business to business*).

Origine des données de fraude

Les données de fraude au prélèvement sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement agréés dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux » de la Banque de France. Les données sont déclarées par les PSP en tant qu'établissement du créancier.

Éléments d'analyse de la fraude

La fraude au prélèvement est analysée à partir des types de fraudes, des zones géographiques d'émission et de destination du prélèvement, du format du mandat de prélèvement et des modalités d'initiation.

Typologie de la fraude au prélèvement	Forme de la fraude
Faux	Le fraudeur créancier émet des prélèvements vers des numéros de compte qu'il a obtenus illégalement et sans aucune autorisation ou réalité économique sous-jacente (« opération de paiement non autorisée » dans la terminologie de l'Autorité bancaire européenne – ABE).
Détournement	Le fraudeur débiteur usurpe l'identité et l'IBAN (*international bank account number*) d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien (« manipulation du payeur par le fraudeur » dans la terminologie de l'ABE).

Zone géographique d'émission et de destination du virement	Forme de la fraude
Prélèvement national	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu en France.
Prélèvement européen	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un autre pays de l'Espace économique européen (EEE).
Prélèvement international	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un pays étranger hors de l'Espace économique européen (EEE).

Format du mandat de prélèvement	Description
Papier	Prélèvement émis sur la base d'un mandat collecté par un canal de type : courrier, formulaire, courriel, télécopie ou téléphone. Ces canaux ont en commun la nécessité de saisir de nouveau le mandat.
Électronique	Prélèvement émis sur la base d'un mandat collecté depuis un canal internet (site de banque en ligne, site ou application mobile du créancier) ou autres canaux télématiques.

Modalité d'initiation	Description
Prélèvement initié sur la base d'un paiement unique	Prélèvement automatique initié par voie électronique qui est indépendant d'autres prélèvements automatiques.
Prélèvement initié dans un fichier ou un lot	Prélèvement automatique initié par voie électronique faisant partie d'un groupe de prélèvements initiés ensemble par le créancier.

MESURE DE LA FRAUDE AU CHÈQUE

Contrairement aux autres moyens de paiement scripturaux, le chèque présente pour particularités de n'exister que sous format papier et d'utiliser la signature du payeur comme seul moyen d'authentification. Ces caractéristiques ne permettent pas la mise en œuvre par les acteurs bancaires de dispositifs d'authentification automatiques en amont du paiement.

Périmètre de la fraude

La fraude au chèque, telle que mesurée dans le présent rapport, porte sur les chèques payables en France, en euros ou en devises (pour ces derniers, il s'agit des chèques tirés sur un compte de paiement tenu en devises), répondant au régime juridique fixé aux articles L. 131-1 à 88 du Code monétaire et financier. Plus précisément, il s'agit des chèques tirés par la clientèle de l'établissement bancaire sur des comptes tenus par celui-ci, ainsi que des chèques reçus des clients de l'établissement pour crédit de ces mêmes comptes.

Cette définition intègre les titres suivants : chèque bancaire, chèque de banque, lettre-chèque pour les entreprises, titre de travail simplifié (TTS) aux entreprises ; elle exclut les chèques de voyage, ainsi que les titres spéciaux de paiement définis par l'article L. 525-4 du Code monétaire et financier et les instruments de paiement spécifiques définis à l'article L. 521-3-2 du même Code, tels que les chèques-vacances, les chèques ou titres restaurant, les chèques culture ou les chèques emploi-service universels, qui recouvrent des catégories variées de titres dont l'usage est restreint, soit à l'acquisition d'un nombre limité de biens ou de services, soit à un réseau limité d'accepteurs.

Origine des données de fraude

Les données de fraude au chèque sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux ». Ces derniers effectuent leur déclaration en qualité d'établissement recevant de son client des chèques à l'encaissement (établissement remettant).

Éléments d'analyse des données de fraude

Les données de fraude au chèque sont analysées à partir des grands types de fraudes définis par l'Observatoire. Pour le chèque, le tableau ci-après récapitule les formes de la fraude les plus couramment observées et la typologie à laquelle elles se rattachent.

Spécificités de l'approche de la fraude brute pour le chèque

Jusqu'en 2020, les données de fraude brute au chèque correspondaient à toutes les opérations par chèque remis à l'encaissement, présenté au paiement et rejeté pour un motif de fraude (fraude brute, ancienne approche).

À partir de 2021, les données de fraude brute au chèque excluent les fraudes déjouées par l'établissement après la présentation du chèque au paiement (fraude brute, nouvelle approche). Ces fraudes déjouées doivent répondre aux deux critères suivants :

1) Le chèque a été rejeté pour un motif de fraude avant que les fonds ne soient utilisables par le remettant grâce à une temporisation ou un blocage de la mise à disposition des fonds sur le compte du client (par exemple : l'utilisation d'un compte d'attente ou d'un compte technique). Le dernier cas comprend les rejets qui sont comptabilisés sur le compte du client remettant en même temps que les crédits.
2) L'établissement bancaire dispose d'une assurance raisonnable, étayée par des indicateurs formalisés, que le chèque pouvait être lié à une remise frauduleuse, c'est-à-dire une remise de chèque ayant pour objet de récupérer le bénéfice d'une fraude au chèque, y compris lorsque cette remise se fait au moyen d'un compte servant d'intermédiaire.

La fraude au chèque, dans son total comme dans sa ventilation par type de fraude, est calculée d'après la nouvelle approche de fraude brute, qui prend en compte les fraudes déjouées après présentation du chèque au paiement.

Typologie de la fraude au chèque	Forme de la fraude
Faux (vol, perte)	Utilisation par le fraudeur d'un chèque perdu ou volé à son titulaire légitime, revêtu d'une fausse signature qui n'est ni celle du titulaire du compte, ni celle de son mandataire. Émission illégitime d'un chèque par un fraudeur utilisant une formule vierge [a] (y compris lorsque l'opération a été effectuée sous la contrainte par le titulaire légitime).
Contrefaçon	Faux chèque créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque.
Falsification	Chèque régulier intercepté par un fraudeur qui l'altère volontairement par grattage, gommage ou effacement.
Détournement/rejeu	Chèque perdu ou volé après compensation dans les systèmes de paiement et présenté de nouveau à l'encaissement (rejeu). Chèque régulièrement émis, perdu ou volé, intercepté dans le circuit d'acheminement vers le bénéficiaire et encaissé sur un compte différent de celui du bénéficiaire légitime (détournement). La formule est correcte, le nom du bénéficiaire est inchangé et la ligne magnétique située en bas du chèque est valide, tout comme la signature du client.

a) Formule vierge : formule mise à la disposition du client par la banque teneur de compte.

MESURE DE LA FRAUDE AUX EFFETS DE COMMERCE

Transactions couvertes

La fraude aux effets de commerce, telle que mesurée dans le présent rapport, porte sur deux instruments de paiement :

- la lettre de change relevé (LCR) : instrument de paiement sur support papier ou dématérialisé par lequel le payeur (généralement le fournisseur) donne à son débiteur (son client) l'ordre de lui payer une somme d'argent déterminée ;
- le billet à ordre relevé (BOR) : ordre de paiement dématérialisé par lequel le payeur se reconnaît débiteur du bénéficiaire et promet de payer une certaine somme d'argent à un certain terme, tous deux spécifiés sur le titre.

Typologie et origine des données de fraude

Les types de fraudes aux effets de commerce sont les mêmes que ceux définis pour les chèques.

Les données de fraude sur les effets de commerce sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux ». Ces derniers effectuent leur déclaration en qualité d'établissement recevant de son client des effets de commerce à l'encaissement (établissement remettant).

MESURE DE LA FRAUDE SUR LES OPÉRATIONS DE TRANSMISSION DE FONDS

Transactions couvertes

Les opérations de transmission de fonds correspondent au service de paiement 6° établi à l'article L. 314-1 du Code monétaire et financier, conformément aux dispositions de la deuxième directive européenne sur les services de paiement (DSP2). Il s'agit d'un service de paiement pour lequel les fonds sont reçus de la part d'un payeur, sans création de comptes de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, et/ou pour lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci.

Origine des données sur la fraude

Les données de fraude sur les opérations de transmission de fonds sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux ». Ces derniers effectuent leur déclaration en qualité d'établissement du payeur (donneur d'ordre) avec une ventilation géographique identique à celle des virements.

MESURE DE LA FRAUDE SUR LES OPÉRATIONS INITIÉES VIA UN PRESTATAIRE DE SERVICE D'INITIATION DE PAIEMENT

Transactions couvertes

Le service d'initiation de paiement correspond au service de paiement 7° établi à l'article L. 314-1 du Code monétaire et financier, conformément aux dispositions de la DSP2. Il s'agit d'un service consistant à initier via un prestataire de service d'initiation de paiement (PSIP) agréé un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement (PSP). Cette opération prend généralement la forme d'un virement.

Origine des données sur la fraude

Les données de fraude sur le service d'initiation de paiement sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services d'initiation de paiement agréés ou établis en France dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux », avec une ventilation par canal d'initiation.

Canal d'initiation	Description
À distance	Paiement initié sur internet depuis un ordinateur, un téléphone portable ou tout autre terminal assimilé.
En proximité	Paiement initié au point de vente, sur automate ou au guichet bancaire, avec présence physique du payeur.

DISPOSITIONS SPÉCIFIQUES POUR LA FRAUDE SUR LES TRANSACTIONS EN MONNAIE ÉLECTRONIQUE

Transactions couvertes

La monnaie électronique constitue une valeur monétaire qui est stockée sous une forme électronique, représentant une créance sur l'émetteur qui doit être préalimentée au moyen d'un autre instrument de paiement, et qui peut être acceptée en paiement par une personne physique ou morale autre que l'émetteur de monnaie électronique (article L. 315-1 du Code monétaire et financier, conformément aux dispositions de la Directive 2009/110/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice, dite « DME 2 »).

On distingue deux catégories de support de monnaie électronique :

- les supports physiques de type carte prépayée ;
- les comptes en ligne tenus par l'établissement émetteur.

Origine des données sur la fraude

Les données de la fraude sur les paiements sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les émetteurs de monnaie électronique dans le cadre de la collecte « Recensement de la fraude aux moyens de paiement scripturaux ». Ces derniers fournissent les données avec une ventilation par canal d'initiation (quel que soit le support utilisé, support physique de type carte prépayée ou compte en ligne tenu par l'établissement).

Canal d'initiation	Description
À distance	Paiement initié depuis un canal internet à partir d'un ordinateur, d'un téléphone portable ou tout autre terminal assimilé.
En proximité	Paiement initié au point de vente, sur automate ou au guichet bancaire, y compris en mode sans contact avec présence physique du payeur.

A5 DOSSIER STATISTIQUE SUR L'USAGE ET LA FRAUDE AUX MOYENS DE PAIEMENT

Des tableaux complémentaires, ainsi que l'ensemble des tableaux contenus dans cette annexe mais qui peuvent présenter parfois une plus grande profondeur historique, sont disponibles pour téléchargement à l'adresse suivante :
https://www.banque-france.fr/system/files/2026-09/OSMP-2025_Annexe-5_Dossier-statistique.xlsx

PANORAMA DES MOYENS DE PAIEMENT

T1 Cartographie des moyens de paiement scripturaux en 2025
(nombre en millions, montant en milliards d'euros, montant moyen en euros, variation et part en pourcentage)

	Nombre de transactions			Montant des transactions			Montant moyen
	2025	Variation 2025/2024	Part	2025	Variation 2025/2024	Part	
Paiement carte [a]	22 355	6,5	62,7	876	3,8	2,4	39
dont sans contact	*12 654*	*10,5*	*35,5*	*236*	*15,7*	*0,7*	*19*
dont paiement par mobile	*3 413*	*38,0*	*9,6*	*75*	*33,9*	*0,2*	*22*
Chèque	674	- 14,0	1,9	331	- 15,7	0,9	491
Virement	6 362	6,5	17,9	32 416	4,4	89,4	5 095
dont VGM [b]	*10*	*- 3,7*	*0,0*	*11 066*	*6,8*	*30,5*	*1 079 425*
dont virement instantané (SCT Inst)	*1 066*	*78,4*	*3,0*	*505*	*118,3*	*1,4*	*473*
Prélèvement	5 040	5,3	14,1	2 300	5,6	6,3	456
Effet de commerce	68	- 3,7	0,2	198	- 3,5	0,5	2 931
Monnaie électronique	102	3,5	0,3	12	880,0	0,0	119
Transmission de fonds	18	53,6	0,1	2	26,5	0,0	105
Total	**34 618**	**5,8**	**97,1**	**36 134**	**4,2**	**99,6**	**1 044**
Retrait par carte [a]	1 024	- 5,1	2,9	129	- 3,0	0,4	126
Total transactions	**35 642**	**5,5**	**100,0**	**36 264**	**4,2**	**100,0**	**1 017**

a) Cartes émises en France uniquement.
b) VGM : virement de gros montant émis au travers de systèmes de paiement de montant élevé (Target2, Euro1), correspondant exclusivement à des paiements professionnels.
Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer*.

Source : Observatoire de la sécurité des moyens de paiement.

T2 Évolution historique des paiements scripturaux

a) En volume
(en millions de transactions)

	2018	2019	2020	2021	2022	2023	2024	2025
Carte	13 179	14 485	13 852	16 129	18 258	19 685	20 983	22 355
dont sans contact	*2 374*	*3 779*	*5 159*	*7 369*	*9 103*	*10 792*	*11 454*	*12 654*
dont par mobile	*11*	*48*	*129*	*357*	*845*	*1 609*	*2 473*	*3 413*
Chèque	1 747	1 587	1 175	1 106	1 008	891	784	674
Virement	4 038	4 269	4 483	4 843	5 158	5 613	5 975	6 362
dont virement instantané (SCT Inst)	*0*	*14*	*45*	*107*	*198*	*408*	*598*	*1 066*
Prélèvement	4 211	4 370	4 622	5 020	4 914	4 616	4 788	5 040
Effet de commerce	81	78	71	75	75	74	70	68
Monnaie électronique	65	62	36	63	75	88	98	102
Transmission de fonds	16	16	15	2	3	8	12	18
Total paiements scripturaux	**23 320**	**24 851**	**24 238**	**27 238**	**29 491**	**30 975**	**32 710**	**34 618**
Retrait par carte	1 439	1 392	1 064	1 086	1 136	1 127	1 079	1 024
Total transactions	**24 759**	**26 243**	**25 302**	**28 324**	**30 627**	**32 102**	**33 789**	**35 642**

b) En montant
(en milliards d'euros)

	2018	2019	2020	2021	2022	2023	2024	2025
Carte	568	600	578	660	746	806	844	876
dont sans contact	*25*	*43*	*80*	*125*	*148*	*175*	*204*	*236*
dont par mobile	*0,2*	*1*	*3*	*8*	*18*	*36*	*56*	*75*
Chèque	891	814	614	589	540	467	392	331
Virement	24 296	25 164	32 712	38 723	38 895	29 942	31 057	32 416
dont virement instantané (SCT Inst)	*0,086*	*7*	*27*	*50*	*119*	*177*	*231*	*505*
Prélèvement	1 645	1 711	1 684	1 895	2 041	2 139	2 178	2 300
Effet de commerce	252	232	197	212	222	218	205	198
Monnaie électronique	1	1	1	1	1	1	1	12
Transmission de fonds	2	2	2	1	1	1	1	2
Total paiements scripturaux	**27 653**	**28 522**	**35 786**	**42 081**	**42 445**	**33 574**	**34 679**	**36 134**
Retrait par carte	137	137	116	124	133	136	133	129
Total transactions	**27 789**	**28 658**	**35 902**	**42 204**	**42 578**	**33 710**	**34 812**	**36 264**

Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer*.

Source : Observatoire de la sécurité des moyens de paiement.

T3 Répartition de la fraude sur les moyens de paiement en 2025

(valeur et montant moyen en euros ; volume en unités ; variation, part et taux en pourcentage)

	Volume			Valeur			Taux de fraude	Montant moyen
	2025	Variation 2025/2024	Part	2025	Variation 2025/2024	Part	2025	
Paiement carte [a)]	6 582 317	- 10,0	91,5	432 455 222	0,0	34,9	0,0494	66
dont sans contact	*700 825*	*- 6,2*	*9,7*	*21 142 482*	*- 6,6*	*1,7*	*0,0090*	*30*
dont par mobile	*106 252*	*- 17,7*	*1,5*	*6 879 848*	*- 23,8*	*0,6*	*0,0092*	*65*
Chèque (nouvelle approche) [b)]	158 405	- 12,0	2,2	228 944 293	- 16,0	18,5	0,0692	1 445
Chèque (ancienne approche)	198 019	- 11,3	2,8	387 099 403	- 17,2	31,2	0,1171	1 955
Virement	290 495	123,3	4,0	484 652 054	36,7	39,1	0,0015	1 323
dont virement instantané (SCT Inst)	*182 568*	*133,1*	*2,5*	*205 871 733*	*91,7*	*16,6*	*0,0408*	*1 128*
Prélèvement	56 263	6,6	0,8	33 254 401	9,3	2,7	0,0014	591
Effet de commerce	317	- 9,7	0,0	19 309 212	6,0	1,6	0,0097	60 912
Monnaie électronique	2 085	- 35,5	0,0	54 723	- 42,9	0,0	0,0005	26
Transmission de fonds	178	107,0	0,0	48 544	172,8	0,0	0,0026	273
Total paiements	**7 090 060**	**- 7,7**	**98,6**	**1 198 718 449**	**3,9**	**96,6**	**0,0033**	**169**
Retrait par carte [a)]	102 602	- 5,0	1,4	42 085 961	3,2	3,4	0,0325	410
Total transactions	**7 192 662**	**- 7,6**	**100,0**	**1 240 804 410**	**3,8**	**100,0**	**0,0034**	**173**

a) Cartes émises en France uniquement.
b) La nouvelle approche de la fraude au chèque consiste à exclure les fraudes qui sont déjouées après remise du chèque à l'encaissement.
Notes : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer*.
À partir de 2021, le total de la fraude aux moyens de paiement scripturaux reprend une nouvelle approche de la fraude au chèque, qui exclut les fraudes qui sont déjouées après remise du chèque à l'encaissement, et intègre la fraude sur la monnaie électronique et les transmissions de fonds.

Source : Observatoire de la sécurité des moyens de paiement.

T4 Évolution historique de la fraude sur les moyens de paiement

a) En volume
(en unités)

	2018	2019	2020	2021	2022	2023	2024	2025
Carte	6 068 959	7 071 095	7 421 137	6 764 752	6 692 988	6 635 955	7 313 819	6 582 317
dont sans contact	*445 919*	*603 509*	*537 061*	*604 278*	*796 027*	*733 359*	*746 923*	*700 825*
dont par mobile	*2 070*	*3 494*	*33 761*	*83 266*	*162 869*	*110 133*	*129 052*	*106 252*
Chèque (nouvelle approche)	nd	nd	190 001	232 277	218 122	206 197	180 059	158 405
Chèque (ancienne approche)	166 421	183 488	220 685	272 970	266 216	255 857	223 309	198 019
Virement	7 736	15 934	35 893	46 718	76 846	90 453	130 092	290 495
dont virement instantané (SCT Inst)	*5*	*729*	*7 131*	*12 913*	*33 193*	*48 630*	*78 316*	*182 568*
Prélèvement	309 377	43 519	6 485	251 010	49 453	77 876	52 799	56 263
Effet de commerce	5	1	62	1	1	34	351	317
Monnaie électronique	nd	nd	nd	2 001	1 945	3 135	3 232	2 085
Transmission de fonds	nd	nd	nd	962	154	102	86	178
Total fraude paiements scripturaux	**6 552 498**	**7 314 037**	**7 684 262**	**7 297 721**	**7 039 509**	**7 013 752**	**7 680 438**	**7 090 060**
Retrait par carte	158 908	165 505	113 067	129 083	123 574	110 221	108 013	102 602
Total fraude transactions	**6 711 406**	**7 479 542**	**7 797 329**	**7 426 804**	**7 163 083**	**7 123 973**	**7 788 451**	**7 192 662**

b) En valeur
(en euros)

	2018	2019	2020	2021	2022	2023	2024	2025
Carte	401 604 986	428 249 931	439 489 315	421 410 285	420 585 823	455 204 894	478 472 400	432 455 222
dont sans contact	*5 234 852*	*8 479 354*	*11 292 261*	*16 274 668*	*23 047 180*	*18 786 086*	*22 648 147*	*21 142 482*
dont par mobile	*73 682*	*216 236*	*2 792 574*	*5 610 270*	*10 942 984*	*7 294 895*	*9 023 196*	*6 879 848*
Chèque (nouvelle approche)	nd	nd	401 611 189	465 021 167	395 416 196	363 929 512	272 398 979	228 944 293
Chèque (ancienne approche)	450 108 464	539 215 175	538 059 139	625 703 442	556 796 815	588 194 101	467 435 789	387 099 403
Virement	97 327 128	161 642 174	266 969 099	287 264 068	313 163 442	312 487 450	354 549 264	484 652 054
dont virement instantané (SCT Inst)	*29 800*	*2 203 240*	*10 562 419*	*22 406 942*	*52 768 218*	*69 003 730*	*107 400 214*	*205 871 733*
Prélèvement	58 346 253	10 990 025	1 891 051	25 318 677	19 853 012	22 320 813	30 416 859	33 254 401
Effet de commerce	226 217	74 686	538 918	12 079	12 079	1 296 652	18 212 791	19 309 212
Monnaie électronique	nd	nd	nd	137 340	77 349	176 276	95 876	54 723
Transmission de fonds	nd	nd	nd	246 362	77 162	55 333	17 796	48 544
Total fraude paiements scripturaux	**1 007 613 048**	**1 140 171 991**	**1 246 947 522**	**1 199 409 978**	**1 149 185 062**	**1 155 470 930**	**1 154 163 965**	**1 198 718 449**
Retrait par carte	37 630 659	41 651 788	33 950 879	42 950 169	43 148 054	40 608 913	40 763 581	42 085 961
Total fraude transactions	**1 045 243 707**	**1 181 823 779**	**1 280 898 401**	**1 242 360 147**	**1 192 333 116**	**1 196 079 843**	**1 194 927 546**	**1 240 804 410**

nd, non disponible.
Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer*.
À partir de 2021, le total de la fraude aux moyens de paiement scripturaux reprend une nouvelle approche de la fraude au chèque, qui exclut les fraudes qui sont déjouées après remise du chèque à l'encaissement, et intègre la fraude sur la monnaie électronique et les transmissions de fonds.

Source : Observatoire de la sécurité des moyens de paiement.

CARTE : ÉMISSION

T5 Paiements par carte émise en France (tableau 1/2)

(volume en milliers, montant en milliers d'euros)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**11 193 795**	**424 105 649**	**12 935 438**	**475 079 750**	**14 868 338**	**537 503 850**
dont paiements sans contact (y compris paiements par mobile)	*5 159 657*	*79 664 370*	*7 368 699*	*125 082 420*	*9 102 931*	*148 006 593*
dont paiements par mobile	*129 105*	*2 734 667*	*357 355*	*7 596 769*	*845 223*	*17 937 091*
Paiements à distance (hors internet)	**134 114**	**7 567 877**	**76 931**	**7 995 010**	**105 781**	**16 994 865**
Paiements sur internet	**2 524 317**	**146 563 476**	**3 116 285**	**177 056 237**	**3 283 604**	**191 418 128**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*444 723*	*19 267 910*	*781 313*	*27 091 534*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*1 883 898*	*72 566 685*	*1 467 342*	*51 612 860*
Retraits	**1 064 095**	**115 958 207**	**1 086 289**	**123 867 648**	**1 135 675**	**132 879 066**
Total	**14 916 322**	**694 195 208**	**17 214 942**	**783 998 644**	**19 393 398**	**878 795 909**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T5 Paiements par carte émise en France (tableau 2/2)

(volume en milliers, valeur en milliers d'euros)

	2023		2024		2025	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**15 903 747**	**570 896 450**	**16 742 274**	**586 536 066**	**17 531 636**	**596 350 786**
dont paiements sans contact (y compris paiements par mobile)	*10 792 452*	*174 706 103*	*11 453 514*	*203 943 905*	*12 653 713*	*235 966 705*
dont paiements par mobile	*1 609 423*	*35 539 253*	*2 472 705*	*56 018 195*	*3 413 403*	*75 011 613*
Paiements à distance (hors internet)	**96 368**	**15 880 261**	**95 731**	**14 873 579**	**83 847**	**11 715 664**
Paiements sur internet	**3 685 180**	**219 662 525**	**4 144 823**	**242 232 777**	**4 739 148**	**267 795 728**
dont paiements 3-D Secure avec authentification forte	*1 282 644*	*136 151 668*	*1 153 075*	*139 292 722*	*1 153 541*	*145 045 956*
dont paiements hors 3-D Secure avec authentification forte	*135 611*	*4 119 307*	*382 740*	*14 661 163*	*611 721*	*23 410 148*
dont paiements 3-D Secure sans authentification forte	*800 728*	*27 212 160*	*896 289*	*31 855 769*	*1 283 806*	*44 055 330*
dont paiements hors 3-D Secure sans authentification forte	*1 466 199*	*52 179 389*	*1 712 719*	*56 423 122*	*1 690 080*	*55 284 294*
dont paiements initiés par le commerçant (MIT)	*877 839*	*30 771 262*	*1 032 022*	*33 940 666*	*1 180 458*	*37 855 917*
dont paiements « one-leg »	*31 151*	*1 997 096*	*43 267*	*2 235 967*	*51 308*	*2 251 701*
dont paiements non 3-D Secure conformes à la DSP2	*250 843*	*9 039 674*	*254 856*	*8 099 577*	*159 030*	*6 299 716*
dont paiements non 3-D Secure non conformes à la DSP2	*306 366*	*10 371 359*	*382 573*	*12 146 912*	*299 284*	*8 876 960*
Retraits	**1 127 043**	**135 511 148**	**1 079 441**	**133 312 840**	**1 024 337**	**129 329 359**
Total	**20 812 338**	**941 950 384**	**22 062 270**	**976 955 262**	**23 378 967**	**1 005 191 537**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T5 *bis* Nombre de cartes et supports

T6 Transactions frauduleuses par carte émise en France (tableau 1/2)

(volume en unités, valeur en euros, taux en pourcentage)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**972 228**	**47 994 762**	**0,011**	**942 376**	**52 426 587**	**0,011**	**1 055 575**	**62 861 464**	**0,012**
dont paiements sans contact (y compris paiements par mobile)	*537 061*	*11 292 261*	*0,014*	*604 278*	*16 274 668*	*0,013*	*796 027*	*23 047 180*	*0,016*
dont paiements par mobile	*33 761*	*2 792 574*	*0,102*	*83 266*	*5 610 270*	*0,074*	*162 869*	*10 942 984*	*0,061*
Paiements à distance (hors internet)	**411 344**	**26 899 103**	**0,355**	**124 596**	**22 193 382**	**0,278**	**174 364**	**42 028 102**	**0,247**
Paiements sur internet	**6 037 565**	**364 595 450**	**0,249**	**5 697 780**	**346 790 316**	**0,196**	**5 463 049**	**315 696 257**	**0,165**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*364 223*	*26 046 078*	*0,135*	*625 296*	*25 695 176*	*0,095*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*4 837 540*	*217 714 555*	*0,300*	*4 213 280*	*165 742 266*	*0,321*
Retraits	**113 067**	**33 950 879**	**0,029**	**129 083**	**42 950 169**	**0,035**	**123 574**	**43 148 054**	**0,032**
Total	**7 534 204**	**473 440 194**	**0,068**	**6 893 835**	**464 360 454**	**0,059**	**6 816 562**	**463 733 877**	**0,053**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T6 Transactions frauduleuses par carte émise en France (tableau 2/2)

(volume en unités, valeur en euros, taux en pourcentage)

	2023			2024			2025		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**966 134**	**61 618 923**	**0,011**	**943 117**	**62 968 479**	**0,011**	**866 181**	**63 007 893**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	*733 359*	*18 786 086*	*0,011*	*746 923*	*22 648 147*	*0,011*	*700 825*	*21 142 482*	*0,009*
dont paiements par mobile	*110 133*	*7 294 895*	*0,021*	*129 052*	*9 023 196*	*0,016*	*106 252*	*6 879 848*	*0,009*
Paiements à distance (hors internet)	**186 499**	**42 177 372**	**0,266**	**183 666**	**40 377 262**	**0,271**	**199 808**	**37 722 329**	**0,322**
Paiements sur internet	**5 483 322**	**351 408 599**	**0,160**	**6 187 036**	**375 126 659**	**0,155**	**5 516 328**	**331 725 000**	**0,124**
dont paiements 3-D Secure avec authentification forte	*722 396*	*132 754 198*	*0,098*	*676 055*	*128 822 135*	*0,092*	*645 766*	*122 727 261*	*0,085*
dont paiements hors 3-D Secure avec authentification forte	*159 680*	*8 966 661*	*0,218*	*189 142*	*11 192 865*	*0,076*	*226 197*	*17 522 421*	*0,075*
dont paiements 3-D Secure sans authentification forte	*593 808*	*22 929 848*	*0,084*	*449 128*	*17 294 653*	*0,054*	*649 597*	*22 797 014*	*0,052*
dont paiements hors 3-D Secure sans authentification forte	*4 007 438*	*186 757 892*	*0,358*	*4 872 711*	*217 817 006*	*0,386*	*3 994 768*	*168 678 304*	*0,305*
dont paiements initiés par le commerçant (MIT)	*1 995 881*	*87 685 148*	*0,285*	*2 487 438*	*106 598 193*	*0,314*	*2 067 773*	*83 896 939*	*0,222*
dont paiements « one-leg »	*416 116*	*30 632 806*	*1,534*	*651 446*	*43 751 776*	*1,957*	*565 445*	*32 313 474*	*1,435*
dont paiements non 3-D Secure conformes à la DSP2	*553 018*	*16 515 229*	*0,183*	*517 251*	*13 877 894*	*0,171*	*239 846*	*5 331 628*	*0,085*
dont paiements non 3-D Secure non conformes à la DSP2	*1 042 423*	*51 924 709*	*0,501*	*1 216 576*	*53 589 143*	*0,441*	*1 121 704*	*47 136 263*	*0,531*
Retraits	**110 221**	**40 608 913**	**0,030**	**108 013**	**40 763 581**	**0,031**	**102 602**	**42 085 961**	**0,033**
Total	**6 746 176**	**495 813 807**	**0,053**	**7 421 832**	**519 235 981**	**0,053**	**6 684 919**	**474 541 183**	**0,047**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2025 (tableau 1/2)

(volume en unités, valeur en euros, part en pourcentage)

	Cartes perdues ou volées				Cartes non parvenues				Cartes altérées ou contrefaites			
	Volume		Valeur		Volume		Valeur		Volume		Valeur	
	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part
Paiements de proximité et sur automate	**526 189**	**60,7**	**38 025 245**	**60,3**	**5 710**	**0,7**	**953 783**	**1,5**	**89 405**	**10,3**	**6 610 733**	**10,5**
dont paiements sans contact (y compris paiements par mobile)	*441 837*	*63,0*	*10 755 307*	*50,9*	*2 485*	*0,4*	*57 873*	*0,3*	*68 203*	*9,7*	*2 741 662*	*13,0*
dont paiements par mobile	*38 316*	*36,1*	*2 546 989*	*37,0*	*446*	*0,4*	*13 071*	*0,2*	*24 372*	*22,9*	*1 544 141*	*22,4*
Paiements à distance (hors internet)	**15 241**	**7,6**	**3 566 360**	**9,5**	**113**	**0,1**	**7 079**	**0,0**	**607**	**0,3**	**229 864**	**0,6**
Paiements sur internet	**261 826**	**4,7**	**21 474 302**	**6,5**	**2 946**	**0,1**	**226 305**	**0,1**	**109 897**	**2,0**	**6 026 501**	**1,8**
dont paiements 3-D Secure avec authentification forte	*33 935*	*5,3*	*9 004 360*	*7,3*	*527*	*0,1*	*111 275*	*0,1*	*289*	*0,0*	*102 375*	*0,1*
dont paiements hors 3-D Secure avec authentification forte	*8 087*	*3,6*	*673 076*	*3,8*	*374*	*0,2*	*32 834*	*0,2*	*94*	*0,0*	*6 922*	*0,0*
dont paiements 3-D Secure sans authentification forte	*35 490*	*5,5*	*1 778 132*	*7,8*	*351*	*0,1*	*8 061*	*0,0*	*712*	*0,1*	*37 736*	*0,2*
dont paiements hors 3-D Secure sans authentification forte	*184 314*	*4,6*	*10 018 734*	*5,9*	*1 694*	*0,0*	*74 135*	*0,0*	*108 802*	*2,7*	*5 879 468*	*3,5*
dont paiements initiés par le commerçant (MIT)	*143 819*	*7,0*	*7 012 415*	*8,4*	*922*	*0,0*	*36 508*	*0,0*	*67 273*	*3,3*	*2 964 465*	*3,5*
dont paiements « one-leg »	*11 943*	*2,1*	*1 084 947*	*3,4*	*314*	*0,1*	*21 326*	*0,1*	*20 034*	*3,5*	*1 851 079*	*5,7*
dont paiements non 3-D Secure conformes à la DSP2	*7 400*	*3,1*	*341 737*	*6,4*	*153*	*0,1*	*4 551*	*0,1*	*840*	*0,4*	*23 158*	*0,4*
dont paiements non 3-D Secure non conformes à la DSP2	*21 152*	*1,9*	*1 579 635*	*3,4*	*305*	*0,0*	*11 750*	*0,0*	*20 655*	*1,8*	*1 040 766*	*2,2*
Retraits	**74 052**	**72,2**	**33 275 728**	**79,1**	**1 664**	**1,6**	**491 167**	**1,2**	**9 775**	**9,5**	**3 131 929**	**7,4**
Total	**877 308**	**13,1**	**96 341 635**	**20,3**	**10 433**	**0,2**	**1 678 334**	**0,4**	**209 684**	**3,1**	**15 999 027**	**3,4**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2025 (tableau 2/2)

(volume en unités, valeur en euros, part en pourcentage)

	Numéros de carte usurpés				Autres				Toutes origines	
	Volume		Valeur		Volume		Valeur		Volume	Valeur
	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part		
Paiements de proximité et sur automate	**97 074**	**11,2**	**7 675 086**	**12,2**	**147 803**	**17,1**	**9 743 046**	**15,5**	**866 181**	**63 007 893**
dont paiements sans contact (y compris paiements par mobile)	*65 424*	*9,3*	*1 990 060*	*9,4*	*122 876*	*17,5*	*5 597 580*	*26,5*	*700 825*	*21 142 482*
dont paiements par mobile	*11 057*	*10,4*	*753 346*	*11,0*	*32 061*	*30,2*	*2 022 301*	*29,4*	*106 252*	*6 879 848*
Paiements à distance (hors internet)	**182 787**	**91,5**	**33 819 081**	**89,7**	**1 060**	**0,5**	**99 945**	**0,3**	**199 808**	**37 722 329**
Paiements sur internet	**5 070 856**	**91,9**	**297 802 490**	**89,8**	**70 803**	**1,3**	**6 195 402**	**1,9**	**5 516 328**	**331 725 000**
dont paiements 3-D Secure avec authentification forte	*598 330*	*92,7*	*110 559 644*	*90,1*	*12 685*	*2,0*	*2 949 607*	*2,4*	*645 766*	*122 727 261*
dont paiements hors 3-D Secure avec authentification forte	*213 382*	*94,3*	*16 301 634*	*93,0*	*4 260*	*1,9*	*507 955*	*2,9*	*226 197*	*17 522 421*
dont paiements 3-D Secure sans authentification forte	*600 650*	*92,5*	*20 493 522*	*89,9*	*12 394*	*1,9*	*479 563*	*2,1*	*649 597*	*22 797 014*
dont paiements hors 3-D Secure sans authentification forte	*3 658 494*	*91,6*	*150 447 690*	*89,2*	*41 464*	*1,0*	*2 258 277*	*1,3*	*3 994 768*	*168 678 304*
dont paiements initiés par le commerçant (MIT)	*1 843 311*	*89,1*	*73 356 757*	*87,4*	*12 448*	*0,6*	*526 794*	*0,6*	*2 067 773*	*83 896 939*
dont paiements « one-leg »	*516 624*	*91,4*	*28 669 437*	*88,7*	*16 530*	*2,9*	*686 685*	*2,1*	*565 445*	*32 313 474*
dont paiements non 3-D Secure conformes à la DSP2	*226 727*	*94,5*	*4 533 727*	*85,0*	*4 726*	*2,0*	*428 455*	*8,0*	*239 846*	*5 331 628*
dont paiements non 3-D Secure non conformes à la DSP2	*1 071 832*	*95,6*	*43 887 769*	*93,1*	*7 760*	*0,7*	*616 343*	*1,3*	*1 121 704*	*47 136 263*
Retraits	**1 842**	**1,8**	**407 267**	**1,0**	**15 269**	**14,9**	**4 779 870**	**11,4**	**102 602**	**42 085 961**
Total	**5 352 559**	**80,1**	**339 703 924**	**71,6**	**234 935**	**3,5**	**20 818 263**	**4,4**	**6 684 919**	**474 541 183**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2025 (tableau 1/2)

(volume en unités, valeur en euros, part en pourcentage)

	Transactions nationales				Transactions européennes			
	Volume		Valeur		Volume		Valeur	
	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part
Paiements de proximité et sur automate	**748 556**	**86,4**	**44 344 704**	**70,4**	**37 802**	**4,4**	**3 784 056**	**6,0**
dont paiements sans contact (y compris paiements par mobile)	*618 301*	*88,2*	*15 217 597*	*72,0*	*31 591*	*4,5*	*2 245 958*	*10,6*
dont paiements par mobile	*93 693*	*88,2*	*5 107 767*	*74,2*	*5 868*	*5,5*	*979 436*	*14,2*
Paiements à distance (hors internet)	**89 281**	**44,7**	**19 044 981**	**50,5**	**62 825**	**31,4**	**10 107 078**	**26,8**
Paiements sur internet	**1 432 194**	**26,0**	**132 543 339**	**40,0**	**2 566 383**	**46,5**	**114 691 889**	**34,6**
dont paiements 3-D Secure avec authentification forte	*236 171*	*36,6*	*67 457 901*	*55,0*	*304 144*	*47,1*	*42 180 665*	*34,4*
dont paiements hors 3-D Secure avec authentification forte	*48 018*	*21,2*	*6 949 937*	*39,7*	*139 418*	*61,6*	*7 766 172*	*44,3*
dont paiements 3-D Secure sans authentification forte	*259 679*	*40,0*	*11 515 059*	*50,5*	*329 341*	*50,7*	*8 589 431*	*37,7*
dont paiements hors 3-D Secure sans authentification forte	*888 326*	*22,2*	*46 620 442*	*27,6*	*1 793 480*	*44,9*	*56 155 621*	*33,3*
dont paiements initiés par le commerçant (MIT)	*714 965*	*34,6*	*34 919 958*	*41,6*	*961 666*	*46,5*	*33 484 337*	*39,9*
dont paiements « one-leg »	*0*	*0,0*	*0*	*0,0*	*0*	*0,0*	*0*	*0,0*
dont paiements non 3-D Secure conformes à la DSP2	*28 066*	*11,7*	*2 420 331*	*45,4*	*204 097*	*85,1*	*2 618 800*	*49,1*
dont paiements non 3-D Secure non conformes à la DSP2	*145 295*	*13,0*	*9 280 153*	*19,7*	*627 717*	*56,0*	*20 052 484*	*42,5*
Retraits	**92 850**	**90,5**	**40 110 780**	**95,3**	**2 638**	**2,6**	**786 754**	**1,9**
Total	**2 362 881**	**35,3**	**236 043 804**	**49,7**	**2 669 648**	**39,9**	**129 369 777**	**27,3**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2025 (tableau 2/2)

(volume en unités, valeur en euros, part en pourcentage)

	Transactions internationales				Total	
	Volume		Valeur		Volume	Valeur
	Nombre	Part	Montant	Part		
Paiements de proximité et sur automate	**79 823**	**9,2**	**14 879 133**	**23,6**	**866 181**	**63 007 893**
dont paiements sans contact (y compris paiements par mobile)	*50 933*	*7,3*	*3 678 927*	*17,4*	*700 825*	*21 142 482*
dont paiements par mobile	*6 691*	*6,3*	*792 645*	*11,5*	*106 252*	*6 879 848*
Paiements à distance (hors internet)	**47 702**	**23,9**	**8 570 270**	**22,7**	**199 808**	**37 722 329**
Paiements sur internet	**1 517 751**	**27,5**	**84 489 772**	**25,5**	**5 516 328**	**331 725 000**
dont paiements 3-D Secure avec authentification forte	*105 451*	*16,3*	*13 088 695*	*10,7*	*645 766*	*122 727 261*
dont paiements hors 3-D Secure avec authentification forte	*38 761*	*17,1*	*2 806 312*	*16,0*	*226 197*	*17 522 421*
dont paiements 3-D Secure sans authentification forte	*60 577*	*9,3*	*2 692 524*	*11,8*	*649 597*	*22 797 014*
dont paiements hors 3-D Secure sans authentification forte	*1 312 962*	*32,9*	*65 902 241*	*39,1*	*3 994 768*	*168 678 304*
dont paiements initiés par le commerçant (MIT)	*391 142*	*18,9*	*15 492 644*	*18,5*	*2 067 773*	*83 896 939*
dont paiements « one-leg »	*565 445*	*100,0*	*32 313 474*	*100,0*	*565 445*	*32 313 474*
dont paiements non 3-D Secure conformes à la DSP2	*7 683*	*3,2*	*292 497*	*5,5*	*239 846*	*5 331 628*
dont paiements non 3-D Secure non conformes à la DSP2	*348 692*	*31,1*	*17 803 626*	*37,8*	*1 121 704*	*47 136 263*
Retraits	**7 114**	**6,9**	**1 188 427**	**2,8**	**102 602**	**42 085 961**
Total	**1 652 390**	**24,7**	**109 127 602**	**23,0**	**6 684 919**	**474 541 183**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T9 Paiements par carte émise et acceptée en France – Transactions nationales (tableau 1/2)

(volume en milliers, montant en milliers d'euros)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**10 978 602**	**413 760 411**	**12 611 966**	**460 274 895**	**14 340 211**	**514 159 801**
dont paiements sans contact (y compris paiements par mobile)	*5 081 519*	*78 386 853*	*7 202 992*	*121 694 861*	*8 781 813*	*141 160 469*
dont paiements par mobile	*126 945*	*2 687 300*	*348 251*	*7 390 633*	*808 622*	*17 132 553*
Paiements à distance (hors internet)	**60 243**	**5 428 918**	**56 236**	**5 540 339**	**87 602**	**13 259 829**
Paiements sur internet	**2 011 431**	**122 128 921**	**2 399 865**	**142 184 895**	**2 393 161**	**146 642 890**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*389 530*	*15 797 723*	*717 916*	*24 981 800*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*1 348 375*	*54 203 060*	*866 207*	*32 704 868*
Retraits	**1 038 647**	**112 337 533**	**1 056 936**	**119 485 544**	**1 101 989**	**128 161 781**
Total	**14 088 924**	**653 655 783**	**16 125 003**	**727 485 673**	**17 922 963**	**802 224 301**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T9 Paiements par carte émise et acceptée en France – Transactions nationales (tableau 2/2)

(volume en milliers, valeur en milliers d'euros)

	2023		2024		2025	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**15 252 122**	**543 567 354**	**16 006 321**	**556 776 079**	**16 698 881**	**564 910 390**
dont paiements sans contact (y compris paiements par mobile)	*10 357 439*	*164 920 568*	*10 909 977*	*190 761 361*	*11 990 226*	*220 177 843*
dont paiements par mobile	*1 533 084*	*33 773 794*	*2 350 573*	*53 025 223*	*3 221 593*	*70 378 206*
Paiements à distance (hors internet)	**82 700**	**12 227 259**	**81 855**	**11 297 010**	**71 941**	**9 425 251**
Paiements sur internet	**2 580 907**	**164 682 672**	**2 818 216**	**179 516 356**	**3 169 650**	**200 229 722**
dont paiements 3-D Secure avec authentification forte	*977 983*	*105 884 327*	*914 093*	*109 906 448*	*889 328*	*115 348 336*
dont paiements hors 3-D Secure avec authentification forte	*57 239*	*1 938 429*	*164 512*	*6 793 036*	*303 292*	*13 336 280*
dont paiements 3-D Secure sans authentification forte	*661 070*	*22 814 974*	*772 768*	*27 751 133*	*982 378*	*35 395 580*
dont paiements hors 3-D Secure sans authentification forte	*884 617*	*34 044 942*	*966 843*	*35 065 740*	*994 652*	*36 149 526*
dont paiements initiés par le commerçant (MIT)	*704 832*	*25 137 618*	*759 880*	*26 194 801*	*827 466*	*28 461 483*
dont paiements non 3-D Secure conformes à la DSP2	*92 513*	*4 489 918*	*99 678*	*3 999 029*	*74 078*	*3 485 859*
dont paiements non 3-D Secure non conformes à la DSP2	*87 272*	*4 417 407*	*107 284*	*4 871 909*	*93 108*	*4 202 183*
Retraits	**1 085 417**	**129 282 806**	**1 038 313**	**126 861 199**	**983 569**	**122 776 909**
Total	**19 001 146**	**849 760 091**	**19 944 705**	**874 450 644**	**20 924 041**	**897 342 272**

Note : MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T9 *bis* Paiements par carte émise en France et acceptée dans l'Espace économique européen – Transactions européennes

T9 *ter* Paiements par carte émise en France et acceptée à l'étranger hors Espace économique européen – Transactions internationales

T10 Transactions frauduleuses par carte émise et acceptée en France – Transactions nationales (tableau 1/2)

(volume en unités valeur en euros taux en pourcentage)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**793 350**	**36 280 495**	**0,009**	**825 325**	**43 515 617**	**0,009**	**989 454**	**53 593 598**	**0,010**
dont paiements sans contact (y compris paiements par mobile)	*522 873*	*10 502 092*	*0,013*	*576 537*	*14 002 613*	*0,012*	*754 985*	*20 231 615*	*0,014*
dont paiements par mobile	*29 807*	*2 447 707*	*0,091*	*75 039*	*4 801 997*	*0,065*	*152 726*	*9 566 583*	*0,056*
Paiements à distance (hors internet)	**74 832**	**8 964 315**	**0,165**	**77 941**	**10 604 251**	**0,191**	**120 708**	**24 857 056**	**0,187**
Paiements sur internet	**2 847 769**	**212 962 645**	**0,174**	**2 577 337**	**191 873 234**	**0,135**	**1 874 565**	**145 299 292**	**0,099**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*159 344*	*11 208 886*	*0,071*	*342 714*	*17 460 124*	*0,070*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*2 150 437*	*111 120 015*	*0,205*	*1 216 884*	*54 916 494*	*0,168*
Retraits	**102 962**	**32 477 429**	**0,029**	**121 642**	**41 437 842**	**0,035**	**115 643**	**41 344 934**	**0,032**
Total	**3 818 913**	**290 684 884**	**0,044**	**3 602 245**	**287 430 944**	**0,040**	**3 100 370**	**265 094 880**	**0,033**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T10 Transactions frauduleuses par carte émise et acceptée en France – Transactions nationales (tableau 2/2)

(volume en unités valeur en euros taux en pourcentage)

	2023			2024			2025		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**885 533**	**50 277 021**	**0,009**	**844 968**	**48 790 727**	**0,009**	**748 556**	**44 344 704**	**0,008**
dont paiements sans contact (y compris paiements par mobile)	*684 776*	*15 698 156*	*0,010*	*677 978*	*16 717 451*	*0,009*	*618 301*	*15 217 597*	*0,007*
dont paiements par mobile	*98 610*	*6 066 551*	*0,018*	*106 442*	*6 777 574*	*0,013*	*93 693*	*5 107 767*	*0,007*
Paiements à distance (hors internet)	**118 903**	**22 602 626**	**0,185**	**108 914**	**21 901 906**	**0,194**	**89 281**	**19 044 981**	**0,202**
Paiements sur internet	**1 913 224**	**152 815 486**	**0,093**	**1 699 339**	**141 354 049**	**0,079**	**1 432 194**	**132 543 339**	**0,066**
dont paiements 3-D Secure avec authentification forte	*314 857*	*72 017 359*	*0,068*	*243 803*	*64 612 099*	*0,059*	*236 171*	*67 457 901*	*0,058*
dont paiements hors 3-D Secure avec authentification forte	*36 576*	*2 353 042*	*0,121*	*29 664*	*2 723 581*	*0,040*	*48 018*	*6 949 937*	*0,052*
dont paiements 3-D Secure sans authentification forte	*258 701*	*12 634 204*	*0,055*	*269 807*	*11 345 394*	*0,041*	*259 679*	*11 515 059*	*0,033*
dont paiements hors 3-D Secure sans authentification forte	*1 303 090*	*65 810 881*	*0,193*	*1 156 065*	*62 672 975*	*0,179*	*888 326*	*46 620 442*	*0,129*
dont paiements initiés par le commerçant (MIT)	*1 044 582*	*49 260 633*	*0,196*	*911 249*	*46 970 926*	*0,179*	*714 965*	*34 919 958*	*0,123*
dont paiements non 3-D Secure conformes à la DSP2	*70 590*	*4 496 448*	*0,100*	*82 822*	*4 288 248*	*0,107*	*28 066*	*2 420 331*	*0,069*
dont paiements non 3-D Secure non conformes à la DSP2	*187 918*	*12 053 800*	*0,273*	*161 994*	*11 413 801*	*0,234*	*145 295*	*9 280 153*	*0,221*
Retraits	**102 357**	**38 832 083**	**0,030**	**97 042**	**38 795 063**	**0,031**	**92 850**	**40 110 780**	**0,033**
Total	**3 020 017**	**264 527 216**	**0,031**	**2 750 263**	**250 841 745**	**0,029**	**2 362 881**	**236 043 804**	**0,026**

Note : MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T10 *bis* Transactions frauduleuses par carte émise en France et acceptée dans l'Espace économique européen – Transactions européennes

T10 *ter* Transactions frauduleuses par carte émise en France et acceptée à l'étranger hors Espace économique européen – Transactions internationales

T11 Ventilation de la fraude à distance par secteur d'activité sur les transactions nationales en 2025

(volume en unités, valeur en euros, taux en volume pour mille, taux en valeur en pourcentage)

	Transactions		Fraude		Taux de fraude	
	Volume	Valeur	Volume	Valeur	Volume (‰)	Valeur (%)
Commerce généraliste et semi-généraliste	890 614 306	50 204 085 569	288 191	23 336 984	0,324	0,046
Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager, etc.)	176 715 601	7 904 517 883	215 410	12 327 203	1,219	0,156
Voyage, transport	392 740 769	33 835 937 783	85 320	20 031 413	0,217	0,059
Téléphonie et communication	423 186 689	15 411 957 300	200 685	14 325 271	0,474	0,093
Alimentation	39 744 767	2 971 229 669	17 191	1 206 448	0,433	0,041
Équipement de la maison, ameublement, bricolage	156 738 154	14 562 703 883	59 796	12 726 272	0,382	0,087
Assurance	15 154 665	3 038 431 148	6 358	1 053 896	0,420	0,035
Santé, beauté, hygiène	60 441 163	3 674 429 166	20 104	1 680 429	0,333	0,046
Services aux particuliers et aux professionnels	529 838 495	41 880 333 545	424 070	33 479 061	0,800	0,080
Approvisionnement d'un compte, vente de particulier à particulier	193 765 707	18 544 507 725	102 858	21 222 733	0,531	0,114
Jeux en ligne	191 745 386	5 459 364 032	72 708	5 235 483	0,379	0,096
Divers	170 905 667	12 167 475 153	28 784	4 963 127	0,168	0,041
Total	**3 241 591 369**	**209 654 972 856**	**1 521 475**	**151 588 320**	**0,469**	**0,072**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France (tableau 1/2)

(volume en milliers, montant en milliers d'euros)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**11 284 433**	**428 180 387**	**13 031 098**	**480 804 099**	**15 093 611**	**551 753 133**
dont paiements sans contact (y compris paiements par mobile)	*5 187 488*	*79 877 184*	*7 437 197*	*125 344 168*	*9 248 429*	*149 971 446*
dont paiements par mobile	*145 527*	*2 979 437*	*388 175*	*8 403 747*	*897 307*	*19 846 999*
Paiements à distance (hors internet)	**69 950**	**7 087 913**	**64 620**	**7 272 724**	**107 228**	**18 523 094**
Paiements sur internet	**2 158 226**	**132 554 575**	**2 565 276**	**155 816 405**	**2 589 260**	**166 197 062**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*409 008*	*18 152 505*	*748 083*	*27 403 752*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*1 448 074*	*59 013 071*	*969 216*	*38 855 848*
Retraits	**1 062 376**	**116 986 747**	**1 083 643**	**125 105 264**	**1 134 543**	**134 637 455**
Total	**14 574 985**	**684 809 622**	**16 744 636**	**768 998 491**	**18 924 643**	**871 110 743**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France (tableau 2/2)

(volume en milliers, montant en milliers d'euros)

	2023		2024		2025	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**16 159 605**	**588 228 633**	**17 012 900**	**604 734 154**	**17 934 022**	**618 572 967**
dont paiements sans contact (y compris paiements par mobile)	*10 982 717*	*178 132 864*	*11 665 395*	*208 538 219*	*12 986 634*	*245 328 249*
dont paiements par mobile	*1 716 563*	*39 282 385*	*2 640 235*	*61 840 034*	*3 684 780*	*83 841 621*
Paiements à distance (hors internet)	**105 756**	**18 799 343**	**106 130**	**18 397 062**	**97 812**	**16 895 103**
Paiements sur internet	**2 821 038**	**190 607 365**	**3 094 197**	**209 322 255**	**3 563 590**	**237 151 847**
dont paiements 3-D Secure avec authentification forte	*1 049 797*	*120 158 448*	*983 884*	*125 202 674*	*972 841*	*133 016 718*
dont paiements hors 3-D Secure avec authentification forte	*86 343*	*3 228 632*	*207 164*	*8 955 485*	*393 022*	*17 453 664*
dont paiements 3-D Secure sans authentification forte	*707 064*	*26 605 058*	*824 916*	*32 032 197*	*1 049 621*	*40 562 592*
dont paiements hors 3-D Secure sans authentification forte	*977 834*	*40 615 228*	*1 078 232*	*43 131 899*	*1 148 106*	*46 118 873*
dont paiements initiés par le commerçant (MIT)	*730 327*	*26 600 426*	*799 769*	*28 458 565*	*898 553*	*32 015 933*
dont paiements « one-leg »	*13 616*	*1 740 365*	*18 288*	*2 203 444*	*19 457*	*2 192 974*
dont paiements non 3-D Secure conformes à la DSP2	*101 735*	*5 110 587*	*108 921*	*4 820 779*	*82 627*	*4 451 790*
dont paiements non 3-D Secure non conformes à la DSP2	*132 156*	*7 163 850*	*151 255*	*7 649 111*	*147 468*	*7 458 176*
Retraits	**1 117 986**	**135 559 666**	**1 069 029**	**133 303 352**	**1 016 045**	**129 310 462**
Total	**20 204 386**	**933 195 008**	**21 282 255**	**965 756 822**	**22 611 470**	**1 001 930 379**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T12 *bis* Paiements par carte émise dans l'Espace économique européen et acceptée en France – Transactions européennes

T12 *ter* Paiements par carte émise à l'étranger hors Espace économique européen et acceptée en France – Transactions internationales

T13 Transactions frauduleuses par carte acceptée en France (tableau 1/2)

(volume en unités, valeur en euros, taux en pourcentage)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**841 280**	**42 883 367**	**0,0100**	**874 166**	**49 441 754**	**0,0103**	**1 084 701**	**67 409 965**	**0,0122**
dont paiements sans contact (y compris paiements par mobile)	*538 313*	*12 238 895*	*0,0153*	*601 803*	*15 600 613*	*0,0124*	*819 535*	*24 406 015*	*0,0163*
dont paiements par mobile	*35 968*	*3 640 684*	*0,1222*	*84 421*	*5 793 427*	*0,0689*	*170 752*	*12 007 511*	*0,0605*
Paiements à distance (hors internet)	**105 972**	**17 644 315**	**0,2489**	**96 257**	**15 211 163**	**0,2092**	**144 965**	**35 446 137**	**0,1914**
Paiements sur internet	**3 176 400**	**248 966 265**	**0,1878**	**2 885 920**	**227 162 875**	**0,1458**	**2 252 283**	**190 461 573**	**0,1146**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*213 403*	*20 406 481*	*0,1124*	*405 445*	*26 105 266*	*0,0953*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*2 366 252*	*129 864 761*	*0,2201*	*1 500 472*	*83 396 334*	*0,2146*
Retraits	**104 960**	**33 084 175**	**0,0283**	**124,077**	**42,256,276**	**0,0338**	**120 217**	**42 811 637**	**0,0318**
Total	**4 228 612**	**342 578 122**	**0,0500**	**3,980,420**	**334,072,068**	**0,0434**	**3 602 166**	**336 129 312**	**0,0386**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T13 Transactions frauduleuses par carte acceptée en France (tableau 2/2)

(volume en unités, valeur en euros, taux en pourcentage)

	2023			2024			2025		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**999 344**	**67 688 751**	**0,0115**	**936 045**	**60 720 918**	**0,0100**	**861 804**	**56 524 793**	**0,0091**
dont paiements sans contact (y compris paiements par mobile)	*769 979*	*21 899 061*	*0,0123*	*750 184*	*21 346 502*	*0,0102*	*711 941*	*20 206 590*	*0,0082*
dont paiements par mobile	*127 622*	*10 042 616*	*0,0256*	*132 824*	*9 630 052*	*0,0156*	*128 315*	*7 776 387*	*0,0093*
Paiements à distance (hors internet)	**142 763**	**32 984 939**	**0,1755**	**142 032**	**33 542 430**	**0,1823**	**116 859**	**28 452 214**	**0,1684**
Paiements sur internet	**2 337 170**	**201 724 304**	**0,1058**	**2 244 878**	**204 136 996**	**0,0975**	**2 005 651**	**194 384 588**	**0,0820**
dont paiements 3-D Secure avec authentification forte	354 651	83 805 192	0,0697	267 924	73 737 188	0,0589	269 865	80 429 433	0,0605
dont paiements hors 3-D Secure avec authentification forte	*71 563*	*5 522 986*	*0,1711*	*44 498*	*4 443 794*	*0,0496*	*72 981*	*9 723 224*	*0,0557*
dont paiements 3-D Secure sans authentification forte	*342 878*	*20 687 862*	*0,0778*	*402 394*	*20 996 741*	*0,0655*	*343 037*	*20 157 257*	*0,0497*
dont paiements hors 3-D Secure sans authentification forte	*1 568 078*	*91 708 264*	*0,2258*	*1 530 062*	*104 959 273*	*0,2433*	*1 319 768*	*84 074 674*	*0,1823*
dont paiements initiés par le commerçant (MIT)	*1 098 829*	*52 343 346*	*0,1968*	*1 013 164*	*53 073 094*	*0,1865*	*879 269*	*45 602 606*	*0,1424*
dont paiements « one-leg »	*92 524*	*12 994 451*	*0,7467*	*134 338*	*20 595 974*	*0,9347*	*144 683*	*16 402 821*	*0,7480*
dont paiements non 3-D Secure conformes à la DSP2	*80 195*	*5 068 095*	*0,0992*	*93 256*	*4 905 339*	*0,1018*	*38 299*	*2 993 040*	*0,0672*
dont paiements non 3-D Secure non conformes à la DSP2	*296 530*	*21 302 372*	*0,2974*	*289 304*	*26 384 866*	*0,3449*	*257 517*	*19 076 207*	*0,2558*
Retraits	**106 749**	**40 292 502**	**0,0297**	**100 323**	**40 070 346**	**0,0301**	**97 273**	**41 655 728**	**0,0322**
Total	**3 586 026**	**342 690 496**	**0,0367**	**3 423 278**	**338 470 690**	**0,0350**	**3 081 587**	**321 017 323**	**0,0320**

Note : *One-leg* signifie que l'émetteur de la carte est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

Transactions frauduleuses par carte émise et acceptée en France – Transactions nationales (cf. T10)

T13 *bis* Transactions frauduleuses par carte émise dans l'Espace économique européen et acceptée en France – Transactions européennes

T13 *ter* Transactions frauduleuses par carte émise à l'étranger hors Espace économique européen et acceptée en France – Transactions internationales

T13 *quater* Répartition de la fraude sur les paiements par carte acceptée en France en 2025

T13 *quinquies* Répartition géographique de la fraude sur les cartes acceptées en France en 2025

CHÈQUE

T14 Chèques échangés

(volume en millions, montant en milliards d'euros, montant moyen en euros)

	2020	2021	2022	2023	2024	2025
Volume	1 175,5	1 105,8	1 008,0	891,5	783,8	673,8
Montant	614,2	588,6	539,8	467,3	392,2	330,6
Montant moyen	**522,5**	**532,3**	**535,5**	**524,1**	**500,4**	**490,7**

Source : Observatoire de la sécurité des moyens de paiement.

T14 *bis* Volume de chèques échangés en détail

T15 Fraude au chèque

(volume en unités, valeur et montant moyen en euros, taux en volume pour mille, taux en valeur en pourcentage)

a) Ancienne approche

	2020	2021	2022	2023	2024	2025
Volume	**220 685**	**272 970**	**266 216**	**255 857**	**223 309**	**198 019**
Taux de fraude (‰)	0,188	0,247	0,264	0,287	0,285	0,294
Valeur	**538 059 139**	**625 703 442**	**556 796 815**	**588 194 101**	**467 435 789**	**387 099 403**
Taux de fraude (%)	0,088	0,106	0,103	0,126	0,119	0,117
Montant moyen	**2 438**	**2 292**	**2 092**	**2 299**	**2 093**	**1 955**

b) Nouvelle approche

	2020	2021	2022	2023	2024	2025
Volume	**190 001**	**232 277**	**218 122**	**206 197**	**180 059**	**158 405**
Taux de fraude (‰)	0,162	0,210	0,216	0,231	0,230	0,235
Valeur	**401 611 189**	**465 021 167**	**395 416 196**	**363 929 512**	**272 398 979**	**228 944 293**
Taux de fraude (%)	0,065	0,079	0,073	0,078	0,069	0,069
Montant moyen	**2 114**	**2 002**	**1 813**	**1 765**	**1 513**	**1 445**

Note : L'ancienne approche tient compte de toute opération par chèque réglée et rejetée pour un motif de fraude. La nouvelle approche de fraude au chèque exclut les fraudes qui sont déjouées après la remise et le règlement du chèque.

Source : Observatoire de la sécurité des moyens de paiement.

T16 Typologie de la fraude au chèque

(volume en unités, valeur en euros, part en pourcentage)

a) Ancienne approche

	2020		2021		2022		2023		2024		2025	
	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part
Volume												
Vol, perte	196 754	89,2	244 750	89,7	237 854	89,3	225 859	88,3	199 649	89,4	177 587	89,7
Falsification	13 894	6,3	18 074	6,6	18 885	7,1	20 583	8,0	14 476	6,5	12 572	6,3
Contrefaçon	7 207	3,3	5 119	1,9	5 969	2,2	5 720	2,2	6 314	2,8	5 400	2,7
Détournement, rejeu	2 830	1,3	5 026	1,8	3 508	1,3	3 695	1,4	2 870	1,3	2 460	1,2
Valeur												
Vol, perte	365 813 764	68,0	398 739 224	63,7	375 576 575	67,5	385 379 003	65,5	292 099 360	62,5	239 393 599	61,8
Falsification	102 801 337	19,1	100 395 756	16,0	93 152 894	16,7	103 932 879	17,7	90 450 964	19,4	72 045 420	18,6
Contrefaçon	32 340 420	6,0	33 725 041	5,4	32 648 566	5,9	29 927 137	5,1	44 888 178	9,6	42 009 290	10,9
Détournement, rejeu	37 103 618	6,9	92 823 421	14,8	55 418 781	10,0	68 955 081	11,7	39 997 287	8,6	33 651 094	8,7

b) Nouvelle approche

	2025	
	Nombre/ montant	Part
Volume		
Vol, perte	142 683	90,1
Falsification	9 677	6,1
Contrefaçon	4 396	2,8
Détournement, rejeu	1 649	1,0
Valeur		
Vol, perte	142 973 133	62,4
Falsification	45 540 584	19,9
Contrefaçon	21 357 952	9,3
Détournement, rejeu	19 072 625	8,3

Note : L'ancienne approche tient compte de toute opération par chèque réglée et rejetée pour un motif de fraude. À partir de 2025, la ventilation par typologie est également disponible pour la nouvelle approche de la fraude au chèque qui exclut les fraudes qui sont déjouées après la remise et le règlement du chèque.

Source : Observatoire de la sécurité des moyens de paiement.

T17 Virements émis par type de virement
(volume en millions, montant en millions d'euros)

	2020		2021		2022		2023		2024		2025	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4 483**	**32 713 128**	**4 843**	**38 722 734**	**5 158**	**38 894 879**	**5 613**	**29 942 161**	**5 975**	**31 056 841**	**6 362**	**32 415 942**
dont virements SEPA – SCT	*4 384*	*10 029 108*	*4 668*	*12 980 883*	*4 689*	*9 655 892*	*4 867*	*9 823 091*	*5 026*	*10 477 482*	*4 939*	*11 162 129*
dont virements SEPA instantanés – SCT Inst	*45*	*26 243*	*107*	*50 053*	*198*	*118 972*	*408*	*177 099*	*598*	*231 175*	*1 066*	*504 742*
dont virements de gros montants – VGM [a]	*9*	*19 042 030*	*9*	*19 661 685*	*19*	*15 907 892*	*30*	*8 533 346*	*11*	*10 360 358*	*10*	*11 066 318*
dont autres virements	*45*	*3 615 748*	*59*	*6 030 114*	*252*	*13 212 124*	*309*	*11 408 625*	*341*	*9 987 826*	*346*	*9 682 753*
Total – hors VGM	**4 474**	**13 671 098**	**4 834**	**19 061 050**	**5 138**	**22 986 988**	**5 583**	**21 408 815**	**5 964**	**20 696 483**	**6 352**	**21 349 624**

a) Il s'agit des virements de gros montant effectués via Target2 ou Euro1.
Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer* ; VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

T17 *bis* Virements émis par canal d'initiation

T17 *ter* Virements émis par destination géographique

T18 Transactions frauduleuses par type de virement (tableau 1/2)
(volume en unités, valeur en euros, taux en pourcentage)

	2020			2021			2022		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**35 893**	**266 969 099**	**0,0008**	**46 718**	**287 264 068**	**0,0007**	**76 846**	**313 163 442**	**0,0008**
dont virements SEPA – SCT	*25 254*	*191 474 396*	*0,0019*	*33 199*	*246 527 533*	*0,0019*	*40 874*	*205 737 587*	*0,0021*
dont virements SEPA instantanés – SCT Inst	*7 131*	*10 562 419*	*0,0402*	*12 913*	*22 406 942*	*0,0448*	*33 193*	*52 768 218*	*0,0444*
dont virements de gros montants – VGM [a]	*51*	*2 439 224*	*0,0000*	*5*	*1 539 120*	*0,0000*	*49*	*1 934 774*	*0,0000*
dont autres virements	*3 457*	*62 493 060*	*0,0017*	*601*	*16 790 473*	*0,0003*	*2 730*	*52 722 863*	*0,0004*
Total – hors VGM	**35 842**	**264 529 875**	**0,0019**	**46 713**	**285 724 948**	**0,0015**	**76 797**	**311 228 668**	**0,0014**

a) Il s'agit des virements de gros montant effectués via Target2 ou Euro1.
Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer* ; VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

T18 Transactions frauduleuses par type de virement (tableau 2/2)

(volume en unités, valeur en euros, taux en pourcentage)

	2023			2024			2025		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**90 453**	**312 487 450**	**0,0010**	**130 092**	**354 549 264**	**0,0011**	**290 495**	**484 652 054**	**0,0015**
dont virements SEPA – SCT	*38 591*	*202 417 172*	*0,0021*	*41 546*	*200 861 356*	*0,0019*	*86 570*	*221 429 149*	*0,0020*
dont virements SEPA instantanés – SCT Inst	*48 630*	*69 003 730*	*0,0390*	*78 316*	*107 400 214*	*0,0465*	*182 568*	*205 871 733*	*0,0408*
dont virements de gros montants – VGM [a]	*32*	*9 828 077*	*0,0001*	*20*	*3 496 816*	*0,0000*	*53*	*1 733 738*	*0,0000*
dont autres virements	*3 200*	*31 238 471*	*0,0003*	*10 210*	*42 790 878*	*0,0004*	*21 304*	*55 617 435*	*0,0006*
Total – hors VGM	**90 421**	**302 659 373**	**0,0014**	**130 072**	**351 052 448**	**0,0017**	**290 442**	**482 918 316**	**0,0023**

a) Il s'agit des virements de gros montant effectués via Target2 ou Euro1.

Note : SEPA, *Single Euro Payment Area*, espace unique de paiement en euros ; SCT Inst, SEPA *Instant Credit Transfer* ; VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

T18 *bis* Transactions frauduleuses par canal d'initiation du virement

T18 *ter* Transactions frauduleuses par destination géographique du virement

T19 Total de la fraude sur le virement

(volume en unités, valeur et montant moyen en euros, taux en volume pour mille, taux en valeur en pourcentage)

	2020	2021	2022	2023	2024	2025
Volume	**35 893**	**46 718**	**76 846**	**90 453**	**130 092**	**290 495**
Taux (‰)	0,0080	0,0096	0,0149	0,0161	0,0218	0,0457
Valeur	**266 969 099**	**287 264 068**	**313 163 442**	**312 487 450**	**354 549 264**	**484 652 054**
Taux (%)	0,0008	0,0007	0,0008	0,0010	0,0011	0,0015
Montant moyen	**7 438**	**6 149**	**4 075**	**3 455**	**2 725**	**1 668**

Source : Observatoire de la sécurité des moyens de paiement.

T20 Fraude sur le virement par typologie

(volume en unités, valeur en euros, part en pourcentage)

	2020		2021		2022		2023		2024		2025	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**28 211**	**87 061 255**	**35 865**	**87 370 131**	**57 443**	**120 006 990**	**63 471**	**134 097 939**	**72 550**	**138 020 994**	**80 550**	**129 973 000**
Part	78,6	32,6	76,8	30,4	74,8	38,3	70,2	42,9	55,8	38,9	27,7	26,8
Falsification	**203**	**3 377 807**	**875**	**5 387 862**	**179**	**2 838 371**	**269**	**2 293 923**	**410**	**3 523 179**	**1 362**	**13 568 743**
Part	0,6	1,3	1,9	1,9	0,2	0,9	0,3	0,7	0,3	1,0	0,5	2,8
Détournement	**5 731**	**157 318 883**	**8 523**	**168 094 274**	**16 991**	**148 732 203**	**25 071**	**152 081 946**	**54 951**	**183 912 411**	**206 412**	**297 102 941**
Part	16,0	58,9	18,2	58,5	22,1	47,5	27,7	48,7	42,2	51,9	71,1	61,3
Autres	**1 748**	**19 211 154**	**1 455**	**26 411 801**	**2 233**	**41 585 878**	**1 642**	**24 013 643**	**2 181**	**29 092 681**	**2 171**	**44 007 370**
Part	4,9	7,2	3,1	9,2	2,9	13,3	1,8	7,7	1,7	8,2	0,7	9,1

Source : Observatoire de la sécurité des moyens de paiement.

T21 Prélèvements émis par type de mandat
(volume en millions, montant en millions d'euros)

	2020		2021		2022		2023		2024		2025	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4 622**	**1 684 258**	**5 020**	**1 895 098**	**4 914**	**2 040 963**	**4 616**	**2 138 539**	**4 788**	**2 178 418**	**5 040**	**2 299 878**
Prélèvements par type de mandat												
dont prélèvements consentis par mandat électronique	nd	nd	1 106	430 781	1 357	1 045 754	1 254	1 021 429	1 228	1 026 731	1 276	1 076 635
dont prélèvements consentis par mandat papier	nd	nd	3 914	1 464 317	3 558	995 210	3 362	1 117 110	3 560	1 151 687	3 764	1 223 243
Prélèvements par mode d'initiation												
dont prélèvements initiés dans un fichier/lot	4 560	1 647 504	4 936	1 819 420	4 645	1 929 438	4 242	2 009 917	4 479	2 064 469	4 765	2 185 118
dont prélèvements initiés sur la base d'un paiement unique	61	36 754	84	75 678	269	111 525	374	128 622	310	113 948	275	114 760

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T21 *bis* Prélèvements émis par origine géographique du payeur

T22 Fraude sur le prélèvement
(volume en unités, valeur et montant moyen en euros, taux en volume pour mille, taux en valeur en pourcentage)

	2020	2021	2022	2023	2024	2025
Volume	**6 485**	**251 010**	**49 453**	**77 876**	**52 799**	**56 263**
Taux de fraude (‰)	0,0014	0,0500	0,0101	0,0169	0,0110	0,0112
Valeur	**1 891 051**	**25 318 677**	**19 853 012**	**22 320 813**	**30 416 859**	**33 254 401**
Taux de fraude (%)	0,0001	0,0013	0,0010	0,0010	0,0014	0,0014
Montant moyen	**292**	**101**	**401**	**287**	**576**	**591**

Source : Observatoire de la sécurité des moyens de paiement.

T22 *bis* Prélèvements frauduleux par origine géographique du payeur

T22 *ter* Prélèvements frauduleux par type de mandat

T23 Typologie de la fraude au prélèvement
(volume en unités, valeur en euros, part en pourcentage)

	2020		2021		2022		2023		2024		2025	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**6 011**	**1 388 326**	**250 493**	**25 201 709**	**43 788**	**14 206 533**	**70 212**	**22 003 546**	**27 550**	**29 252 682**	**51 063**	**26 063 586**
Part	92,7	73,4	99,8	99,5	88,5	71,6	90,2	98,6	52,2	96,2	90,8	78,4
Détournement	**62**	**10 720**	**517**	**116 968**	**5 665**	**5 646 479**	**7 664**	**317 267**	**25 249**	**1 164 176**	**5 200**	**7 190 815**
Part	1,0	0,6	0,2	0,5	11,5	28,4	9,8	1,4	47,8	3,8	9,2	21,6

Note : Jusqu'en 2020, la fraude au prélèvement contenait deux autres typologies, « Falsifications » et « Autres », ce qui explique que la ventilation ne représente pas toujours 100 % de la fraude.

Source : Observatoire de la sécurité des moyens de paiement.

AUTRES

Monnaie électronique

T24 Nombre de supports par des prestataires agréés ou établis en France

T25 Usage de la monnaie électronique par typologie de transaction

T26 Transactions frauduleuses par monnaie électronique

Effets de commerce : lettre de change relevé (LCR) et billet à ordre (BOR)

T27 Paiements par effet de commerce

T28 Typologie de la fraude aux effets de commerce

Transmission de fonds

T29 Opérations par transmission de fonds

T30 Opérations frauduleuses par transmission de fonds

Service d'initiation de paiement

T31 Opérations initiées par l'établissement en qualité de prestataire de services d'initiation de paiement (service 7 de l'article 314-1 du Code monétaire et financier)

T32 Transactions frauduleuses initiées via un établissement agissant en qualité de prestataire de services d'initiation de paiement (service 7 de l'article 314-1 du Code monétaire et financier)

Éditeur
Banque de France

Directeur de la publication
Erick Lacourrège
Directeur général des Moyens de paiement
Banque de France

Rédacteur en chef
Julien Lasalle
Adjoint au directeur des études et de la surveillance des paiements
Banque de France

Secrétariat de rédaction
Aurélie Barberet, Pierre Bienvenu, Clément Bourgeois, Véronique Bugaj, Alexandre Capony, Julien Cisamolo, Caroline Corcy, Anne-Marie Fourel, Trân Huynh, Fatih Kurt, Isabelle Maranghi, Adrien Mocek, Ségolène Mure, Cyril Ronfort, Marine Soubielle, Valérie Tallarita, Armand Thomas

Réalisation
SGS & Co
et Studio Création
Direction de la Communication

Contact
Observatoire de la sécurité des moyens de paiement
Code courrier : S2B-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Impression
Navis
Imprimé en France

Dépôt légal
Septembre 2026
ISSN 2557-1230 (en ligne)
ISSN 2556-4536 (imprimé)

Internet
www.observatoire-paiements.fr

Le *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement* est en libre téléchargement sur le site internet de la Banque de France (*www.banque-france.fr*).

BANQUE DE FRANCE

EUROSYSTÈME

www.banque-france.fr