OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2024

BANQUE DE FRANCE
EUROSYSTÈME

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2024

Adressé à
Monsieur le Ministre de l'Économie, des Finances
et de la Souveraineté industrielle 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 2025

SOMMAIRE

SYNTHÈSE 4

2024 EN CHIFFRES 6

CHAPITRE 1
ÉTAT DE LA FRAUDE EN 2024 9

1.1 Vue d'ensemble 10

1.2 État de la fraude sur la carte de paiement 12

1.3 État de la fraude sur le chèque 19

1.4 État de la fraude sur le virement 20

1.5 État de la fraude sur le prélèvement 21

1.6 État de la fraude par manipulation 22

CHAPITRE 2
BILAN DES RECOMMANDATIONS SUR LA PRÉVENTION ET LE REMBOURSEMENT DES OPÉRATIONS DE PAIEMENT FRAUDULEUSES 27

2.1 Contexte des travaux 27

2.2 Synthèse 27

2.3 Bilan de l'application des recommandations générales relatives au traitement des contestations d'opérations de paiement 28

2.4 Bilan des recommandations applicables au traitement de cas spécifiques 29

2.5 Bilan des recommandations à l'attention des consommateurs et de leurs représentants 32

2.6 Bilan des recommandations visant à prévenir la fraude 33

CHAPITRE 3
ACTIONS CONDUITES PAR L'OBSERVATOIRE AU TITRE DE LA PRÉVENTION DE LA FRAUDE 35

3.1 Prévention de la fraude sur les paiements par carte à distance 35

3.2 Sécurisation des communications et coopération avec les acteurs des télécommunications et du numérique 41

3.3 Utilisation de la carte de paiement pour l'accès aux sites pornographiques 46

3.4 Le suivi des actions et recommandations de l'Observatoire contre la fraude au chèque 49

3.5 Rappel des principales recommandations de l'Observatoire sur les sujets de veille technologique et sur les instruments SEPA 51

CHAPITRE 4
L'APPORT DE L'INTELLIGENCE ARTIFICIELLE (AI) DANS LA LUTTE CONTRE LA FRAUDE : ENJEUX ET PERSPECTIVES 59

4.1 Propos introductif 59

4.2 Les enjeux techniques relatifs à l'optimisation de la performance des modèles 60

4.3 Les enjeux métiers 67

4.4 Les enjeux de conformité 69

4.5 Recommandations 70

ANNEXES 73

A1 Conseils de prudence pour l'utilisation des moyens de paiement 75

A2 Missions et organisation de l'Observatoire 88

A3 Liste nominative des membres de l'Observatoire 90

A4 Méthodologie de mesure de la fraude aux moyens de paiement scripturaux 93

A5 Dossier statistique sur l'usage et la fraude aux moyens de paiement 103

SYNTHÈSE

L'adoption toujours croissante de moyens de paiement innovants, comme le virement instantané (10 % des virements émis) ou le paiement par mobile (15 % des paiements par carte au point de vente), a continué à porter le développement de l'usage des moyens de paiement scripturaux en 2024 : + 5,2 % en nombre d'opérations et + 3,4 % en montants échangés.

***Le chapitre 1 du présent rapport de l'Observatoire souligne que ce développement s'est accompagné d'une stabilité du montant annuel de fraude depuis 2022**, juste au-dessous du seuil de 1,2 milliard d'euros, avec une maîtrise satisfaisante du niveau de fraude sur les canaux de paiement les plus utilisés :*

- *La **carte**, qui est le principal moyen de paiement du quotidien, voit son taux de fraude se stabiliser à son plus bas niveau historique, pour la troisième année consécutive (53 euros de fraude pour 100 000 euros de paiements), avec en particulier la poursuite de l'amélioration du taux de fraude sur les paiements digitaux (mobile et e-commerce) ;*

- *Le **virement** reste associé à un taux de fraude globalement très faible (1 euro de fraude pour 100 000 euros de paiements en moyenne). Les usages du grand public demeurent structurellement plus exposés (43 euros pour 100 000 euros de paiements pour les virements émis depuis les espaces de banque en ligne) que ceux des entreprises et des administrations, mais les taux de fraude restent inférieurs à ceux de la carte, y compris pour les virements instantanés (46 euros pour 100 000 euros de paiements) ;*

- *Le **chèque** enregistre un recul de la fraude de plus de 25 % en montant, alors que son usage a diminué de 16 % en montant, ce qui réduit son taux de fraude à son plus bas niveau depuis 2021, à 69 euros pour 100 000 euros de paiements.*

*Après deux années de progression très significative entre 2021 et 2023, la part de la **fraude par manipulation** s'est stabilisée en 2024 à 32 % du montant total de la fraude, soit 382 millions d'euros[1].*

***Le chapitre 2 présente le bilan établi par l'Autorité de contrôle prudentiel et de résolution (ACPR) et la Banque de France concernant l'application des recommandations publiées en avril 2023 sur la prévention de la fraude et le remboursement des cas de fraude.** Ce bilan, étayé par des statistiques inédites, fait notamment état d'un renforcement général de la sécurité des parcours de paiement d'une part, et d'une amélioration des procédures de traitement des contestations afin de mieux tenir compte des différents paramètres techniques et contextuels d'autre part. Les autorités resteront toutefois attentives à la correction de certaines pratiques résiduelles, qui doivent se conformer à la réglementation ou mieux prendre en compte les recommandations.*

***Le chapitre 3 dresse un état des lieux des actions engagées par l'Observatoire en matière de prévention de la fraude**, qui recouvrent principalement :*

- *La conduite d'un plan d'action visant à sécuriser les paiements par carte à distance effectués hors protocole technique 3-D Secure, qui associe des mesures collectives contraignant le recours aux canaux les plus vulnérables et des mesures individuelles ciblant les commerçants les plus exposés à la fraude. Ce plan, qui a déjà contribué à l'amélioration du taux de fraude sur les paiements par carte sur internet en 2024, est appelé à se poursuivre en 2025 et 2026 ;*

- *Les actions conduites par le secteur des télécommunications pour prévenir les usurpations d'identité à travers leurs réseaux – avec en particulier le déploiement effectif fin 2024/début 2025 du mécanisme d'authentification des numéros (MAN) destiné à certifier le numéro présenté lors de la réception d'un appel téléphonique –, et la promotion des services de prévention des SMS frauduleux ;*

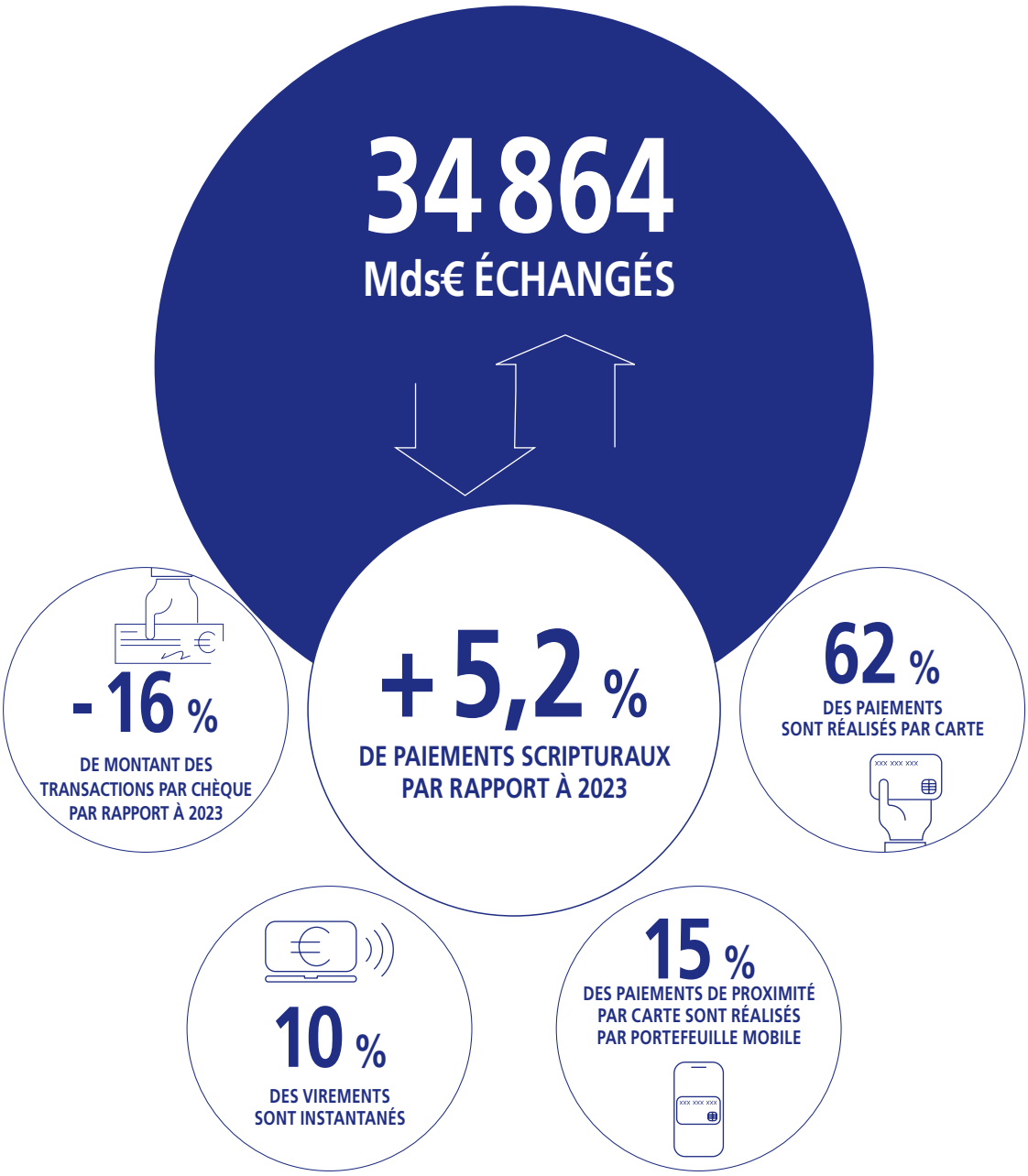
- *La précision de certaines recommandations de l'Observatoire pour renforcer la sécurité du chèque, surtout en ce qui concerne l'envoi des chéquiers par voie postale et la simplification des procédures de mise en opposition.*

Le chapitre 4 rend compte des travaux de veille de l'Observatoire sur l'utilisation des techniques d'intelligence artificielle et de* scoring *à des fins de lutte contre la fraude. *Il détaille notamment les conditions de succès de telles solutions pour les professionnels des paiements en matière de gestion des données et de pilotage.*

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 et ainsi offrir à tous les utilisateurs, particuliers comme entreprises, une authentique liberté de choix dans leurs usages au quotidien****. Dans son programme de travail pour 2025-2026, l'Observatoire orientera en particulier ses travaux de veille technologique sur la sécurité des paiements au moyen d'actifs numériques tels que les cryptoactifs, dont les* stablecoins*. Parallèlement, il poursuivra les actions de prévention de la fraude engagées en partenariat avec les acteurs du secteur des télécommunications et, dans une nouvelle perspective compte tenu de leur importance, avec les acteurs du numérique.*

1 La fraude par manipulation, telle que mesurée par l'Observatoire, couvre uniquement les escroqueries par détournement du moyen de paiement. Pour l'essentiel, ce sont les cas où le fraudeur manipule le client 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 antifraude). L'Observatoire mesure l'ampleur de cette fraude indirectement (au travers d'un *proxy*) par la somme des opérations frauduleuses par carte avec authentification forte et par virement de banque en ligne. En revanche, les escroqueries pour lesquelles la victime a autorisé un paiement à destination d'un escroc (cas de la fraude à la romance, de faux sites de e-commerce, d'une souscription d'un faux produit d'investissement ou d'un faux crédit, etc.) sont exclues du périmètre statistique de l'Observatoire.

L'USAGE DES MOYENS DE PAIEMENT EN 2024



L'ÉVOLUTION DE LA FRAUDE EN 2024

0,053 %
STABILISATION DU TAUX DE FRAUDE SUR LA CARTE À SON PLUS BAS NIVEAU HISTORIQUE

-74 %
DE TAUX DE FRAUDE POUR LES PAIEMENTS DE PROXIMITÉ PAR CARTE RÉALISÉS PAR PORTEFEUILLE MOBILE DEPUIS 2022

-94 M€
DE TRANSACTIONS FRAUDULEUSES SUR LE CHÈQUE

1,189
Md€ DE PRÉJUDICE

-0,6 %
DE FRAUDE EN VALEUR

0,046 %
DE TAUX DE FRAUDE SUR LES VIREMENTS INSTANTANÉS

382 M€
DE FRAUDE PAR MANIPULATION

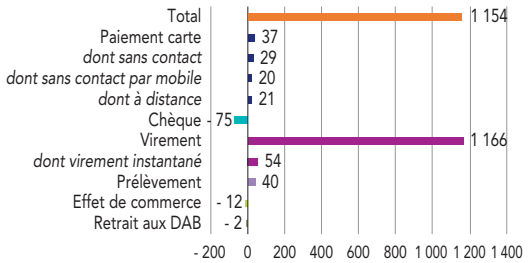
1

ÉTAT DE LA FRAUDE EN 2024

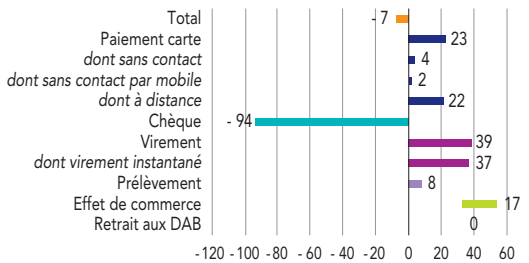
Données clés

G1 Évolution des moyens de paiement entre 2023 et 2024

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



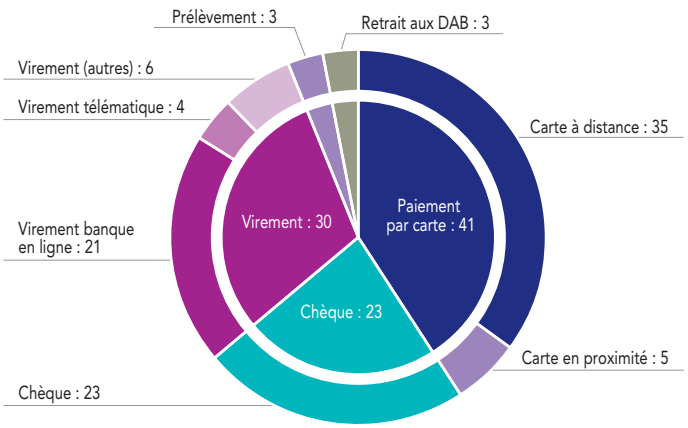
b) Fraude (en millions d'euros)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

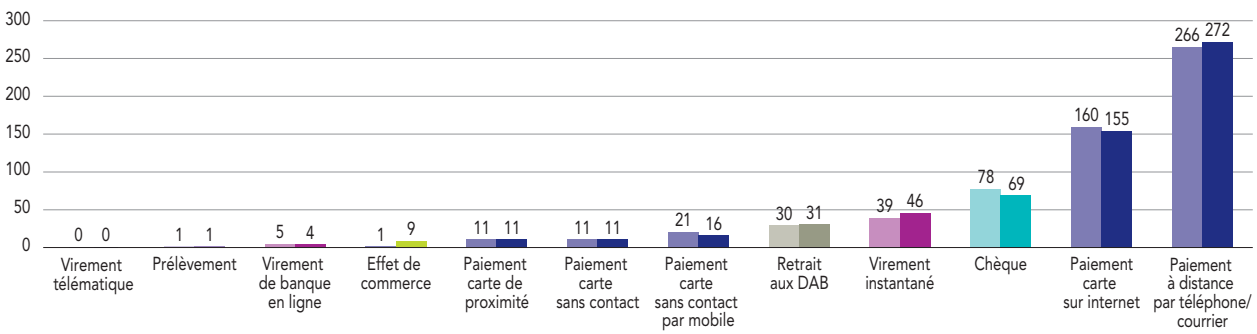
G2 Les principales sources de fraude en valeur (en %)



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 2023 et 2024 (en euros de fraude pour 100 000 euros de paiement)



Note : DAB, distributeurs automatiques de billets.

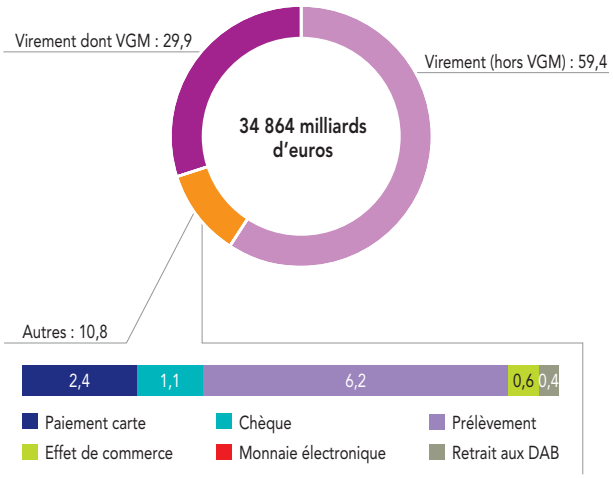
Source : Observatoire de la sécurité des moyens de paiement.

1.1 Vue d'ensemble

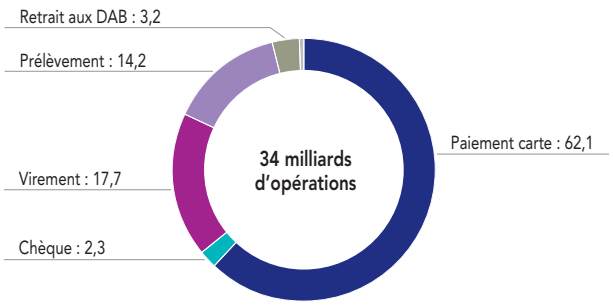
1.1.1 Cartographie des moyens de paiement

G4 Usage des moyens de paiement scripturaux en 2024 (en %)

a) En montant



b) En volume



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 33,8 milliards de transactions en 2024 (+ 5,2 % par rapport à 2023), pour un total de 34 864 milliards d'euros (+ 3,4 % par rapport à 2023).

Tandis que les usages innovants affichent des taux de croissance élevés, l'usage du chèque poursuit sa baisse : – 16 % en montant, et ne représente plus que 2,3 % des transactions scripturales en volume.

Les virements restent prépondérants dans le total des flux en montant, avec une part stable à 89 %. Les virements de gros montant (VGM) atteignent 30 % des montants échangés par virement, pour seulement 0,03 % des volumes. Le virement instantané poursuit son essor (+ 46 % en volume et + 31 % en montant) et représente désormais 10 % des virements en volume (contre 7,3 % en 2023).

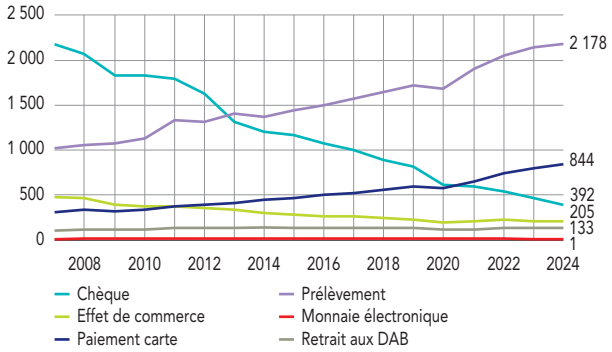
La carte bancaire reste le moyen de paiement scriptural privilégié des Français et son usage continue de progresser. Sa part, hors retraits, dans les volumes de transactions passe de 61,4 % en 2023 à 62,1 % en 2024. Alors que la croissance des flux en volume du paiement sans contact ralentit (+ 6 % par rapport à 2023, contre + 19 % entre 2022 et 2023), le paiement par mobile poursuit sa forte progression (+ 54 % en volume par rapport à 2023). Ainsi, le paiement par mobile représente en 2024 près de 15 % des paiements par carte de proximité, contre 10 % en 2023.

Après des années de stabilité, l'année 2024 enregistre une légère baisse des retraits d'espèces par carte (– 4,2 % en volume et – 1,6 % en montant).

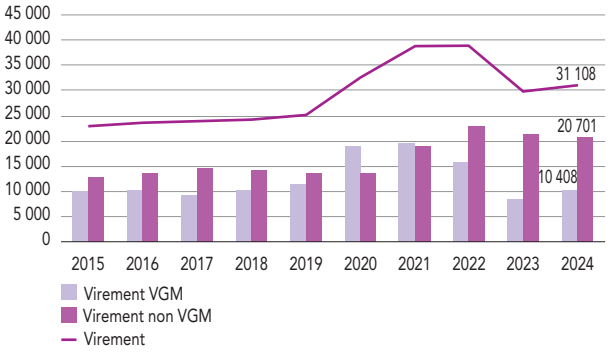
Le prélèvement suit la tendance générale observée sur l'ensemble des moyens de paiement : + 3,7 % en volume et + 1,9 % en montant par rapport à 2023.

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

a) Par instrument (hors virement)



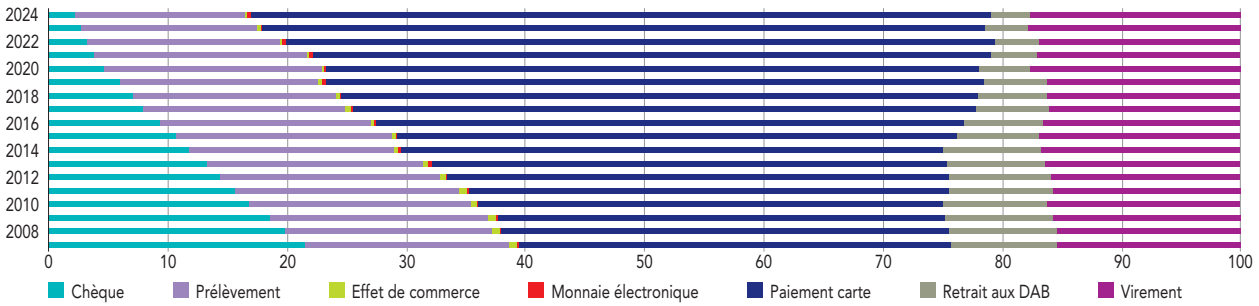
b) Par virement



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.

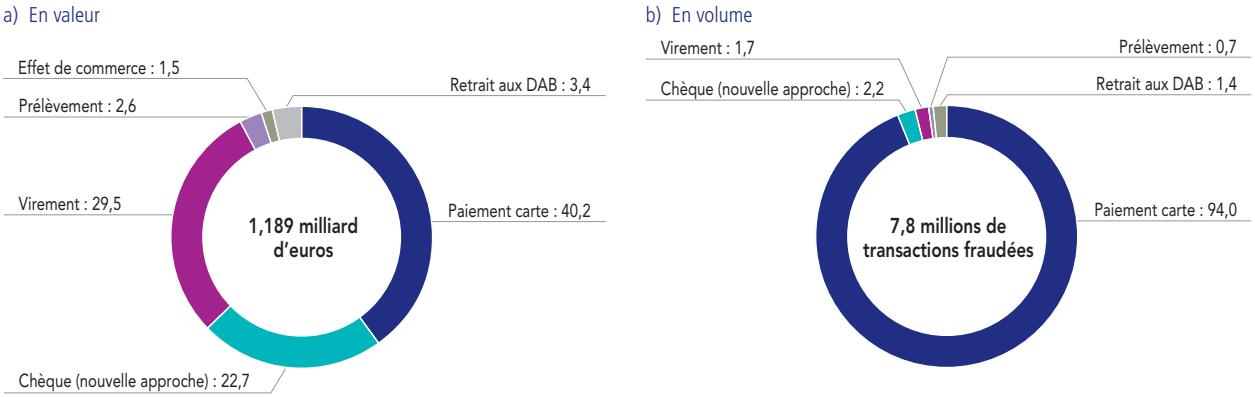
Source : Observatoire de la sécurité des moyens de paiement.

1.1.2 Panorama de la fraude aux moyens de paiement

Alors que les transactions scripturales progressent tant en volume qu'en valeur, le montant total de la fraude se stabilise à 1,189 milliard d'euros (– 0,6 % par rapport à 2023). Toutefois, le nombre de transactions fraudées augmente de 9,3 % pour atteindre 7,8 millions d'opérations.

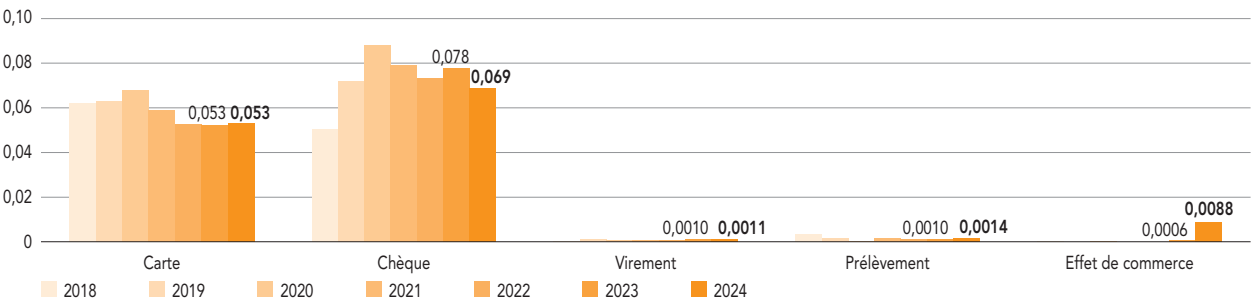
Au regard des principales évolutions observées, cette stabilisation résulte, d'une part, d'une baisse notable de la fraude sur le chèque (– 93,6 millions d'euros) qui est beaucoup plus rapide que celle des flux, et d'autre part, d'une hausse de la fraude sur le virement (+ 39 millions d'euros, dont + 37 millions d'euros sur le virement instantané) et de la carte (+ 23 millions d'euros), qui est essentiellement issue des paiements par carte à distance (+ 22 millions d'euros). Par ailleurs, de faux encaissements de lettres de change, ciblés sur quelques établissements bancaires, expliquent la fraude de 18 millions d'euros sur les effets de commerce, dont les flux restent par ailleurs en baisse (– 6 % par rapport à 2023). Enfin, la fraude sur le prélèvement augmente (+ 8 millions d'euros), soit une progression de + 36 % par rapport à 2023.

G7 Répartition de la fraude (en %)



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.

1.2 État de la fraude sur la carte de paiement

1.2.1 Vue d'ensemble – Cartes émises en France

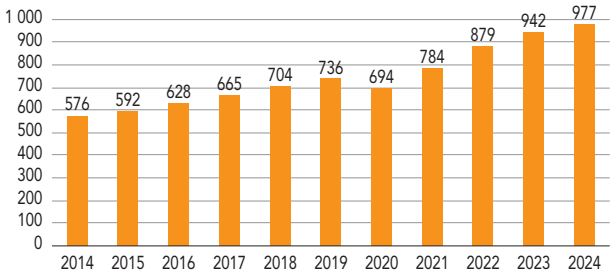
La carte demeure le moyen de paiement principal du quotidien, avec des flux qui continuent de progresser en 2024 en volume comme en valeur (respectivement de + 6 % et + 4 %). Les paiements effectués par mobile continuent de se développer très rapidement (+ 54 %), et représentent désormais 15 % des paiements de proximité.

La valeur de la fraude atteint 519 millions d'euros (+ 4,6 % par rapport à 2023), en miroir de la hausse des flux. Le canal des paiements par carte sur internet reste le plus exposé : il représente 72 % de la fraude en valeur, pour seulement 25 % des montants échangés.

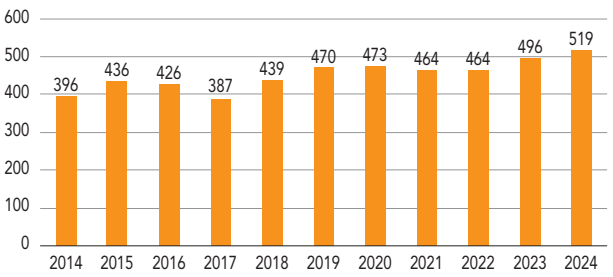
La sécurité de la carte continue de bénéficier des principes de l'authentification forte sur les transactions à distance ainsi que de l'amélioration permanente des outils de détection de la fraude des différents acteurs de l'écosystème des paiements. Après avoir enregistré une diminution proche de 10 % sur deux années consécutives (en 2021 et 2022), le taux de fraude sur les opérations par carte effectuées en France se stabilise à 0,053 % en 2024, et reste ainsi à son plus bas niveau historique. Alors que les paiements de proximité et les retraits d'espèces conservent des taux de fraude stables et faibles (0,011 % pour les premiers et 0,031 % pour les seconds), les paiements sur internet voient leur taux de fraude diminuer à nouveau (0,155 % en 2024, contre 0,160 % en 2023). Ce résultat peut refléter les premiers 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. Les paiements à distance hors internet, qui concernent les paiements pour lesquels les clients

G9 Les cartes émises en France en 2024

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



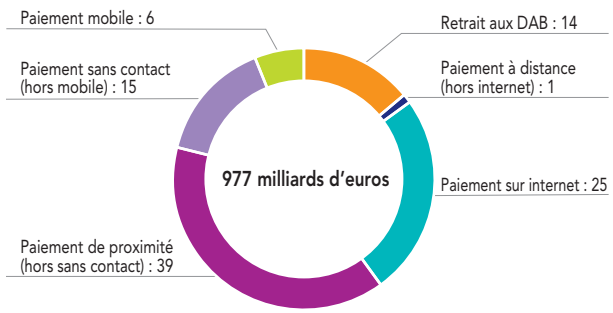
b) Valeur totale de la fraude (en millions d'euros)



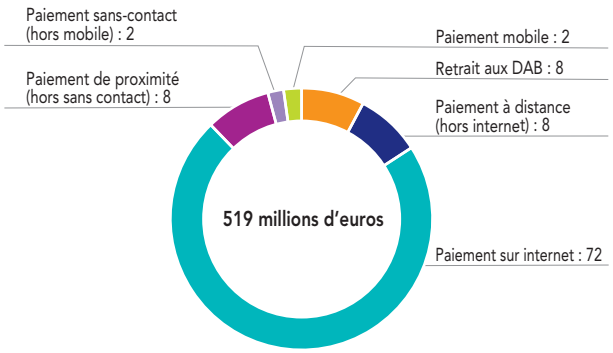
Source : Observatoire de la sécurité des moyens de paiement.

G10 Le canal d'utilisation des cartes émises en France en 2024 (en %)

a) Répartition du montant des opérations



b) Répartition de la valeur de la fraude



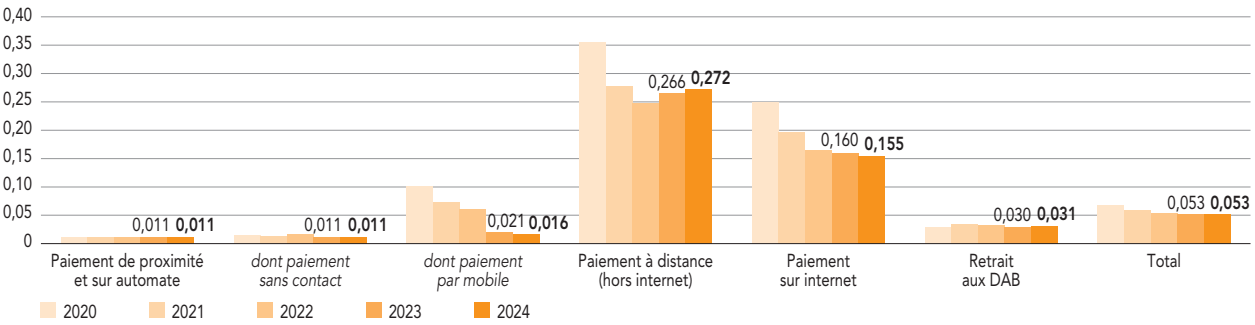
Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

communiquent les informations relatives à leur carte de paiement par téléphone ou courrier (*Mail order – telephone order*, MOTO), enregistrent une hausse de leur taux de fraude pour la seconde année consécutive (0,272 % en 2024, contre 0,266 % en 2023 et 0,247 % en 2022). Le plan de l'OSMP accompagne toutefois une baisse des montants échangés par ce canal (– 6 %), qui s'associe à une baisse quasi équivalente de la fraude (– 4 % à 40 millions d'euros).

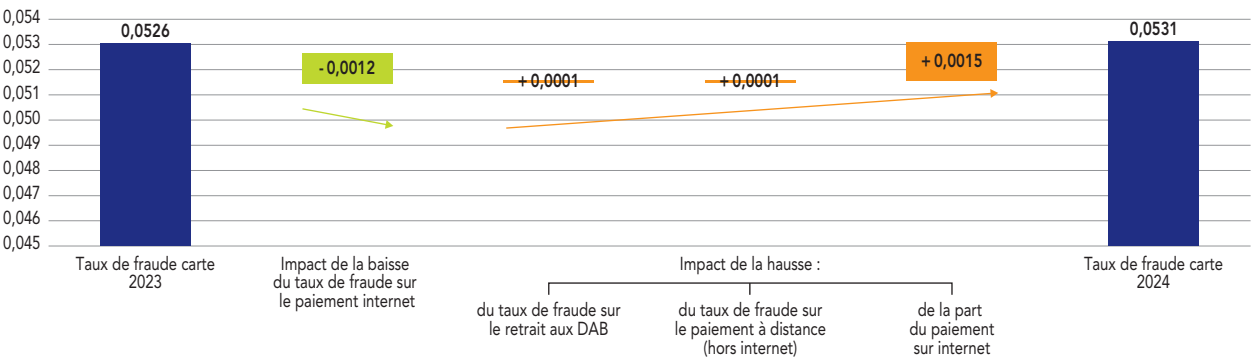
Enfin, le taux de fraude des paiements par mobile poursuit sa baisse (– 22 % en 2024 comparé à 2023) après avoir été divisé par trois en 2023. Cette tendance, qui se confirme dans le temps, est directement liée à un meilleur contrôle de l'enrôlement de l'utilisateur dans la solution de paiement par mobile grâce au recours systématique à une authentification forte du porteur, à la suite du rappel des exigences réglementaires de l'Autorité bancaire européenne et de l'Observatoire en la matière. Ces progrès sont d'autant plus notables que ce moyen de paiement est en plein essor depuis quelques années : son utilisation a été multipliée par sept depuis 2021, et a constitué près de 15 % du nombre de paiements par carte de proximité en 2024.

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



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 %)



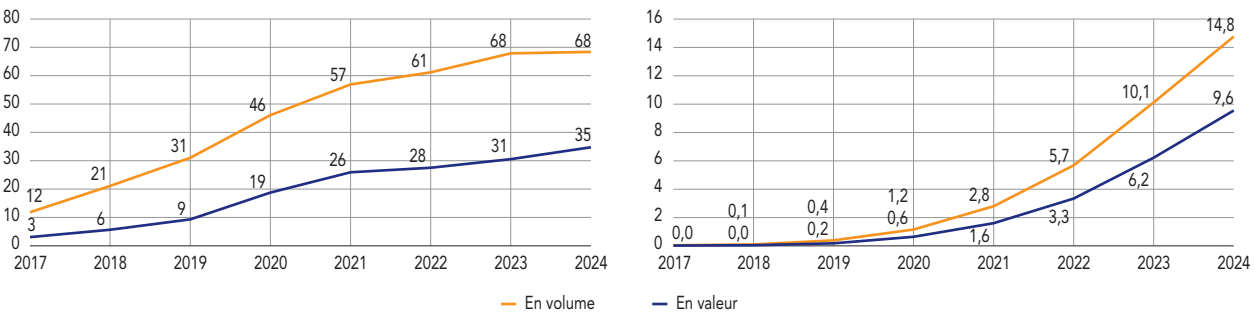
Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

G12 Paiement par carte de proximité (en %)

a) Part du paiement sans contact

b) Part du paiement par mobile

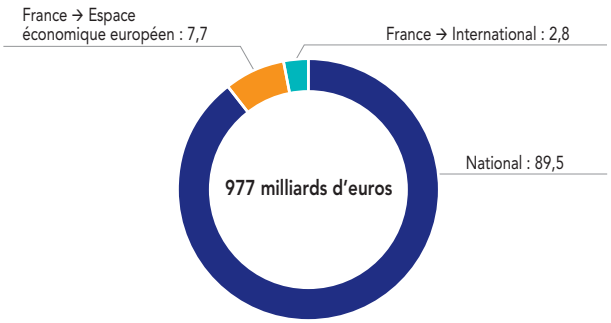


Source : Observatoire de la sécurité des moyens de paiement.

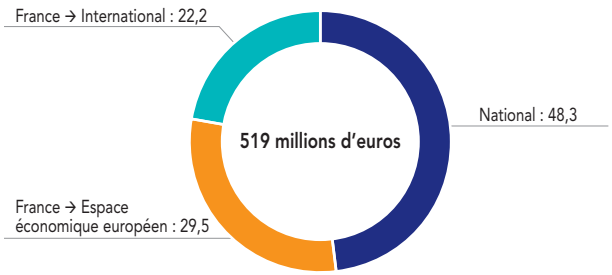
1.2.2 Répartition de la fraude par zone géographique – Cartes émises en France

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

a) Répartition du montant des opérations

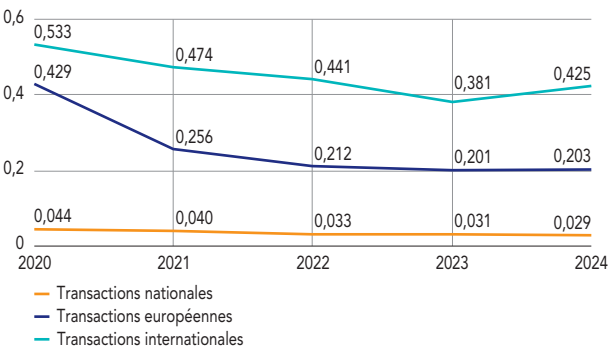


b) Répartition de la valeur de la fraude



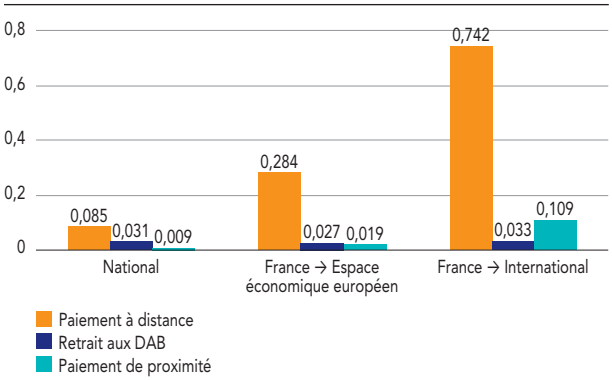
Source : Observatoire de la sécurité des moyens de paiement.

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 %)

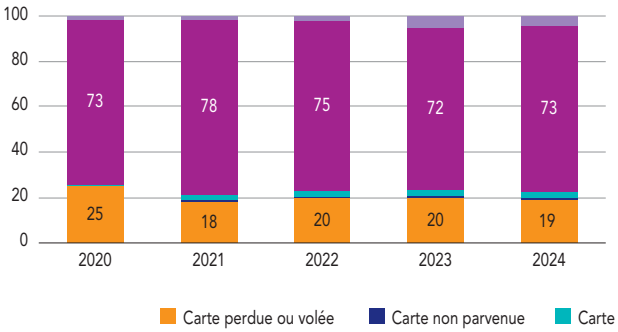


Note : DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

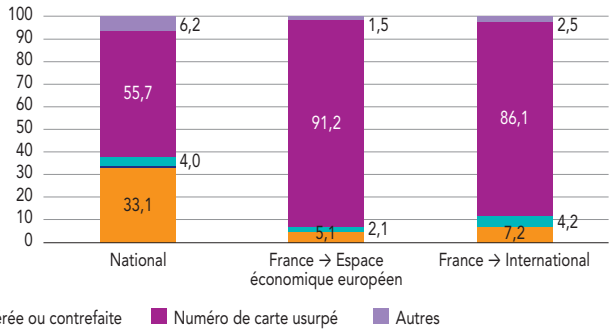
En 2024, les transactions internationales (incluant celles vers l'Espace économique européen) représentent près de 52 % des montants de fraude à la carte (contre 47 % en 2023). Tandis que le taux de fraude sur les transactions nationales atteint un plus bas historique (0,029 %), le taux de fraude des transactions internationales par carte à l'international repart à la hausse (+ 12 %). Ces transactions internationales sont constituées à 90 % de paiements à distance, qui sont historiquement plus fraudés que leurs équivalents nationaux et dont le taux de fraude augmente par rapport à 2023 (0,74 % en 2024, contre 0,65 % en 2023). Les paiements de proximité à l'international restent quant à eux plus exposés à la fraude, 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.

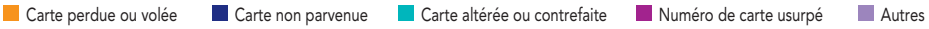
1.2.3 Répartition de la fraude par mode opératoire – Cartes émises en France

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



G17 Typologies dans la valeur de la fraude par zone géographique en 2024 (en %)





Source : Observatoire de la sécurité des moyens de paiement.

La part de la fraude fondée sur l'usurpation de numéros de carte demeure prépondérante. Elle se stabilise en 2024 à 73 % (72 % en 2023). La technique employée reste principalement l'hameçonnage par courriel ou par SMS.

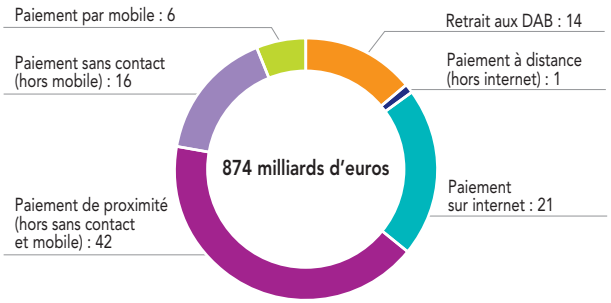
La part de la fraude liée à la perte ou au vol de carte reste constante également, toujours à un faible niveau (19 % en 2024). Très logiquement, l'usage des cartes perdues ou volées se manifeste d'abord sur le territoire national (33 % de la fraude), tandis que la fraude par usurpation du numéro de carte se concrétise d'abord sur internet, constat partagé dans l'ensemble des zones géographiques, même si celle-ci est davantage représentée sur les transactions européennes et internationales.

Les autres types de fraude, comme les cartes non parvenues ou contrefaites, restent marginaux.

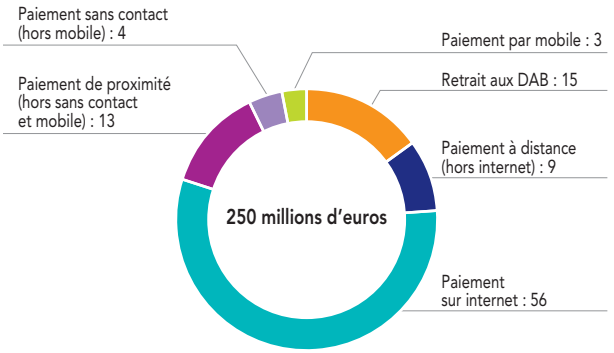
1.2.4 Répartition de la fraude sur les opérations nationales

G18 Transactions nationales par carte en montant (en %)

a) Répartition des transactions

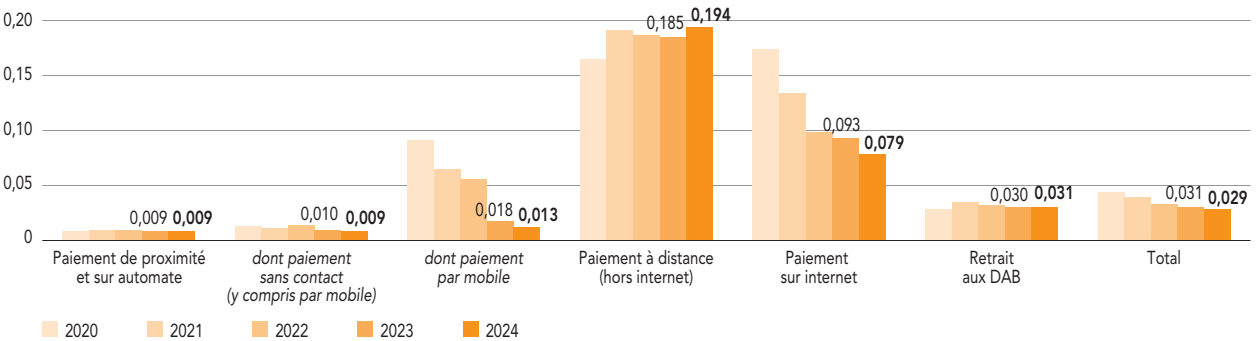


b) Répartition de la fraude



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 %)



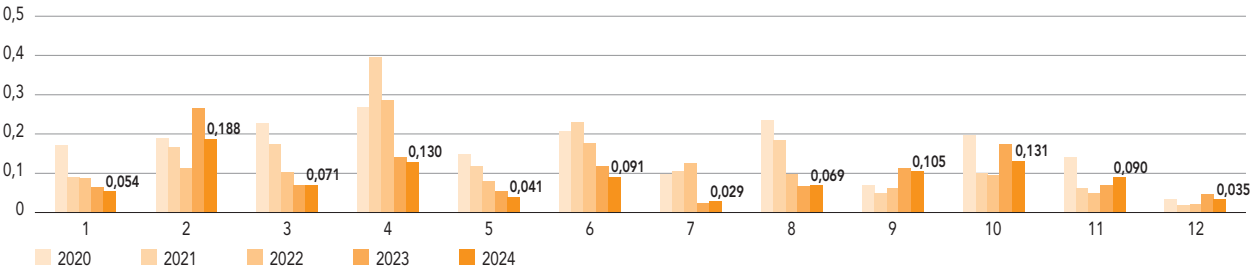
Note : DAB, distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

Les transactions nationales sont de plus en plus sécurisées : le taux de fraude atteint un plus bas historique à 0,029 %.

Avec 163 millions d'euros de fraude, les paiements à distance pèsent pour près de 65 % dans le total de la fraude nationale, quand ils ne représentent que 22 % des montants échangés. Toutefois, les paiements sur internet continuent de bénéficier des actions et des efforts de sensibilisation conduits par l'ensemble des acteurs de l'écosystème des paiements. Ainsi, le taux de fraude sur ces paiements recule encore de 15 % par rapport à 2023 pour s'établir à 0,079 % (contre 0,093 % l'an passé), si bien que celui-ci a été plus que divisé par deux depuis 2020.

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

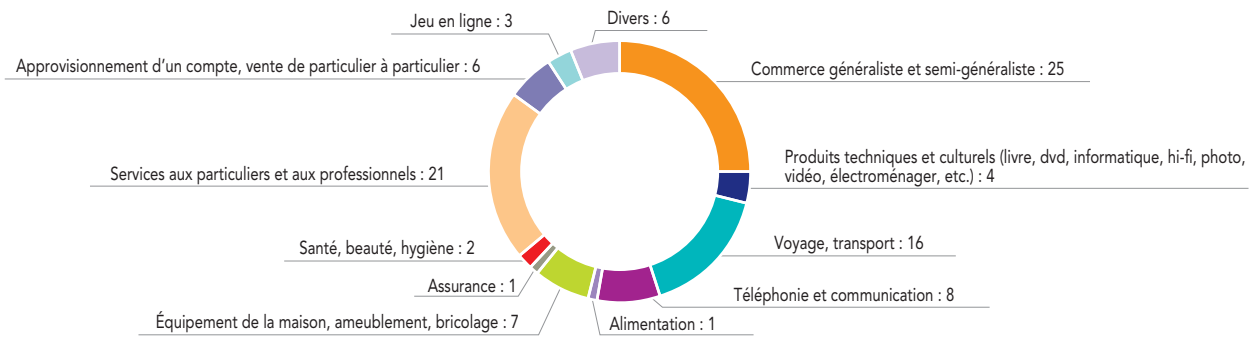
G20 Évolution du taux de fraude sur les paiements nationaux par carte sur internet, par secteur (en %)



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

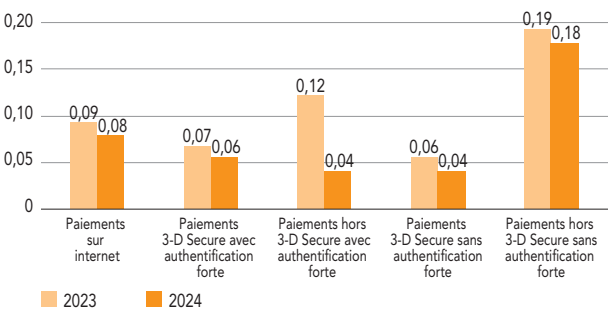
Source : Observatoire de la sécurité des moyens de paiement.

G21 Répartition de la fraude sur les paiements nationaux par carte sur internet en valeur, par secteur en 2024 (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.

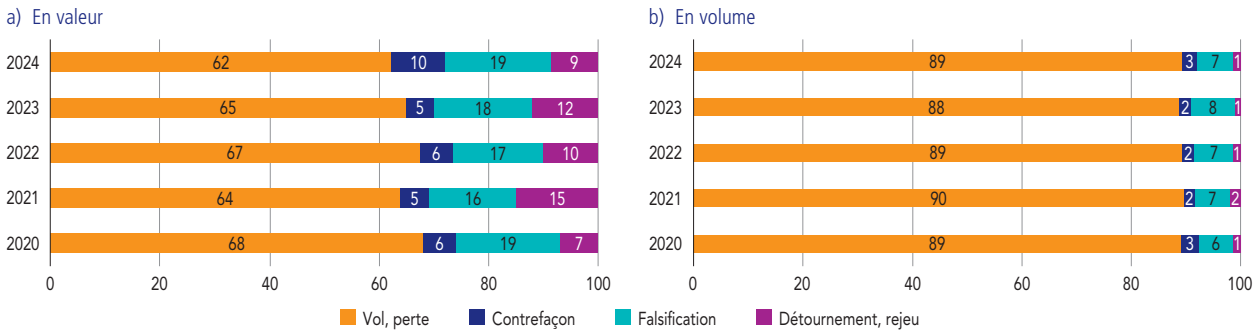
Les paiements nationaux par carte sur internet qui i) n'ont pas recours au protocole d'échange 3-D Secure (ou protocole privatif équivalent) et ii) ne mettent pas en œuvre l'authentification forte demeurent proportionnellement trois fois plus fraudés que les autres canaux. Ce taux de fraude structurellement plus élevé sur les paiements à distance effectués en dehors de 3-D Secure justifie les mesures mises en place depuis juin 2024 par l'Observatoire sur ce type de paiements, dont le déploiement se poursuivra en 2025 et 2026 avec une feuille de route qui a été précisée *(cf. chapitre 3)*.

Parmi les paiements hors 3-D Secure, 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 (63 %). Ils affichent un taux de fraude de plus de deux fois supérieur à celui de l'ensemble des paiements sur internet (0,179 %, contre 0,079 %).

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 des transactions qui s'inscrivent dans ces dispositifs d'exemption reste inférieur à celui des transactions avec authentification forte (0,04 %, contre 0,06 %). Ces indicateurs confirment que les exemptions s'appliquent aux transactions les moins risquées.

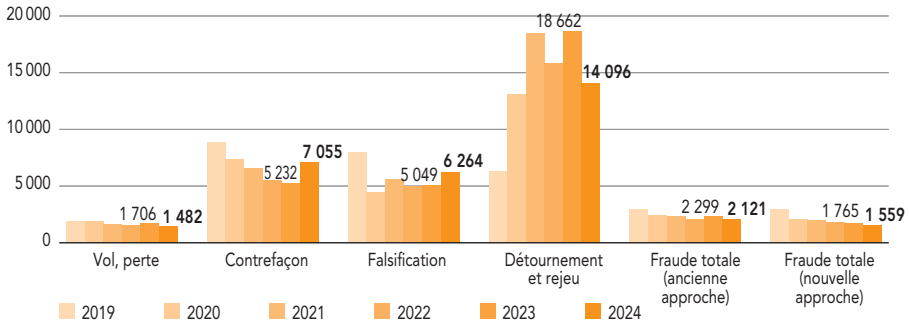
1.3 État de la fraude sur le chèque

G23 Répartition de la fraude sur le chèque par typologie de fraude (en %)



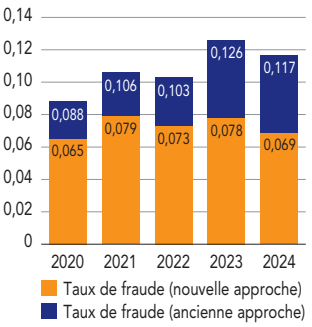
Source : Observatoire de la sécurité des moyens de paiement.

G24 Montant moyen de la fraude sur le chèque par typologie (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.

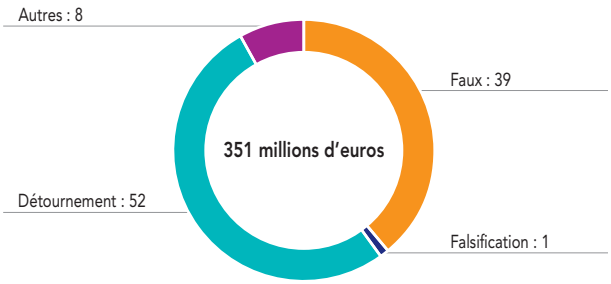
En 2024, la valeur des opérations frauduleuses continue de décroître pour s'établir à 270 millions d'euros (– 26 % par rapport à 2023). Ce fléchissement significatif tient en grande partie à l'instauration par les banques de dispositifs de blocage ou de temporisation des remises de chèques qui a permis de neutraliser 41 % de remises frauduleuses pour 187 millions d'euros de fraude déjouée.

Le taux de fraude sur le chèque baisse sensiblement de 0,078 % en 2023 à 0,069 % en 2024, après exclusion de la fraude déjouée (nouvelle approche). 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. L'acheminement des chéquiers reste donc un point de vigilance important dans le cycle de vie des chèques.

Ces bons résultats traduisent de façon visible les effets à plus long terme de la mise en place des recommandations contre la fraude au chèque publiées en 2021 par l'Observatoire. Le chèque demeure toutefois le moyen de paiement affichant le taux de fraude le plus élevé. L'Observatoire appelle donc l'ensemble des acteurs de la filière chèque à poursuivre les progrès et à se concentrer particulièrement sur la mise en place des recommandations liées i) à la protection des chèques lors de leur acheminement chez le client et ii) à la simplification des procédures de mise en opposition pour perte ou vol *(cf. chapitre 3 pour le détail du suivi des recommandations de l'Observatoire sur le chèque)*.

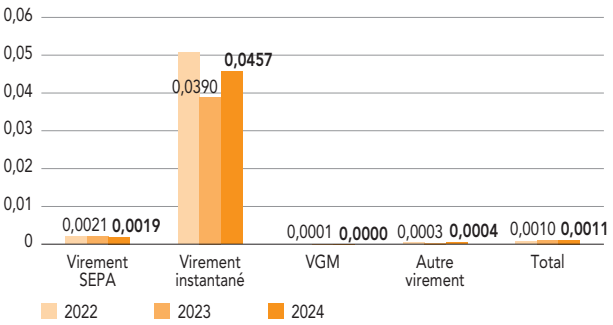
1.4 État de la fraude sur le virement

G26 Répartition de la fraude au virement en valeur par typologie de fraude en 2024 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

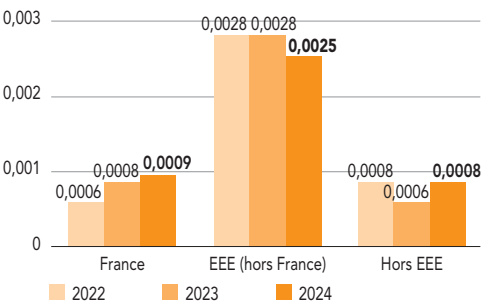
G27 Taux de fraude par type de virement (en %)



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

Source : Observatoire de la sécurité des moyens de paiement.

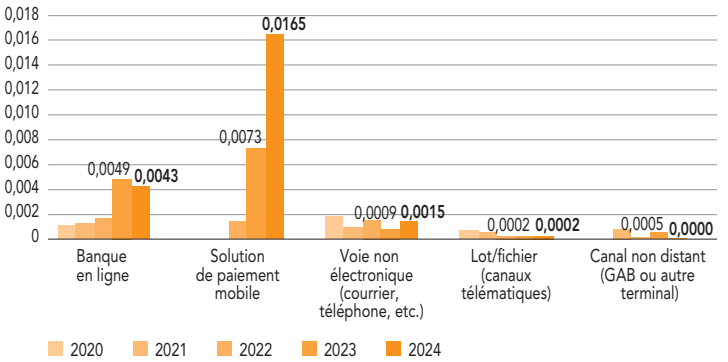
G28 Évolution du taux de fraude au virement par zone géographique (en %)



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.

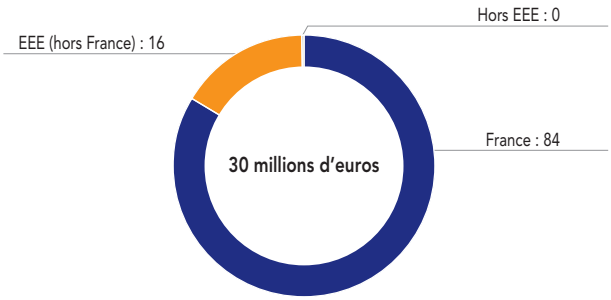
La fraude au virement augmente de 12 % en valeur pour atteindre 351 millions d'euros en 2024. Cette hausse accompagne une évolution structurelle de la fraude au virement : les canaux télématiques utilisés par les entreprises restent très peu exposés à la fraude (taux de fraude extrêmement faible de 0,0002 %), tandis que les fraudeurs attaquent davantage les solutions de banque en ligne (taux de fraude de 0,0043 %) et de paiement par mobile. 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 valider une opération. Par ailleurs, les fraudeurs recourent de plus en plus aux comptes ouverts en France pour récupérer leurs fonds (+ 13 % du taux de fraude au niveau domestique), même si les virements européens sont proportionnellement plus de deux fois plus fraudés que les virements nationaux.

Le taux de fraude du virement instantané progresse légèrement (0,046 % en 2024, contre 0,039 % en 2023). Il se situe toutefois toujours en dessous de celui de la carte (0,053 %), alors même que ces deux moyens de paiement – majoritairement utilisés par les consommateurs – s'appuient sur des mécanismes de sécurité semblables. Il s'agit, en particulier, du recours aux mêmes dispositifs d'authentification forte du payeur pour les paiements en ligne.

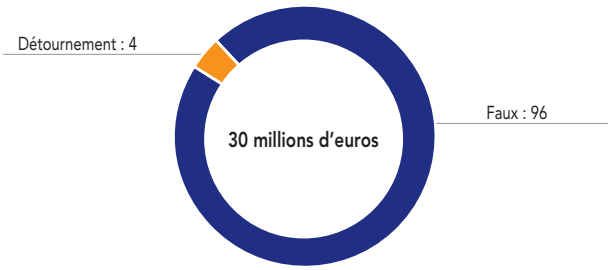
1.5 État de la fraude sur le prélèvement

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

a) Par zone géographique



b) Par typologie de fraude

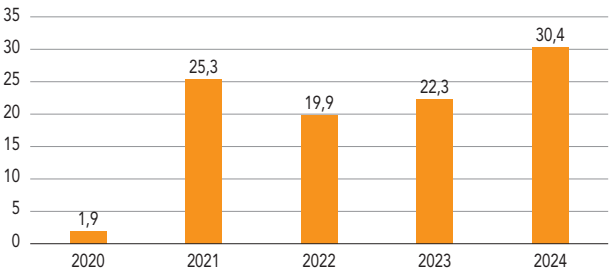


Note : EEE, Espace économique européen.

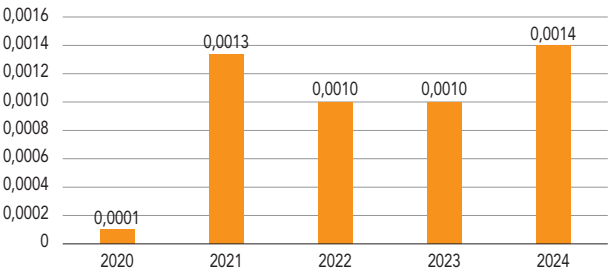
Source : Observatoire de la sécurité des moyens de paiement.

G31 Fraude au prélèvement

a) En valeur (en millions d'euros)



b) Taux (en %)



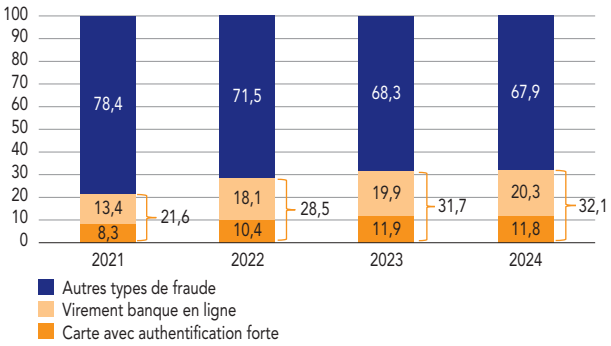
Source : Observatoire de la sécurité des moyens de paiement.

Alors que le montant des flux échangés est resté stable (+ 2 %), la valeur de la fraude au prélèvement continue d'augmenter (+ 36 %) pour atteindre 30,4 millions d'euros. Le taux de fraude augmente mécaniquement (0,0014 % en 2024, contre 0,0010 % en 2022 et en 2023). La fraude émane presque exclusivement de créanciers fraudeurs, qui émettent de faux ordres, donc sans disposer de mandat de prélèvement ni de relation économique avec la victime. La fraude par détournement, c'est-à-dire par lequel le fraudeur débiteur usurpe l'identité et le numéro de compte bancaire international (IBAN, *international bank account number*) d'un tiers pour signer un mandat de prélèvement, reste minoritaire en 2024 (4 %).

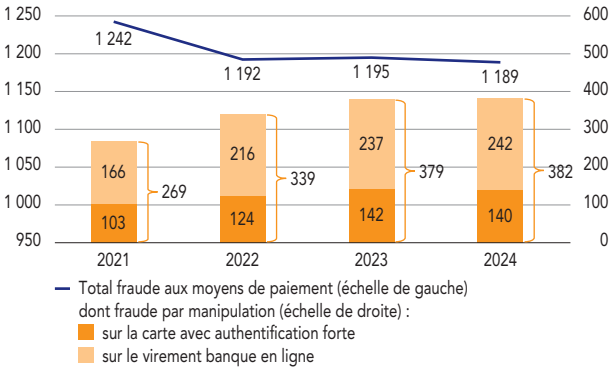
1.6 État de la fraude par manipulation

G32 Évolution de la fraude par manipulation, en valeur

a) Poids (en %)

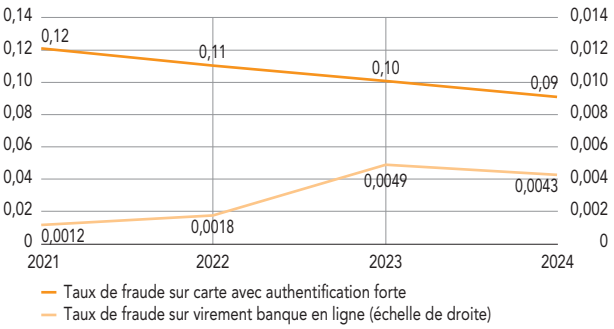


b) En montant (en millions d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G33 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, qui sont les deux canaux ciblés par les fraudeurs.

Après une nette progression entre 2021 et 2023 (+ 47 %), la fraude par manipulation est en légère hausse tant en montant (+ 0,7 %, à 382 millions d'euros) qu'en part relative dans le total de la fraude (en passant de 31,7 % en 2023 à 32,1 % en 2024). La baisse de la part de la fraude sur les opérations par carte fortement authentifiées (– 0,8 % en valeur) est compensée par la hausse de la part de la fraude opérée depuis la banque en ligne (+ 2,3 %). En revanche, du fait de la hausse des flux sous-jacents, les taux de fraude sont en baisse sur ces deux canaux.

Cette stabilisation globale de la part de la fraude par manipulation est imputable i) aux nombreux efforts de sensibilisation des différents acteurs de l'écosystème et ii) à la mise en place par les prestataires de services de paiement de 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*, etc.). Le mécanisme d'authentification des numéros, exigé par la loi Naegelen visant à lutter contre les appels frauduleux, a été déployé à partir d'octobre 2024. Il devrait progressivement empêcher les fraudeurs d'usurper les numéros de téléphone des prestataires de services de paiement. Le déploiement d'un service de vérification de la cohérence des coordonnées bancaires (IBAN) à partir d'octobre 2025 devrait aussi aider à lutter contre les fraudes par manipulation, notamment celles avec substitution frauduleuse d'IBAN.

ENCADRÉ

❶

Indicateurs, enseignements et préconisations des services du ministère de l'Intérieur sur la fraude aux moyens de paiement en 2024

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 2024.

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

Le 10 juillet 2025, le Service statistique ministériel de la sécurité intérieure (SSMSI) a publié l'atlas complet des statistiques 2024 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. En effet, 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 avec celles publiées par l'Observatoire.

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

Toutefois, 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.

Bien que 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 411 700 victimes en 2023 à 417 300 victimes en 2024, le rythme de sa progression ralentit nettement (+ 1,4 % entre 2023 et 2024, contre + 6 % entre 2023 et 2022).

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 cible davantage les personnes physiques que les personnes morales**. En effet, d'après l'étude du SSMSI, les personnes morales représentent 9 % des victimes en 2024, contre 16 % en 2016.

1. Cf. ministère de l'Intérieur, « Insécurité et délinquance en 2024 », 9e édition du bilan statistique.

2. D'après l'enquête Vécu et ressenti en matière de sécurité (VRS) de 2022 du SSMSI, environ 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 du SSMSI souligne qu'en 2024, **la moitié des escroqueries et fraudes aux moyens de paiement sont liées au numérique**. Cette part est en forte augmentation depuis 2016, passant de 31 % en 2016 à 50 % en 2024. 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 victimes pour 1 000 habitants dans cette tranche d'âge.

Les 18-44 ans, à eux seuls, comptent pour près de 45 % des victimes alors qu'ils ne constituent que 32 % 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 2024, pour les seuls FOVI à l'encontre des personnes morales, la Direction nationale de la police judiciaire (DNPJ) a été informée de 649 affaires pour un préjudice total de 34 millions d'euros, contre 657 [4] affaires en 2023 pour un préjudice total de 49 millions d'euros [5].

Parce qu'elles couvrent tous les profils de victimes, les personnes physiques comme les personnes morales, les tendances générales mesurées par l'Observatoire font, quant à elles, état d'une croissance : la fraude au virement par détournement augmente en valeur (+ 20 %) et en volume (+ 118 %).

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

Depuis 2018, **la plateforme Perceval** de la gendarmerie permet de recueillir auprès des utilisateurs le signalement des usages frauduleux de cartes de paiement sur internet. Les enregistrements effectués sur cette plateforme peuvent être plus facilement rapprochés des tendances constatées par l'Observatoire. Elle fait état de 227 711 signalements en 2024 (contre 258 700 en 2023, soit une baisse de 12 %). 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, rapproché des statistiques de l'Observatoire, continue de décroître sur Perceval. Ainsi, 37 % de la fraude à la carte sur les paiements internet telle que quantifiée par l'Observatoire aurait été signalée sur Perceval en 2023, contre 44 % en 2024 et 51 % en 2022. Les victimes ont tendance à ne déclarer que les fraudes les plus importantes : en 2024, le montant moyen par transaction frauduleuse est de 60 euros d'après les statistiques de l'Observatoire, contre 168 euros d'après Perceval (637 euros par signalement qui comprend en moyenne 3,82 transactions).

4. Les chiffres 2023 présentés ici peuvent être légèrement supérieurs à ceux présentés dans les rapports annuels de l'OSMP de 2023. Cela s'explique par le temps de latence qui existe entre, d'une part, la date 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 entraîne une réactualisation régulière des totaux des années concernées à la hausse.

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

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 d'escroqueries en ligne de déposer plainte à distance [6]. En 2024, cette plateforme a recensé 53 300 dépôts de plainte relatifs à une escroquerie ou une fraude aux moyens de paiement. Cela représente 11 % du total des victimes d'escroquerie ou de fraude aux moyens de paiement recensées par le SSMSI, taux en baisse par rapport à 2023 (14 %).

L'Observatoire rappelle aux victimes l'utilité de déclarer leurs fraudes sur les plateformes Perceval ou Thésée, après avoir vérifié leur éligibilité. Les forces de l'ordre peuvent ainsi disposer des informations nécessaires au démantèlement 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 mettent en lumière une très forte baisse des piratages des terminaux de paiement et de retrait sur ces dernières années. Néanmoins, **les gestionnaires de stations-essence, les gestionnaires de DAB et les commerçants doivent rester vigilants quant au risque** de tentatives 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 bien à un dépôt de plainte effectué en présentiel au commissariat de police ou en 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 10 juillet 2025 dans son bilan statistique sur l'insécurité et la délinquance en 2024.

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 implication 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

BILAN DES RECOMMANDATIONS SUR LA PRÉVENTION ET LE REMBOURSEMENT DES OPÉRATIONS DE PAIEMENT FRAUDULEUSES

2.1 Contexte des travaux

Dans un contexte de développement des cas de fraude utilisant des techniques de manipulation de la victime, l'Observatoire de la sécurité des moyens de paiement (OSMP) avait adopté en avril 2023 un ensemble de treize recommandations. Celles-ci visent à la fois à clarifier les modalités d'application du cadre législatif en matière de remboursement des opérations contestées et à renforcer les mécanismes de prévention de la fraude.

Dans le cadre de ces recommandations, l'Observatoire avait par ailleurs confié à la Banque de France et à l'Autorité de contrôle prudentiel et de résolution (ACPR) la réalisation d'un bilan après dix-huit mois d'application. Le présent chapitre restitue donc le bilan des actions conduites par les deux autorités.

L'**ACPR** a lancé à l'été 2024 une enquête par questionnaire auprès de quatorze prestataires de services de paiement constituant un échantillon représentatif des différents profils de prestataires de services de paiement (réseaux bancaires traditionnels, banques en ligne, banques mutualistes, banques généralistes et établissements de paiement). Cette enquête a été suivie d'interventions individuelles auprès de chacun des établissements en vue de vérifier la mise en œuvre des recommandations.

La **Banque de France** a mis en place une collecte statistique portant spécifiquement sur le traitement des contestations pour motif de fraude reçues par les prestataires de services de paiement. Elle a couvert les six principaux groupes bancaires français, avec des données portant sur chaque semestre de la période 2023-2024 ainsi que le premier trimestre 2025.

2.2 Synthèse

Le bilan de l'application des recommandations résultant des évaluations de l'ACPR et de la Banque de France est positif :

- **La sécurité des parcours de paiement a été globalement renforcée, en particulier sur internet et sur les applications bancaires,** selon deux axes : une meilleure information communiquée au client (nature de l'opération en cours, montant, bénéficiaire, rappels de vigilance) et l'introduction de frictions volontaires (par exemple par des choix ou des questions explicites). Cette combinaison permet à l'utilisateur de mieux réagir face aux tentatives de manipulation ;
- **Le traitement des contestations pour motif de fraude s'est également amélioré conformément aux recommandations :** il s'appuie désormais sur l'analyse des trois familles de critères recommandées par l'Observatoire (paramètres techniques associés à l'opération, modalités d'authentification forte mise en œuvre et éléments de contexte), en tirant notamment parti des informations enrichies issues des nouveaux parcours d'authentification. Les refus de remboursement sont ainsi davantage étayés, même si des efforts sont encore à faire par certains établissements pour mettre à disposition les éléments de preuve techniques en cas de demande du client ;

- En particulier, **le remboursement systématique et immédiat des paiements frauduleux n'ayant pas fait l'objet d'une authentification forte est bien constaté sur les paiements par carte**. Des progrès restent néanmoins attendus sur le remboursement des paiements frauduleux par virement sans authentification forte, qui doit bénéficier d'un traitement similaire.

L'ACPR et la Banque de France continueront à suivre dans le temps les pratiques individuelles des établissements, en particulier de ceux qui présentent encore des marges de progression dans l'application des recommandations. Elles continueront également à assurer le suivi **des indicateurs statistiques de qualification des contestations et de remboursement** des principaux établissements établis en France.

2.3 Bilan de l'application des recommandations générales relatives au traitement des contestations d'opérations de paiement

Recommandation n° 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.

Recommandation n° 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.

Recommandation n° 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.

Les interventions conduites par l'ACPR ont permis de mettre en évidence un niveau satisfaisant de conformité à ces trois recommandations : les procédures de traitement des contestations tiennent désormais compte des exigences de délais fixés par la réglementation et par les recommandations n° 1 et n° 2.

En particulier, le formalisme des contestations exigé par les établissements a été assoupli, permettant désormais de les prendre en compte :

- sans remise d'un dépôt de plainte par la victime pour tous les établissements ;
- et sans remise d'un formulaire signé pour 12 établissements sur les 14 interrogés.

L'autorité note toutefois des progrès encore attendus de la part de quelques établissements concernant la recommandation n° 3 :

- 5 établissements sur 14 font encore état de difficultés opérationnelles pour remettre l'ensemble des éléments attendus à leur client lorsque celui-ci les demande.

Les établissements concernés continueront à faire l'objet d'un suivi individuel de la part de l'ACPR.

2.4 Bilan des recommandations applicables au traitement de cas spécifiques

Recommandation n° 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 [1] 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 [2]), 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*), 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.

1 La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la contestation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs, etc.).

2 Sauf pour les prélèvements contestés dans les huit semaines suivant le débit du compte, pour lesquels le payeur dispose d'un droit au remboursement inconditionnel. SEPA – *Single Euro Payment Area*, espace unique de paiement en euros.

Recommandation n° 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.

Recommandation n° 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, l'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 le 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, et 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 qu'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.

Les interventions conduites par l'ACPR ont permis de mettre en évidence un niveau satisfaisant de conformité à ces trois recommandations : en particulier, les établissements ont bien intégré dans leur processus de traitement des contestations l'analyse des trois familles de critères (paramètres techniques associés à l'opération, modalités d'authentification forte mise en œuvre et éléments de contexte) requis par la recommandation n° 6.

L'ACPR note toutefois des progrès encore attendus de la part de quelques établissements :

- Tous les établissements annoncent pouvoir procéder au remboursement des frais occasionnés par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs, etc.) et au versement de pénalités de retard dues en cas de remboursement tardif. Toutefois, 5 d'entre eux (sur une base de 14 établissements évalués) ne disposent pas d'un système automatisé pour le faire ;
- Concernant la recommandation n° 4, 2 établissements sur les 12 concernés [3] attendent le résultat de la recherche de mandat dans le cadre de prélèvements contestés plus de huit semaines après leur débit en compte avant de procéder au remboursement, ce qui va à l'encontre du principe de remboursement à J+1 inscrit dans la réglementation et rappelé par la recommandation n° 4. Ces établissements devraient rembourser immédiatement le client en faisant état d'une possible reprise des fonds sous 30 jours en cas d'obtention de la preuve d'un mandat signé par le client et non révoqué, autorisant le prélèvement contesté.

L'ACPR continuera à suivre individuellement les établissements concernés.

En complément, les statistiques collectées par la Banque de France permettent d'analyser la façon dont les établissements donnent suite aux contestations reçues, selon un processus aligné avec l'arbre de décision présenté en préambule des recommandations.

- Le premier filtre consiste à déterminer si l'opération peut être considérée comme autorisée par l'utilisateur. Il vise notamment à exclure les opérations résultant d'un litige commercial (par exemple, bien ou service non livré ou non conforme aux attentes du client, ou liquidation judiciaire du commerçant) et les cas où le client a consenti à l'opération tout en étant victime d'une escroquerie (par exemple, faux site usurpant l'identité d'un e-commerçant, faux investissements, chantage amoureux ou paiement de rançongiciel). En effet, ces ordres de paiement ont été consentis par l'utilisateur et ne permettent donc pas l'application de la réglementation en matière de remboursement des cas de fraude.

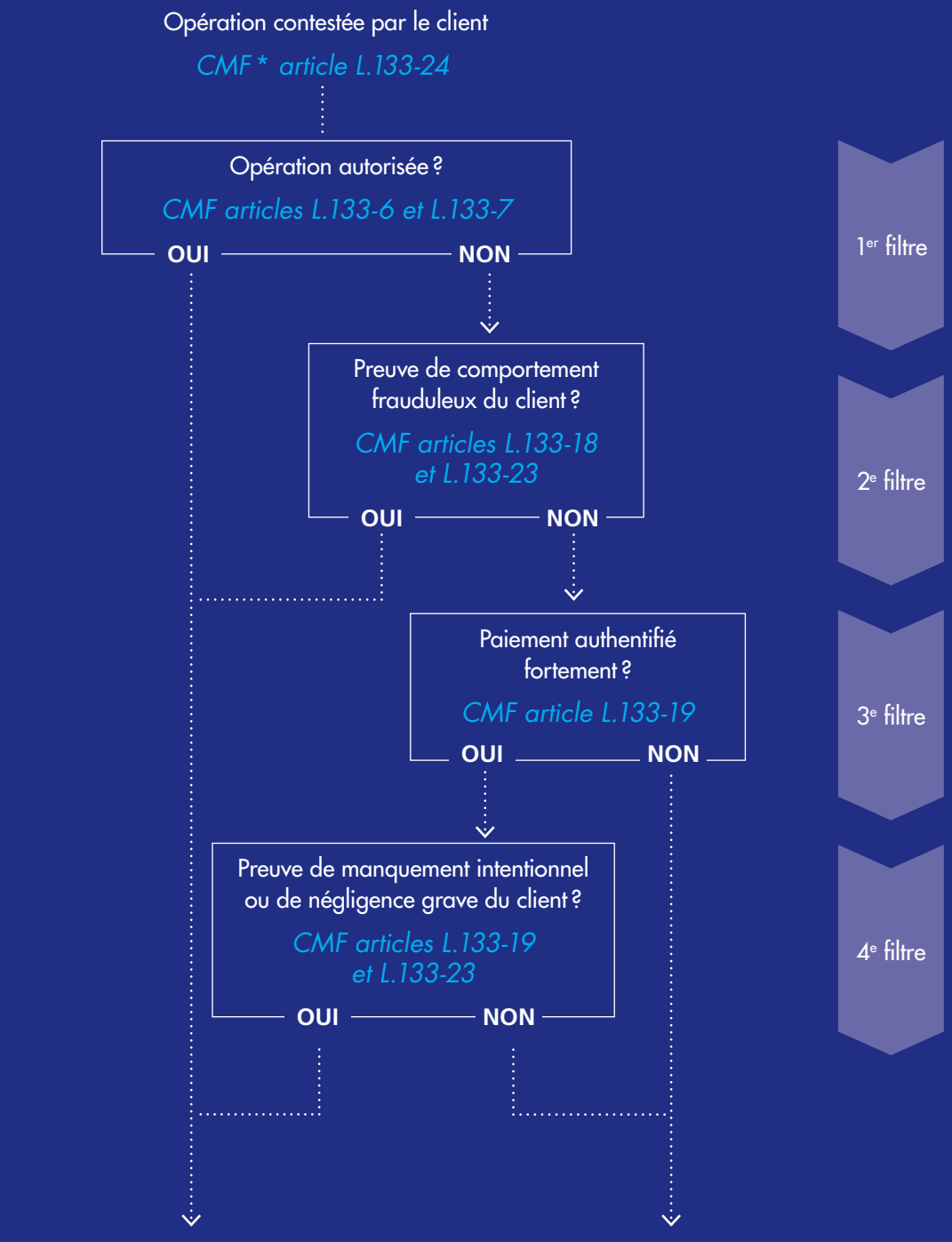
  ➡ Ce filtre a conduit les banques à exclure 12 % du nombre de contestations, concentrant 26 % du montant total des contestations.

- Le deuxième filtre consiste à identifier les cas de contestation abusive de la part du client, lorsque lui-même ou son entourage proche sont bien à l'origine de l'opération (par exemple, cas d'un achat passé par les enfants du client à son insu, en utilisant son terminal et ses outils d'authentification forte).

  ➡ Ce filtre conduit à exclure 4 % du nombre des contestations, représentant 3 % de leur montant total.

3 Sur les quatorze prestataires de services de paiement évalués par l'ACPR, deux n'offrent pas de services de prélèvement.

PROCESSUS DE TRAITEMENT D'UNE OPÉRATION CONTESTÉE



* CMF, Code monétaire et financier

À l'issue de ces deux premiers filtres, les contestations restantes (soit 84 % du nombre de transactions initialement contestées pour 70 % du montant total) correspondent aux opérations qualifiées de frauduleuses au sens des travaux de l'Observatoire. C'est sur cette base que doit être apprécié le taux effectif de remboursement des banques.

- Le troisième filtre vise à identifier les contestations d'opérations n'ayant pas fait l'objet d'une authentification forte, qui doivent être systématiquement remboursées en application de la recommandation n° 4.

  ➡ **Concernant les paiements par carte sans authentification forte, le taux de remboursement ressort à 98 % en montant, soit un niveau conforme à la recommandation n° 4 ;**

  ➡ **Concernant les virements sans authentification forte, le taux de remboursement observé est très insuffisant, à 20 % en montant. Dans la mesure où les banques ne peuvent pas invoquer la négligence grave de l'utilisateur sur ce type d'opération, cet indicateur met en exergue une non-conformité persistante. Celle-ci porte toutefois sur une faible proportion des contestations (moins de 10 % du nombre de cas). La Banque de France sera attentive à l'évolution de cet indicateur et interviendra individuellement au niveau des établissements.**

- Le quatrième filtre vise à identifier, parmi les transactions contestées ayant fait l'objet d'une authentification forte, celles pour lesquelles la banque est en mesure de démontrer que le client a fait preuve de négligence grave dans la protection de ses identifiants personnels ou de ses moyens d'authentification, justifiant alors le refus de remboursement.

  ➡ **À l'issue de ces deux derniers filtres, le taux global de remboursement tous paiements confondus s'établit à 91 % en nombre d'opérations et à 62 % en montant.**

  ➡ **Ce taux global s'inscrit en repli sur les deux dernières années, dans un contexte où le renforcement des parcours client permet une meilleure information du client tout au long du parcours d'authentification en vue de mieux mettre en échec les tentatives de manipulation.**

  ➡ **De fait, les établissements sont davantage en situation de déterminer dans quelle mesure l'utilisateur a pu être négligeant au regard des alertes qui lui ont été adressées et des choix qui lui ont été proposés pour les opérations incriminées.**

2.5 Bilan des recommandations à l'attention des consommateurs et de leurs représentants

Recommandation n° 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.).

Recommandation n° 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 ou des démarches en ligne sur les plateformes Perceval ou Thésée, voire 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 ou, le cas échéant, le dépôt de plainte auprès des forces de l'ordre, etc.

Les travaux conduits par l'ACPR et la Banque de France auprès des prestataires de services de paiement ne permettent pas de mesurer la bonne application de ces recommandations par les consommateurs. L'Observatoire relève néanmoins que, après la publication de ses recommandations, les prestataires de services de paiement ont fait un travail important de sensibilisation pour rappeler les bonnes pratiques de sécurité à leurs clients.

2.6 Bilan des recommandations visant à prévenir la fraude

Recommandation n° 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.

Recommandation n° 10 :

Modalités d'enregistrement des IBAN bénéficiaires de virements

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 le numéro de compte bancaire international (IBAN, *International Bank Account Number*) et le 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.

Recommandation n° 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.

Recommandation n° 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.

Recommandation n° 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 contenus, 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* ou le *SIM-swapping*.

Les interventions conduites par l'ACPR ont permis de mettre en évidence un niveau satisfaisant de conformité aux recommandations n° 9, n° 10, n° 11 et n° 12, avec un engagement fort des établissements évalués dans les outils de prévention de la fraude. En particulier, en réponse à la recommandation n° 11, les parcours d'authentification des établissements affichent tous désormais des informations permettant de bien caractériser l'opération (nature, montant, bénéficiaire, etc.).

L'ACPR note toutefois que des progrès sont encore attendus de la part de quelques d'établissements :

- concernant la recommandation n° 9, 3 établissements sur 13 [4] ne procèdent toujours pas à une authentification forte pour l'accès aux comptes depuis un nouvel appareil, préférant fonder leur analyse sur leur modèle interne d'appréciation du risque ;
- concernant la recommandation n° 10, 2 établissements sur 12 sont invités à communiquer plus explicitement sur les spécificités du virement instantané au moment où l'utilisateur doit choisir entre virement traditionnel et virement instantané ;
- concernant la recommandation n° 12, l'ACPR invite les établissements qui ne le proposent pas encore à développer des offres permettant de fixer des limitations en matière de paiement afin de prévenir la fraude, telles que les listes blanches ou noires pour les prélèvements (1 établissement concerné sur 12) ou le paramétrage en ligne de plafond de virement (5 établissements concernés sur 13), ce qui est une exigence réglementaire pour les virements instantanés [5].

L'ACPR continuera à suivre individuellement les établissements concernés.

Enfin, au titre de la recommandation n° 13, la coopération de l'Observatoire avec le secteur des télécommunications continue à se renforcer de façon tout à fait positive. Dans le même temps, la coopération avec les acteurs du numérique, en particulier les plateformes et applications de messagerie, peut encore sensiblement progresser *(cf. chapitre 3, section 2)*.

4 Le nombre d'établissements concernés par une recommandation peut être différent du nombre total d'établissements évalués (quatorze), car certaines recommandations ne sont pas applicables au modèle d'affaires de certains établissements.

5 Article 5 *bis* (6) du règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012.

3

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

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

3.1.1 Rappel des recommandations adoptées par l'Observatoire et de leur contexte

Au début de l'année 2024, les statistiques de fraude sur les paiements par carte à distance ont fait apparaître un écart important entre les différentes catégories de paiement à distance. Le taux de fraude affiche ainsi une forte variation (pouvant aller du simple au triple) :

- d'une part, selon le canal utilisé, entre les paiements par internet et les paiements à distance hors internet tels que les paiements effectués par courrier ou par téléphone ;
- d'autre part, s'agissant des paiements par internet, selon le protocole utilisé, entre les paiements effectués via le protocole 3-D Secure et les paiements effectués, au contraire, sans recours à ce protocole, dits paiements *direct to authorisation* (DTA).

La maîtrise de la fraude sur les paiements avec authentification forte s'explique par le déploiement de l'authentification forte du payeur pour les opérations de paiement électroniques et pour toute opération sensible susceptible de comporter un risque de fraude [1].

La mise en œuvre de l'authentification forte pour les paiements par internet a été rendue possible par le déploiement de la deuxième version du protocole 3-D Secure destiné à la gestion des échanges entre le commerçant, le porteur de la carte et leurs prestataires de services de paiement (PSP) respectifs. Le protocole 3-D Secure peut également prendre en charge les exemptions à l'authentification forte prévues par le règlement délégué UE n° 2018/389 du 27 novembre 2017 (ou RTS, *regulatory technical standard*) : de telles exemptions sont possibles par exemple dans le cas d'opérations récurrentes, d'opérations de faible montant ou encore d'opérations qui présentent un faible niveau de risque.

La fraude apparaît également maîtrisée pour les paiements exemptés d'authentification forte effectués au moyen du protocole 3-D Secure. En effet, le protocole 3-D Secure permet l'application des règles de détection de la fraude élaborées par le PSP émetteur, souvent enrichies par les indicateurs de fraude du système interbancaire de paiement par carte. Ainsi, lorsqu'un paiement présente un risque de fraude jugé élevé par le PSP émetteur, celui-ci peut exiger l'authentification forte du porteur même lorsque le paiement est éligible à une exemption.

À l'inverse, la fraude est sensiblement plus élevée sur les paiements CIT (*customer initiated transaction*, paiement initié par le client) exemptés d'authentification forte effectués hors 3-D Secure, ainsi que sur les paiements MIT (*merchant initiated transaction*, paiement initié par le commerçant, par exemple dans le cas de paiements fractionnés ou de paiement d'un abonnement).

De même, une fraude significative est observée sur les paiements MOTO (*mail order, telephone order*, paiements par carte initiés par courrier ou par téléphone), favorisée par les caractéristiques mêmes de ces paiements à distance effectués hors internet. En effet, à ce jour, il n'existe pas de solution communément déployée pour l'authentification forte de tels paiements, de sorte qu'en cas de détournement de données de paiement (numéro de carte et date d'expiration), le fraudeur peut aisément procéder à des paiements à l'insu du porteur.

1 L'authentification forte est prévue par la directive UE n° 2015/2366 du 25 novembre 2015 sur les services de paiement, dite DSP 2.

Ces constats avaient conduit l'Observatoire à adopter en juin 2024 un ensemble de cinq recommandations portant sur deux volets :

- d'abord sur les paiements MOTO, en invitant les commerçants à limiter strictement le recours aux paiements MOTO aux seuls cas d'usage spécifiques pour lesquels ces canaux sont indispensables, à correctement sécuriser les usages restants et à favoriser autant que possible les canaux de paiement plus sécurisés (paiements sur internet, paiements sur un terminal de paiement, etc.) ;
- ensuite sur les paiements par internet, en invitant les commerçants à recourir systématiquement au protocole 3-D Secure pour les paiements effectués par internet autres que les MIT et à correctement sécuriser les paiements MIT par l'application d'une authentification forte à la signature du mandat et par la présentation d'une référence de chaînage valide pour les échéances rattachées à ce mandat.

Afin de favoriser le déploiement de ces recommandations, l'Observatoire avait recommandé l'application de limites de vélocité par les PSP émetteurs. Ainsi, ces derniers étaient invités à rejeter les paiements MOTO et les paiements CIT hors 3-D Secure, dès lors que le montant de la transaction aurait conduit au dépassement d'une limite de vélocité qui est calculée ainsi :

Vélocité = montant cumulé des achats / carte / commerçant / 24 heures

La conduite de ce plan de sécurisation des paiements par carte à distance a été confiée à un Comité de pilotage *ad-hoc* de l'Observatoire, réunissant sous l'égide de la Banque de France, les prestataires de services de paiement, les réseaux de paiement par carte, les prestataires d'acceptation techniques et les représentants des commerçants. En fonction des échanges et décisions du Comité de pilotage, ce plan de sécurisation a régulièrement été actualisé et publié en français et en anglais sur le site internet de l'Observatoire.

3.1.2 Déploiement des recommandations et indicateurs avancés d'impact

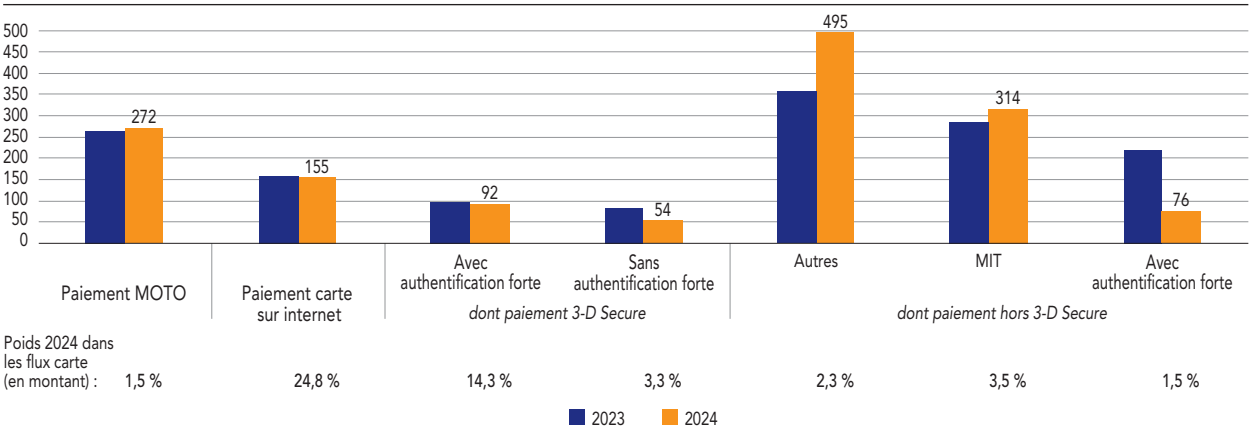
3.1.2.1 Analyse des statistiques 2024

Les statistiques de fraude 2024 confirment que les paiements par carte à distance restent beaucoup plus exposés à la fraude que les paiements de proximité et les retraits par carte. En effet, parmi les transactions par carte, si les paiements à distance ne représentent que 26 % des montants échangés, ils représentent 80 % des montants de fraude. Ces indicateurs justifient l'implication de l'Observatoire pour mieux sécuriser les paiements par carte à distance, en agissant au-delà des seules obligations réglementaires relatives à l'authentification forte.

Les statistiques de 2024 *(cf. graphique)*, qui comparent les taux de fraude des paiements par carte à distance selon les canaux et protocoles, confirment aussi l'analyse, qui avait conduit l'Observatoire à adopter ce plan de sécurisation en juin 2024.

Il y a d'une part, les canaux faiblement exposés à la fraude, principalement les paiements 3-D Secure, que ceux-ci fassent l'objet d'une authentification forte (*strong customer authentication*, SCA) ou non, ainsi que les paiements avec authentification forte mais sans le recours à 3-D Secure. Pour ces derniers, il s'agit des

Fraude sur les paiements par carte à distance (en euros pour 100 000 euros de paiement)



MIT, *merchant initiated transaction*, paiement initié par le commerçant ; MOTO, *mail order*, *telephone order*, paiements par courrier ou par téléphone.
Note : Le paiement MOTO est un paiement à distance hors internet (réalisé par courrier, postal ou électronique [courriel], ou par téléphone/télécopie).
Source : Observatoire de la sécurité des moyens de paiement.

paiements initiés au moyen de portefeuilles mobiles, où l'authentification forte se fait directement au niveau de l'application de paiement.

Il y a d'autre part, les canaux qui sont sensiblement plus exposés à la fraude, à savoir les paiements MOTO, les MIT et tous les autres paiements CIT sur internet qui ne recourent pas à 3-D Secure. Pour cette dernière catégorie, il s'agit des paiements pour lesquels l'exemption est gérée directement dans les flux d'autorisation (DTA) et des paiements internationaux dits *one-leg* où l'acquéreur est situé en dehors de l'espace économique européen (EEE). Le taux de fraude de ces différentes catégories est trois à cinq fois plus élevé que les autres paiements par carte à distance. Ainsi, en 2024, les paiements MOTO représentent encore 9,7 % des montants de fraude sur les paiements par carte à distance, contre seulement 5,8 % des flux.

À la lumière de ces statistiques, l'Observatoire cherche ainsi à mieux sécuriser les flux MOTO et MIT et à systématiser autant que possible le recours à 3-D Secure pour le reste des transactions CIT. Il est rappelé que les paiements internet hors 3-D Secure reconnus comme authentifiés fortement par le PSP émetteur, tels que les paiements effectués à l'aide d'un portefeuille mobile, ne sont pas couverts par le plan de l'Observatoire.

3.1.2.2 Les mesures mises en œuvre depuis juin 2024

Sur le volet des paiements MOTO, la limite de vélocité a été abaissée à 500 euros dès juin 2024, sauf pour une liste de secteurs limitativement énumérés. Toutefois, l'Observatoire a décidé de suspendre l'abaissement de la limite de vélocité qui était initialement prévue à 250 euros en septembre 2024, puis à 100 euros en octobre 2024. Plusieurs facteurs ont, en effet, plaidé en faveur d'une telle temporisation :

- premièrement, les transactions catégorisées comme MOTO mélangent à la fois des usages légitimes (une transaction à distance par téléphone ou courrier) et des usages illégitimes (une transaction par carte sur internet ou en proximité catégorisée à tort comme MOTO), et il est impossible pour le PSP émetteur de les distinguer avec certitude les uns des autres ;
- deuxièmement, les commerçants, qui acceptent aujourd'hui des paiements MOTO, ont besoin de temps pour déployer des parcours alternatifs et pour accompagner leurs clients (par exemple page internet, paiement par lien, sécurisation des données de la carte par saisie sur clavier ou équipement en terminaux) ;
- troisièmement, même si une expérimentation d'authentification forte des paiements initiés par téléphone (*telephone order*, TO) a été conduite à l'automne 2024, à l'initiative de Voxpay et de la Société Générale, confirmant la faisabilité de cette authentification, les commerçants ne peuvent pas encore y recourir, dans l'attente de sa mise en œuvre opérationnelle ;
- enfin, les données collectées par le Comité de pilotage auprès des professionnels des paiements, ont montré que les secteurs exemptés de la limite de vélocité, représentaient environ deux tiers des flux et de la fraude.

Par conséquent, deux décisions ont été prises. La première est de maintenir la limite de vélocité à 500 euros, en attendant qu'une solution d'authentification forte reposant sur le protocole 3-D Secure soit déployée et reconnue par les différents acteurs de la chaîne monétique. La seconde consiste à engager un dialogue avec une dizaine de commerçants prioritaires, appartenant à des secteurs exemptés de la limite de vélocité à 500 euros mais présentant une exposition à la fraude régulièrement supérieure à la moyenne de la Place. Sur la base de critères d'identification qui ont été intégrés au plan de l'Observatoire et publiés *(cf. annexe 4)*, neuf commerçants ont été ciblés par l'Observatoire. Parmi eux, six ont présenté un plan d'action en cours de déploiement, visant à limiter les flux MOTO au strict nécessaire par le déploiement de canaux de paiement alternatifs et à mieux sécuriser les flux restants ; les trois autres sont soumis à la limite de vélocité à 500 euros.

Sur le volet des paiements internet, la limite de vélocité sur les paiements par carte hors 3-D Secure a progressivement été abaissée, par paliers successifs de 500 euros en juin 2024 à 1,01 euro en mai 2025. 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. Toutefois, cette limite de vélocité a été étendue aux commerçants et acquéreurs situés au Royaume-Uni et en Suisse, dont les écosystèmes de paiement sont rôdés au protocole 3-D Secure. Pour les MIT, compte tenu des difficultés rencontrées pour établir un ensemble de règles communes pour identifier *a posteriori* les chaînages invalides, l'Observatoire a aussi proposé de procéder à l'identification de commerçants prioritaires sur la base de critères également intégrés au plan et publiés *(cf. annexe 4)*. Parmi les neuf commerçants identifiés, six ont mis en conformité leurs pratiques ou présenté un plan d'action pour mieux sécuriser leurs flux MIT ; pour les trois autres, les PSP émetteurs ont été autorisés à rejeter les demandes de renseignement à 0 euro dès lors que celles-ci servent à qualifier en MIT des transactions qui devraient être qualifiées de CIT et donc soumises aux règles d'authentification forte.

3.1.2.3 Les effets du plan de l'Observatoire sur les flux et la fraude

Si les premières mesures de l'Observatoire ont été déployées au second semestre 2024, la plupart des mesures susceptibles d'avoir un impact sur les flux et la fraude l'ont été en 2025, par exemple l'abaissement de la limite de vélocité sur les paiements sur internet hors 3-D Secure de 100 euros à 1,01 euro. Par conséquent, les statistiques de fraude portant sur l'ensemble de l'année 2024 ne permettent pas encore de mesurer pleinement les effets du plan de sécurisation. Pour orienter son plan d'action, le Comité de pilotage s'appuie en parallèle sur des données mensuelles collectées auprès des principaux PSP émetteurs et acquéreurs.

Toutefois, à la lumière de ces différents jeux de données, certaines tendances ont été amorcées en 2024 et devraient se poursuivre plus franchement en 2025.

- **L'Observatoire prend tout d'abord note d'une baisse des flux MOTO, qui est probablement sous-tendue par une plus forte promotion d'autres solutions de paiement (paiement sur internet, voire paiement de proximité).** Ces flux ont reculé de 6 % entre 2023 et 2024. Dans le même temps, les montants de fraude sur les flux MOTO n'ont baissé que de 4 % (40 millions d'euros de fraude en 2024), ce qui se traduit mécaniquement par une légère hausse du taux de fraude. Les indicateurs avancés, dont dispose le Comité de pilotage, laissent penser que cette baisse des flux MOTO devrait se poursuivre en 2025, avec cette fois-ci une baisse des taux de fraude afférents.
- **L'Observatoire relève ensuite, parmi les paiements sur internet, une érosion des canaux les moins sécurisés au bénéfice des canaux mieux sécurisés.** Si les MIT représentent 14 % des flux en montants en 2023 comme en 2024, les autres canaux moins sécurisés voient leurs poids légèrement reculer de 9,7 % à 9,3 %. À l'inverse, deux catégories progressent : d'une part, les paiements avec authentification forte au moyen d'un portefeuille mobile (6,1 % des flux en 2024, contre 1,9 % en 2023) et les paiements exemptés d'authentification forte dans 3-D Secure (13,2 % des flux en 2024, contre 12,4 % en 2024).
- **L'Observatoire se satisfait enfin de la poursuite de la baisse du taux de fraude sur les paiements par carte sur internet, qui passe de 0,160 % en 2023 à 0,155 % en 2024.** Cette baisse, certes modeste (– 3 %), est imputable à un plus fort recours aux canaux les plus sécurisés, et aussi à une amélioration sensible des taux de fraude sur ces mêmes canaux plus sécurisés. Ainsi, les paiements 3-D Secure qui sont exemptés d'authentification forte, présentent un taux de fraude historiquement bas de 0,054 %, contre 0,084 % en 2023. Cette baisse remarquable de 36 % illustre la forte amélioration des capacités de détection de la fraude par les systèmes de surveillance des transactions des acteurs monétiques, lorsque ceux-ci s'appuient sur 3-D Secure.

3.1.3 Nouvelles mesures pour 2025/2026

Pour continuer à renforcer la sécurité des paiements par carte à distance, l'Observatoire a décidé d'un certain nombre de mesures complémentaires, outre celles déjà actées par le Comité de pilotage dédié.

La force de ce plan de sécurisation repose sur la mise en œuvre coordonnée de mesures par l'ensemble des PSP émetteurs établis en France. Si ce plan est correctement mis en œuvre par les principaux PSP émetteurs français, l'Observatoire renouvelle son appel, auprès de l'ensemble des émetteurs établis en France, à correctement mettre en œuvre les recommandations relatives aux limites de vélocité.

3.1.3.1 Poursuite de la démarche de ciblage des commerçants à risque

L'Observatoire s'attachera à suivre jusqu'à leur terme les plans d'action soumis par les commerçants à risque identifiés début 2025 sur la base des données du deuxième semestre 2024 (commerçants dits « de la première vague »). En complément, l'Observatoire propose de conduire une deuxième vague d'identification de commerçants à risque sur la base des données du premier semestre 2025. Comme pour la première vague, l'identification sera mise en œuvre par les PSP émetteurs, qui appliqueront les critères de l'annexe 4 du plan de sécurisation publié par l'OSMP. Cette identification couvrira à nouveau les deux volets du plan, à savoir les paiements MOTO d'une part, et les paiements sur internet hors 3-D Secure d'autre part.

Début septembre 2025, le secrétariat de l'Observatoire demandera aux commerçants concernés par cette deuxième vague de lui soumettre un plan d'action d'ici fin octobre 2025.

3.1.3.2 Extension du plan de l'Observatoire aux paiements internationaux

Le plan de l'Observatoire excluait initialement de son périmètre les paiements internationaux, réalisés par des porteurs français auprès de commerçants situés en dehors de l'espace économique européen (EEE). En effet, s'ils ne sont pas établis dans l'EEE, leurs PSP acquéreurs

ne sont pas soumis aux exigences de la DSP 2 en matière d'authentification forte, et n'utilisent pas toujours les dernières versions du protocole 3-D Secure. Néanmoins ces paiements dits « *one leg* » (car seule la jambe « émission » de la transaction est située dans l'EEE) sont de plus en plus fraudés, impactant les porteurs français : s'ils ne représentent que 1 % des flux par internet en montant (en croissance de 12 % en 2024 par rapport à 2023), ils ont été à l'origine de près de 12 % des montants de fraude. Ce taux de fraude est exceptionnellement élevé à 1,96 %, soit un niveau treize fois supérieur au reste des paiements sur internet. Au regard de ces indicateurs, il est devenu impératif d'agir sur la sécurité des paiements internationaux par carte à distance.

C'est la raison pour laquelle, après avoir déjà étendu son plan aux paiements acceptés au Royaume-Uni et en Suisse, l'Observatoire propose de déployer son plan aux autres pays en dehors de l'EEE, par une approche progressive et débrayable.

Pour les pays qui manifestent une très bonne appropriation du protocole 3-D Secure (c'est-à-dire avec un taux d'utilisation pour plus de 80 % des transactions), il est proposé d'appliquer une limite de vélocité sur les paiements par internet hors 3-D Secure à 250 euros le 13 octobre 2025, puis 100 euros le 12 novembre 2025 et 30 euros le 12 janvier 2026.

Pour les pays qui manifestent une appropriation moyenne du protocole 3-D Secure (c'est-à-dire avec un taux d'utilisation compris entre 30 % et 80 % des transactions), il est proposé d'appliquer une limite de vélocité sur les paiements par internet hors 3-D Secure à 2 000 euros le 12 janvier 2026, puis 1 000 euros le 13 avril 2026 et 500 euros le 11 mai 2026.

Pour les pays qui ne sont, au contraire, pas expérimentés dans l'usage du protocole 3-D Secure (c'est-à-dire avec un taux d'utilisation dans moins de 30 % des transactions), l'Observatoire propose d'appliquer une limite de vélocité à 2 000 euros le 12 janvier 2026, puis 1 000 euros le 10 juin 2026 et 500 euros le 10 septembre 2026.

La catégorisation exacte des pays sera publiée sur le site internet de l'Observatoire dans le cadre d'une mise à jour du plan de sécurisation. Le Comité de pilotage garde à tout moment la capacité d'ajuster ce plan pour répondre aux enjeux de sécurité et de continuité de l'activité commerciale.

3.1.3.3 Poursuite du plan d'action sur les paiements MOTO

L'Observatoire renouvelle tout d'abord son appel à accélérer le développement d'une solution d'authentification des paiements initiés par téléphone *(cf. recommandation n° 5)*, en espérant que les déploiements techniques et commerciaux pourront être concrètement engagés en 2026. Une première expérimentation a été conduite à l'automne 2024, sous l'égide de la société Voxpay et de la Société Générale. Le Groupement cartes bancaires CB a mis en place un groupe de travail pour identifier une solution qui puisse être généralisée. En effet, des travaux sont encore nécessaires pour prendre en compte la diversité des solutions d'authentification forte proposées aux porteurs (notification sur application mobile, « SMS renforcé », etc.) et les standards doivent être ajustés pour que les transactions MOTO fortement authentifiées soient catégorisées et reconnues comme telles tout au long de la chaîne monétique.

Par ailleurs, il convient que l'écosystème monétique revoie la qualification de certains flux, qui sont improprement qualifiés de MOTO. L'Observatoire rappelle à cet effet que les paiements MOTO devraient être réservés aux paiements initiés auprès d'un centre d'appels ou par un bon de commande transmis par courrier ou courriel, pour lesquels le numéro de la carte est communiqué en dehors de tout canal électronique chiffré. Les situations où le numéro de la carte est communiqué par le biais de canaux électroniques sécurisés, comme, par exemple, les « cartes logées » et autres protocoles entre entreprises, ne devraient pas être qualifiées de MOTO, ni dans les systèmes d'information monétiques, ni dans les statistiques de l'OSMP.

Conformément à la recommandation n° 1 du plan de sécurisation, visant à limiter les paiements MOTO aux seuls cas d'usage où un autre mode de paiement n'est pas possible, **l'Observatoire rappelle certains principes essentiels, principalement à l'attention du secteur du tourisme et du voyage, aujourd'hui exempté de la limite de vélocité à 500 euros :**

- Tout paiement de proximité en présence du porteur (auprès de commerciaux itinérants, d'agences de voyages, d'hôtels, d'agences de location de voiture, etc.) doit se faire sur un terminal de paiement électronique ;
- À la fin d'une prestation de services, la régularisation et le règlement pour solde de tout compte (*checkout*) doit se faire : i) en proximité, sur le terminal de paiement (ou sur la solution intégrée au système de caisse) au moyen

d'une transaction techniquement liée à une autorisation sécurisée par une authentification forte sur le terminal de paiement (par exemple, solution PLBS – paiement pour la location de biens et services – dans l'écosystème Cartes bancaires CB) ; ii) à distance, au moyen d'une transaction de type MIT techniquement liée à une autorisation ou un mandat sécurisé par une authentification forte ;

- Les plateformes de réservation sur internet ne doivent pas recourir à la qualification MOTO : soit celles-ci assurent l'encaissement pour compte de tiers, en disposant des autorisations réglementaires adéquates, et les fonds sont reversés au bénéficiaire par virement ou par tout autre moyen de paiement (hôtel, loueur de voitures, etc.) ; soit celles-ci communiquent de façon sécurisée les données de la carte au bénéficiaire, qui initie la demande d'autorisation en la reliant à la demande d'authentification réalisée par la plateforme de réservation.

Prenant acte que deux tiers des flux et de la fraude sur les paiements MOTO appartiennent aujourd'hui à des secteurs exemptés de toute limite de vélocité, l'Observatoire mandate enfin le Comité de pilotage pour conduire progressivement une levée des exemptions sectorielles. Les exemptions actuelles concernent principalement les secteurs du voyage, du tourisme, des assurances et des biens de première nécessité (eau, gaz, télécommunications, etc.). **L'objectif est d'aboutir, à terme, à l'application d'une limite de vélocité à 500 euros pour l'ensemble des secteurs économiques d'ici fin 2026.** Seul le secteur de la vente sur catalogue continuerait de bénéficier d'une exemption, en l'absence de solution d'authentification pour les paiements par carte initiés sur support papier. Il est à noter que la procédure permettant des dérogations individuelles resterait valable, permettant ainsi à certains commerçants d'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)*. Les modalités seront définies par le Comité de pilotage et publiées sur le site internet de l'Observatoire. L'approche privilégiée serait de commencer avec des limites de vélocité plus élevées, par exemple 2 000 ou 4 000 euros, pour progressivement atteindre la limite fixée à 500 euros. De plus, l'approche privilégiée consiste à faire une distinction, parmi les secteurs exemptés, entre ceux exposant un panier moyen « faible » permettant d'appliquer plus rapidement la limite de vélocité à 500 euros et ceux avec un panier moyen « élevé », pour lesquels la transition vers 500 euros demandera plus de temps.

3.1.3.4 Poursuite du plan d'action sur les paiements internet hors 3-D Secure

La limite de vélocité sur les paiements internet hors 3-D Secure sera abaissé à 0,01 euro le 1er janvier 2026, contre 1,01 euro depuis le 12 mai 2025. Pour ce faire, les commerçants sont invités à bien vérifier la qualification de leurs demandes d'autorisation inférieures ou égales à 1 euro, afin de distinguer les cas d'usage des différents services utilisés (vérification de compte ou de carte, vérification de solde, pré-autorisation, mandat de MIT, etc.).

Le succès de ce plan suppose aussi que les PSP émetteurs assurent un niveau suffisant d'acceptation des demandes d'exemption sollicitées par les commerçants dans 3-D Secure au titre du faible niveau de risque de la transaction (exemptions dites « TRA acquéreur » [2]). En effet, dans le cadre de cette exemption, le commerçant assume le cas échéant, sous la responsabilité de son PSP, le préjudice de la fraude. Même si le PSP émetteur reste à tout moment libre de requérir l'application d'une authentification forte en raison des risques encourus, l'Observatoire veillera à ce que les standards d'acceptation au titre de la TRA acquéreur soient globalement homogènes au sein de la Place.

Les PSP émetteurs soulignent que le plan de sécurisation de l'OSMP a permis une amélioration substantielle du niveau de conformité des MIT, qui présentent de plus en plus des références de chaînage valide. Une tolérance dite de « *grandfathering* » pouvait encore exister jusqu'à fin 2024 pour les MIT, dont les mandats avaient été signés par les consommateurs à une date antérieure à la mise en place des règles de la DSP 2 en matière d'authentification forte (officiellement le 14 septembre 2019). En parallèle, les innovations des systèmes monétiques permettent désormais de poursuivre le mandat de MIT au moment du renouvellement de la carte, sans aucune action de la part du consommateur. Conformément à la recommandation n° 2 de son plan de sécurisation, l'Observatoire demande aux commerçants de poursuivre la mise en conformité de leurs MIT, ce qui suppose parfois de demander aux consommateurs de confirmer le mandat avec une authentification forte, si ça n'avait pas été le cas la première fois.

Malgré cette amélioration de la conformité, l'Observatoire note que le taux de fraude des paiements MIT, qui sont initiés par le commerçant, reste structurellement trois fois plus élevé que le taux de fraude des transactions CIT, initiées par le consommateur (0,314 % pour les MIT, contre 0,092 % pour les paiements 3-D Secure avec authentification forte). Portés par la croissance de l'économie numérique, les MIT sont notamment présents dans les situations de paiement d'abonnement, de paiement échelonné, de paiement lié à une réservation, ou encore de paiement

au moyen d'une solution de paiement électronique tierce. Les échanges avec les commerçants à risque, qui ont soumis un plan d'action, ont révélé qu'une part significative de cette fraude pouvait être due à des litiges commerciaux : par exemple, contestant avoir souscrit un abonnement, les consommateurs signalent les transactions comme frauduleuses auprès de leur PSP. Ces transactions n'ayant pas fait l'objet d'une authentification forte, ces derniers remboursent généralement leurs clients après avoir émis une demande de rétrofacturation (*chargeback*) auprès du commerçant concerné.

Par conséquent, l'Observatoire souhaite compléter son plan d'action d'une nouvelle recommandation visant à mieux sécuriser ces MIT, tant vis-à-vis de la fraude que des litiges commerciaux, de façon à mieux protéger le consommateur dans ces nouveaux usages.

Nouvelle recommandation : Sécurisation des MIT
(*merchant initiated transaction*, paiement initié par le commerçant)

L'authentification forte systématique, sans aucune exemption possible, pour la signature des mandats de MIT est une exigence réglementaire rappelée par l'Autorité bancaire européenne (Q&A, *Question and Answer*, n° 4031 publiée le 1er mars 2019).

En complément, et dans l'optique de toujours mieux sécuriser les MIT, l'Observatoire appelle les acteurs de l'écosystème monétique à renforcer la transparence des mandats de MIT dans les fenêtres d'authentification 3-D Secure. Au moment de s'authentifier fortement, les termes du mandat devraient être clairement formalisés et rappelés au consommateur (montant, fréquence, échéance bénéficiaire, services associés, etc.).

En parallèle, les PSP émetteurs sont invités, dans la mesure du possible, à fournir à leurs clients des outils de gestion des mandats de MIT, par exemple par la fourniture d'un tableau de bord permettant d'identifier les mandats de MIT en cours et, le cas échéant, de les contester ou de les résilier.

Enfin, dès lors qu'ils disposent de la preuve de la signature du mandat par authentification forte, les PSP émetteurs sont invités à mieux distinguer les fraudes des litiges commerciaux dans le traitement des contestations comme dans les reportings réglementaires sur la fraude aux moyens de paiement.

3.2 Sécurisation des communications et coopération avec les acteurs des télécommunications et du numérique

3.2.1 Contexte

À la suite de la mise en place de l'authentification forte et des mécanismes de mesure du risque des transactions (*scoring*), impulsée par la deuxième directive européenne sur les services de paiement (DSP 2), les fraudeurs se sont adaptés en déployant des techniques d'attaque par manipulation. C'est le cas de la fraude au faux conseiller bancaire, qui consiste soit à faire valider les opérations frauduleuses par les victimes elles-mêmes, soit à ce que les fraudeurs s'approprient les outils d'authentification forte pour réaliser directement des opérations frauduleuses. Ces manipulations passent souvent par une interaction directe, au téléphone ou sur les applications de messagerie, entre les fraudeurs et leurs victimes.

De surcroît, les réseaux criminels ont aussi de plus en plus recours aux outils d'intelligence artificielle, qui leur permettent d'industrialiser leurs attaques tout en les rendant plus crédibles. Les technologies d'intelligence artificielle facilitent différentes techniques utilisées par les fraudeurs : falsification documentaire, manipulation de voix ou d'image, traduction automatique des messages dans la langue de la victime, clonage de sites ou d'applications, etc. L'intelligence artificielle vient ainsi enrichir des techniques de fraude, qui sont apparues depuis plusieurs années mais qui voient leur potentiel de nuisance renforcé. Il est en ainsi de :

- l'envoi ou la diffusion de communications (SMS, messages échangés via des applications de messagerie instantanée, réseaux sociaux, etc.) usurpant l'identité de l'expéditeur (*phishing* ou *smishing*, c'est-à-dire hameçonnage) ou la création de sites ou d'applications miroirs, afin de collecter les données personnelles des clients ;
- l'usurpation de numéros d'appelants (*spoofing*) permettant de tromper le destinataire sur l'origine des appels reçus (par exemple, en affichant le numéro du conseiller bancaire, du standard de la banque ou de son service de mise en opposition des cartes) ;
- le détournement de la ligne téléphonique de la victime, au moyen de la duplication de sa carte SIM (*SIM swapping*) ou en faisant une demande de changement d'opérateur (après avoir obtenu le relevé d'identité opérateur, RIO) qui permet au fraudeur de recevoir sur son téléphone à la place de la victime les informations et demandes d'authentification ;

2 TRA – *Transaction Risk Analysis*, analyse de risque des transactions.

- le détournement et le piratage des messageries électroniques de particuliers ou de professionnels, permettant au fraudeur d'usurper leur identité et d'envoyer par exemple de fausses coordonnées bancaires à l'occasion d'une transaction en cours ;
- la multiplicité des cas de fuite de données impliquant des sociétés grand public et permettant aux acteurs malveillants de cibler leurs victimes et de crédibiliser leurs scénarios d'attaque grâce aux informations personnelles collectées ;
- les annonces ou publicités frauduleuses sur internet et les réseaux sociaux, parfois relayées par des intermédiaires rémunérés, comme les influenceurs, qui permettent de récupérer les données personnelles du client et potentiellement de l'amener vers une escroquerie.

Dans ce contexte de fort renouvellement de la fraude par manipulation, l'Observatoire s'est attaché à renforcer sa coopération avec les acteurs des télécommunications et du numérique, y compris les réseaux sociaux et les fournisseurs de terminaux mobiles. À chaque fois, l'Observatoire a associé les différentes autorités concernées : Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF). Le groupe de travail constitué en 2023 a ainsi poursuivi son action en 2024.

3.2.2 Les actions possibles du côté des prestataires de services de paiement

Pour lutter contre les fraudes par manipulation, les prestataires de services de paiement disposent de certains leviers qu'ils peuvent mobiliser, dès lors qu'ils ne dépendent pas de tiers. Outre les actions de prévention et de sensibilisation des clients aux risques de fraude qui se sont multipliées depuis deux ans, l'Observatoire a pris connaissance de plusieurs initiatives intéressantes qui consistent à :

- 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° 1 :

Afin de lutter contre les fraudes par manipulation, les prestataires de services de paiement 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.

3.2.3 La coopération avec les opérateurs de télécommunications

3.2.3.1 La lutte contre le *spoofing* : le programme MAN et les mesures complémentaires

La lutte contre le *spoofing* repose d'abord sur le mécanisme d'authentification des numéros (MAN), déployé par l'Association des plateformes de normalisation des flux interopérateurs (APNF) qui réunit les opérateurs attributeurs de numéros provenant du plan de numérotation national. Ce mécanisme vise à appliquer les dispositions du IV de l'article L. 44 du Code des postes et des communications électroniques issues de la loi dite « Naegelen »[3]. Le MAN comporte deux volets :

- D'une part, une infrastructure technique permettant aux opérateurs téléphoniques d'authentifier les appels téléphoniques. La mise en place de l'infrastructure et le raccordement de la très grande majorité des opérateurs se sont achevés en juin 2024. L'authentification consiste à garantir, à l'aide d'un certificat électronique, que l'appel provient bien de la ligne associée au numéro présenté comme numéro appelant.

- D'autre part, l'interruption de l'acheminement (c'est-à-dire la coupure) des appels qui ne sont pas correctement authentifiés. Les appels émis présentant des numéros fixes sans être authentifiés sont coupés depuis le 1er octobre 2024. Les appels émis présentant des numéros mobiles sans être authentifiés sont coupés depuis fin janvier 2025.

En pratique, d'après la Fédération française des télécoms, 98,17 % des numéros fixes attribués sont couverts par au moins un certificat MAN, ce qui signifie que quasiment tous les opérateurs sont raccordés au système. Dans le même temps, toujours d'après les professionnels du secteur des télécommunications, environ 0,03 % des appels sont coupés par le MAN en raison de l'absence ou de l'invalidité du certificat.

Il convient toutefois de rappeler certaines limitations du MAN :

- Les appels téléphoniques passant par le réseau téléphonique commuté (RTC) ne peuvent pas être raccordés à l'infrastructure technique, même s'il faut rappeler qu'il s'agit d'un réseau de communication en voie d'extinction, progressivement remplacé par la fibre ;
- Les appels téléphoniques passés depuis l'étranger et présentant un numéro de téléphone mobile (appels en itinérance ou *roaming*) ne sont pas non plus couverts par le MAN. En revanche, les appels en provenance de l'étranger et émis avec un numéro fixe français sont coupés ;
- Enfin et surtout, l'efficacité du dispositif repose sur la bonne certification des appels par les opérateurs téléphoniques.

L'Observatoire a été informé de certains cas de *spoofing*, y compris sur des numéros de téléphone fixe, qui se seraient concrétisés en 2025 après le déploiement du MAN. Ces cas sont en cours d'investigation par le secteur des télécommunications et l'Arcep.

Si le contrôle du respect de la loi Naegelen relève de la mission de l'Arcep, les conséquences du *spoofing* sur la fraude aux moyens de paiement sont du ressort de l'Observatoire. En conséquence, l'Observatoire surveille la bonne mise en œuvre de la loi et mesure ses effets sur les fraudes reposant sur une usurpation du numéro de téléphone. L'objectif du MAN est notamment d'assurer la traçabilité de l'ensemble des appels et de permettre aux autorités compétentes de remonter, en cas de besoin, à l'opérateur d'origine des appels, qu'ils soient légitimes ou frauduleux. Le MAN mobilise donc dès à présent les opérateurs pour garantir l'authenticité des numéros que leurs clients présentent aux destinataires des appels.

Dans ce cadre, afin d'assurer la pleine efficacité opérationnelle du MAN, des réflexions sont en cours avec l'ensemble des acteurs pour accompagner la montée en charge du dispositif, renforcer les procédures de vérification des appels et faciliter l'analyse des signalements.

En parallèle du programme MAN, les prestataires de services de paiement sont invités à protéger leurs numéros particulièrement exposés, tels que les numéros des centres d'opposition aux cartes bancaires perdues ou volées ou les numéros des centres de lutte contre la fraude. L'Observatoire appelle dans ce cadre les établissements à :

- participer à une expérimentation d'un mécanisme dit « *Do Not Originate* » (DNO), qui consisterait, pour les opérateurs téléphoniques, à bloquer les appels émis depuis un numéro identifié comme exclusivement destiné à recevoir des appels, après en avoir reçu la liste par les PSP ;
- lancer une réflexion sur l'instauration d'un numéro d'appel unique, à l'instar du n° 159 au Royaume-Uni, qui permettrait aux consommateurs d'être mis en relation avec leur PSP en cas de soupçon de fraude.

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 à partir de 2026 un mécanisme de protection de ces numéros particulièrement exposés au *spoofing*.

Recommandation n° 3 :

L'Observatoire appelle les PSP et les acteurs de télécommunication à étudier l'opportunité de mettre en place un numéro unique permettant de joindre les services antifraude 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.

3 Article 10 de la loi n° 2020-901 du 24 juillet 2020 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux.

3.2.3.2 La lutte contre le *smishing* : la protection des OAdC (*Originator Address Codes*, identifiants d'émetteur de SMS)

Le *smishing* (ou hameçonnage par SMS, contraction de « SMS » et « *phishing* »), utilisé pour rediriger les clients vers de faux sites ou faux numéros d'appel, est rendu d'autant plus efficace lorsque i) le SMS frauduleux mentionne comme expéditeur un OAdC, c'est-à-dire un libellé comportant 11 caractères alphanumériques plutôt qu'un numéro débutant par 06 ou 07, et que ii) cet OAdC laisse entendre au destinataire du SMS que ce dernier provient d'un expéditeur légitime (banque, service public, etc.), à l'instar du *spoofing*. L'AF2M [4] a mis en place, en lien avec les prestataires assurant l'acheminement des SMS, un mécanisme de protection des OAdC, par la gestion de deux listes :

- OAdC sensibles (ou interdits sauf autorisation) : l'usage de ces OAdC correspondant à des marques, entreprises ou services publics existants est réservé à leur détenteur légitime. Ces OAdC ne doivent être utilisés qu'avec l'autorisation de ce détenteur.
- OAdC strictement interdits : l'usage de ces OAdC pouvant susciter une confusion avec une marque, une entreprise ou un service public existants est interdit. À ce titre, l'AF2M a établi une liste noire des OAdC présentant une proximité trompeuse avec les OAdC sensibles, et pour lesquels l'émission de SMS doit être bloquée par les opérateurs.

La liste des OAdC sensibles et celle des OAdC interdits sont mises à jour de manière régulière, notamment sur la base des signalements envoyés par les particuliers au 33700 (plateforme nationale de déclaration des SMS non sollicités mise en place par l'AF2M), de façon à renforcer constamment l'efficacité générale du dispositif. Le mécanisme de protection des OAdC étant déjà opérationnel, l'action de l'Observatoire cherche essentiellement à valoriser la notoriété du 33700 auprès des professionnels des paiements, des entreprises, des administrations et du grand public.

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 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.

3.2.3.3 La lutte contre le *SIM swapping* : le recours à l'API multi-opérateurs « *SIM Verify* »

Afin de prévenir les conséquences du *SIM swapping* sur les titulaires des lignes, les opérateurs proposent une interface de programmation d'application (API, *application programming interface*) appelée « *SIM Verify* ». Elle permet de savoir si une carte SIM a récemment été renouvelée sur une ligne téléphonique donnée. Cette API est multi-opérateurs et couvre désormais la quasi-totalité des lignes mobiles françaises. La consultation de cette API peut ainsi être intégrée dans les outils de détection et de prévention de la fraude des PSP, notamment pour certaines opérations sensibles reposant encore sur le SMS (par exemple, l'authentification forte où le SMS est couplé à un autre facteur ou l'enrôlement dans une nouvelle solution d'authentification forte). Cette démarche est particulièrement pertinente en cas de transaction identifiée comme à risque et pour laquelle une réémission récente de carte SIM est un facteur aggravant qui peut justifier un rejet de l'opération par le PSP. Lors d'échanges intervenus dans le cadre de l'Observatoire, plusieurs PSP ont partagé leur retour d'expérience très positif sur l'efficacité de cet outil pour la prévention en temps réel de la fraude avec les opérateurs et l'AF2M. Des pistes d'enrichissement de l'API ont été soumises pour examen à l'AF2M (par exemple, communication du lieu ou de l'horodatage de réémission de la carte SIM, ou encore prise en compte des portabilités entre opérateurs).

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'API 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.

3.2.3.4 Nouveaux axes de réflexion

Les échanges organisés sous l'égide de l'Observatoire permettent d'identifier en permanence de nouveaux défis et opportunités en matière de sécurisation des communications.

- **L'un de ces défis porte sur le déploiement progressif des RCS (*Rich Communication Service*, service de communication enrichi),** qui est un protocole de communication universel créé par la GSMA, l'association mondiale des opérateurs de téléphonie mobile, qui pourrait progressivement se substituer aux SMS. Les RCS existent sous un format standard pour la communication entre

personnes (RCS) et sous un format augmenté dédié à la communication des professionnels (RBM, *RCS Business Messaging*). Dans le cadre du RBM, les professionnels sont plus facilement identifiés par leur marque et leur logo et les destinataires peuvent interagir par le biais de boutons d'action (par exemple, « aller en boutique », « nous contacter » ou « bénéficier de l'offre »). Ce nouveau protocole permet d'importer dans toutes les messageries téléphoniques les standards de communication utilisés dans les applications propriétaires de messageries (par exemple Messenger, WhatsApp, Signal, Telegram, etc.). Dans la mesure où ce protocole est désormais déployé à la fois sur Androïd et sur Apple (à fin 2024, 48 % du marché français des *smartphones* était déjà compatible), les PSP doivent s'intéresser à la sécurisation de leurs communications par RCS, notamment pour y protéger rigoureusement leurs marque et logo. L'Observatoire appelle, dans le même temps, les agrégateurs et les opérateurs téléphoniques à sécuriser leurs processus de façon à empêcher l'usurpation d'identité d'une banque dans les communications par RCS.

- **Un autre de ces défis porte sur la forte augmentation des appels non sollicités, avec des numéros inconnus, sur les téléphones portables.** Pour les utilisateurs, dans ce flot d'appels, il est difficile d'identifier un appel légitime de son PSP. Des solutions propriétaires, disponibles sur certains téléphones ou chez certains opérateurs, peuvent être souscrites par les utilisateurs pour mieux filtrer ces appels (Anti-spam appels d'Orange, Hiya, etc.). En parallèle, les législateurs ont souhaité encadrer de plus en plus rigoureusement le démarchage téléphonique (loi Hamon de 2014 qui a introduit le dispositif Bloctel, loi Naegelen de 2020 et la récente loi Cazenave, adoptée en mai 2025). L'Observatoire sera intéressé par les effets de ces lois sur l'activité des fraudeurs. Toutefois, il semble encore manquer un dispositif efficace de signalement des numéros de téléphone, soupçonnés d'être utilisés par des escrocs, qui serait l'équivalent du 33700 pour les SMS. En effet, un tel dispositif permettrait aux opérateurs téléphoniques et autorités publiques de mener leurs investigations et leurs contrôles sur ces lignes.
- **Le dernier de ces défis porte sur la lutte contre les publicités frauduleuses.** Présentes sur internet et les réseaux sociaux, celles-ci renvoient vers des sites frauduleux, imitant souvent celui de commerçants ou d'administrations légitimes, sur lesquels les victimes vont fournir des données personnelles et sensibles. Des outils de filtrage sont intégrés sur certains navigateurs ou fournis avec des solutions de sécurité payantes. En parallèle, la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) prévoit la mise en place d'un filtre de cybersécurité anti-arnaque à destination du grand public. L'Observatoire suivra le déploiement de ce dispositif et, en fonction de son efficacité, le valorisera dans ses communications auprès du grand public.

3.2.4 Une feuille de route pour renforcer la coopération avec les acteurs du numérique

Si les escrocs continuent d'utiliser les canaux traditionnels de communication (téléphone, SMS, etc.), l'Observatoire est aussi conscient que les fraudeurs sont tout aussi actifs sur internet, les réseaux sociaux et les messageries propriétaires. C'est la raison pour laquelle l'Observatoire souhaite désormais accentuer sa coopération avec les acteurs du numérique, à l'image de ce qu'il a engagé depuis 2023 avec le secteur des télécommunications.

Deux autorités sont particulièrement engagées dans la régulation des services numériques en France, à savoir l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et la direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF). L'Arcom a notamment été désignée en France comme l'autorité indépendante chargée de coordonner la mise en œuvre du règlement européen sur les services numériques (DSA, *Digital Services Act*, règlement (UE) 2022/2065).

À l'image de ce qui a pu être fait au Royaume-Uni pour mieux lutter contre les escroqueries, avec l'association professionnelle *Stop Scams UK* qui réunit le secteur bancaire, le secteur des télécommunications et le secteur du numérique, l'Observatoire cherchera à entamer une coopération avec les grands acteurs du numérique, tels que Google, Meta, Apple ou encore TikTok, pour mieux lutter contre les fraudes bancaires.

Cette coopération cherchera, entre autres, à progresser autour de **quatre axes** :

1. **L'échange d'informations entre les acteurs du numérique et les prestataires de services de paiement**
   À l'instar du programme FIRE au Royaume-Uni (*Fraud Intelligence Recriprocal Exchange*) entre les acteurs bancaires et Meta, il s'agit de structurer un canal efficace d'échanges d'informations relatives à l'activité des fraudeurs. Celui-ci pourrait notamment permettre aux PSP français de signaler aux acteurs

4 L'Association française pour le développement des services et usages multimédias multi-opérateurs représente le secteur des télécoms au sein de l'Observatoire depuis la création de ce dernier.

du numérique, y compris par le mécanisme prévu à l'article 16 du DSA, 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 [5] 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 [6].

Par ailleurs, pour les très grandes plateformes en ligne désignées par la Commission européenne, l'ensemble des informations susceptibles de leur être remontées, en particulier par les PSP, pourraient les amener à mieux évaluer les 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.

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 téléphone. Ceux-ci coexistent avec la plateforme de déclaration 33700 mise en place par l'AF2M, sans que ceux-ci ne communiquent entre eux.

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 ou Telegram). Or, en l'absence de procédures de vérification d'identité et de connaissance client, aussi poussées que dans le secteur financier, les fraudeurs parviennent aisément à i) usurper l'identité des PSP sur ces applications numériques, par exemple en affichant le logo d'un établissement bancaire comme image de profil, ou ii) 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.

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.

   Certaines plateformes en ligne ont développé des outils de protection de droit des marques, comme le *Brand rights protection* (Protection des droits de la marque) mis à disposition par Meta. Ils permettent aux marques de protéger leur propriété intellectuelle en signalant la contrefaçon, le non-respect d'une marque déposée ou de droits d'auteur, ou encore l'usurpation d'identité des contenus, afin que ceux-ci soient retirés.

   À cet égard, il pourra être demandé aux plateformes de prendre en compte, dans le traitement des éventuels signalements faits par des PSP, les listes noires de l'ACPR et de l'AMF, et de leurs équivalents européens, ou des autres listes noires mises en place par des autorités publiques, afin de retirer les contenus, liens ou références en ligne vers des sites identifiés sur ces listes [7].

Recommandation n° 6 :

À l'instar de l'initiative *Stop Scams* au Royaume-Uni, l'Observatoire appelle les acteurs du numérique, les acteurs des télécommunications et les professionnels du paiement à réfléchir à une structuration durable de la gouvernance de leur coopération de façon à lutter plus efficacement contre les fraudes au paiement et plus largement contre les escroqueries financières.

3.3 Utilisation de la carte de paiement pour l'accès aux sites pornographiques

Des initiatives juridiques ont vu le jour en France et dans l'Union européenne pour renforcer la protection des mineurs en ligne, notamment face aux contenus pornographiques. En France, en application d'un cadre réglementaire renouvelé en mai 2024, l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) avait autorisé à titre exceptionnel et temporaire le recours à des systèmes de « vérification de l'âge » reposant sur la carte de paiement pour intégrer de la friction dans l'accès aux sites et ainsi limiter l'accès à ces sites aux mineurs.

L'Observatoire a mis en place une cellule de veille dédiée dans le cadre de ce dispositif temporaire, en lien avec l'Arcom et l'ensemble des acteurs concernés, qui s'inscrit dans le cadre de ses travaux de prévention de la fraude à la carte.

3.3.1 Évolutions législatives et réglementaires en France et en Europe

La protection des mineurs constitue un enjeu primordial de société. En France, l'exposition des mineurs à la pornographie est proscrite par le Code pénal depuis 1994 [8]. Or les sites diffusant des contenus à caractère pornographique restent consultés par de nombreux mineurs. La France a sensiblement renforcé son arsenal juridique ces dernières années. La loi précise depuis 2020 que les sites pornographiques ne peuvent pas se contenter d'une simple déclaration de majorité de la part d'un utilisateur, consacrant ainsi une jurisprudence ancienne. En 2024, la loi visant à sécuriser et à réguler l'espace numérique [9] a renforcé les pouvoirs de l'Arcom pour faire appliquer cette disposition. L'Arcom dispose ainsi de pouvoirs de sanction pécuniaire, de blocage et de déréférencement administratifs des sites pornographiques laissés accessibles aux mineurs, en infraction avec le droit pénal français. Les sites concernés sont ceux établis en France, en dehors de l'Union européenne, ainsi que ceux situés dans l'Union européenne identifiés par un arrêté ministériel [10].

Les sites pornographiques doivent mettre en œuvre un système de vérification de l'âge de leurs utilisateurs pour s'assurer qu'ils sont majeurs. L'Arcom a élaboré, avec l'appui de la Commission nationale de l'informatique et des libertés (CNIL), un référentiel technique [11] qui définit des exigences minimales à respecter pour les systèmes de vérification d'âge. Ce référentiel, entré en application le 11 janvier 2025, autorisait, à titre dérogatoire pour une période de trois mois, l'utilisation de la carte de paiement pour empêcher les mineurs d'accéder à ces sites. Celle-ci prenait la forme d'un micro-paiement avec authentification renforcée ou d'une simple authentification renforcée, effectuée par un tiers de confiance, tel qu'un prestataire de services de paiement. Seules les plateformes pornographiques établies en France ou en dehors de l'Union européenne, qui sont soumises au référentiel depuis le 11 janvier 2025, ont pu bénéficier de cette tolérance jusqu'au 11 avril 2025 [12].

La tolérance temporaire de l'utilisation de la carte bancaire à des fins de friction dans l'accès aux sites visait essentiellement à accommoder un délai de mise en conformité pour contracter avec les différents fournisseurs de solution de vérification de l'âge, avec une solution technique (le paiement en ligne) devenue une commodité facilement mobilisable et protectrice de la vie privée. Le recours à la carte de paiement permettait de créer de la friction pour tous les visiteurs de ces sites et protéger les mineurs les plus jeunes qui ne disposeraient pas encore de carte ou dissuader l'accès de ceux qui en disposeraient. Depuis le 12 avril 2025, les sites pornographiques ne sont plus autorisés à proposer cette méthode et doivent s'appuyer sur des systèmes de vérification d'âge qui présentent les garanties prévues par le référentiel précité de l'Arcom en matière de fiabilité et de protection de la vie privée.

5 À noter que la suspension de l'accès à une plateforme en ligne est encadrée à l'article 23 du DSA, qui prévoit cette possibilité « *pendant une période raisonnable et après avoir émis un avertissement préalable* », pour les utilisateurs qui « *fournissent fréquemment des contenus manifestement illicites* ».

6 Article 16 (3°) du DSA. Le DSA ne crée pas de motifs d'illicéité de contenus. Il se rapporte au droit existant en définissant le contenu illicite comme tout contenu non conforme au droit de l'Union ou au droit d'un État membre.

7 Dans une décision du 24 avril 2024, le tribunal judiciaire de Paris a souligné que, dans le cadre du DSA, les très grandes plateformes en ligne ont « *l'obligation d'évaluer tout risque systémique, ce qui inclut la diffusion de contenus contrefaisants par l'intermédiaire de leurs services* », et que les « *mesures d'adaptation peuvent consister en l'adaptation des systèmes de publicité et l'adoption de mesures ciblées destinées à limiter la présentation de publicités* » illégales ou contraires aux conditions d'utilisation de la plateforme en ligne. En l'espèce, le juge souligne que les standards publicitaires de Meta indiquent qu'une technologie automatisée examine les publicités avant leur diffusion en ligne. Dans ce cadre, le tribunal a enjoint à Meta de « *filtrer* » et empêcher la diffusion sur Facebook, Instagram et Messenger, des publicités diffusées par des annonceurs n'ayant pas de compte authentifié et qui reproduisent, dans le texte ou l'image, les marques Barrière (Tribunal judiciaire de Paris, 3ème chambre, 3ème section, 24 avr. 2024, Groupe Lucien Barrière / Meta ; cf. aussi, dans la même affaire : Tribunal judiciaire de Paris, 10 sept. 2024).

8 Article 227-24 du Code pénal, qui prenait la suite de l'ancienne incrimination de l'outrage aux bonnes mœurs.

9 Loi du 11 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN, sécuriser et réguler l'espace numérique).

10 Cf. l'arrêté du 26 février 2025 désignant les services de communication au public en ligne et les services de plateforme de partage de vidéos établis dans un autre État membre de l'Union européenne soumis aux articles 10 et 10-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique | Légifrance.

11 Cf. Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne | Arcom.

12 Les plateformes pornographiques établies dans d'autres États membres de l'UE et désignées par l'arrêté mentionné dans l'appel de note n° 3, ne sont assujetties au référentiel que depuis le 7 juin 2025.

Au niveau européen, le règlement sur les services numériques [13] prévoit de renforcer la protection des mineurs sur toutes les plateformes en ligne accessibles aux mineurs (article 28). Les lignes directrices de la Commission européenne en la matière, qui ont été publiées le 14 juillet 2025, précisent les exigences notamment en matière de vérification de l'âge. À l'instar de toutes les « très grandes plateformes en ligne » désignées de plus de 45 millions d'utilisateurs mensuels dans l'Union, les sites pornographiques sont soumis à des obligations plus strictes, et directement supervisées au niveau européen par la Commission (articles 34 et 35). À partir de 2026, avec l'entrée en application du règlement eIDAS v2 [14], le portefeuille européen d'identité numérique pourra être utilisé sur les très grandes plateformes, y compris pornographiques, pour prouver sa majorité. Dans l'attente de la disponibilité de ces solutions, la Commission a attribué un marché public pour développer une solution temporaire (le « *mini wallet* », un portefeuille à périmètre réduit), qui sera mise à disposition des États membres, afin que ces derniers la déclinent au niveau national.

3.3.2 Activités de la cellule de veille

La cellule de veille dédiée de l'Observatoire a été chargée de suivre le déploiement, par les sites pornographiques, de l'utilisation de la carte de paiement comme mesure d'accès durant la période temporaire de trois mois et d'évaluer en parallèle l'incidence sur la fraude à la carte. La cellule a réuni la Banque de France, l'Arcom, des représentants de la Gendarmerie nationale, de Cybermalveillance, des principaux groupes bancaires français, de la Fédération bancaire française et des réseaux de paiement par carte, et a dressé plusieurs constats.

- **D'une part, l'Arcom a constaté qu'un faible nombre de systèmes de vérification d'âge a été déployé sur les sites pornographiques concernés durant la période temporaire**, quelle que soit leur nature (par exemple au travers d'une authentification renforcée liée à la carte de paiement, d'un selfie, par e-mail, avec un ticket chez le buraliste ou un portefeuille électronique). Lorsque des solutions de vérification d'âge étaient proposées, l'option de vérification par la carte de paiement était souvent payante, ce qui a conduit à un très faible niveau d'utilisation.
- **D'autre part, l'Arcom a adressé des lettres d'observation à cinq éditeurs de contenus pornographiques qui n'avaient pas mis en place de système de vérification de l'âge**, puis des mises en demeure à deux d'entre eux qui étaient restés en situation de manquement. L'ensemble de ces services a mis en place un système à la suite de ces interventions de l'Arcom. Ceux qui avaient mis en place un système de vérification assis sur la carte l'ont retiré. Depuis le 12 avril 2025, à la connaissance de l'Arcom, plus aucun site pornographique n'admet la carte de paiement comme outil de friction pour l'accès aux sites. À noter que d'autres services qui n'ont pas reçu de courrier de l'Arcom, et qui sont établis dans d'autres États membres, ont indiqué début juin 2025 dans la presse leur intention de se rendre volontairement inaccessibles en France ou ont mis en place des sites miroirs [15] (pour, dans ce dernier cas, contourner des décisions de blocage du juge judiciaire dans le cadre de procédures distinctes de celles de l'Arcom).
- Enfin, les effets du dispositif sur la fraude à la carte sont restés limités. Les participants de la Cellule de veille n'ont pas remonté de signaux d'alerte particuliers sur la période. Les risques surveillés par la cellule portaient sur la compromission de données de carte et les campagnes d'hameçonnage qui auraient pu utiliser le référentiel comme prétexte pour collecter des données de carte et revendre les empreintes de carte collectées. Des campagnes d'hameçonnage peuvent toutefois être conduites *a posteriori*, ce qui appelle à maintenir une certaine vigilance. Par ailleurs, très peu d'informations relatives à l'usage des sites pornographiques sont partagées par les utilisateurs à des tiers, en particulier à leur banque, ce qui peut contribuer à la sous-déclaration des cas de fraude sur les sites pornographiques par les clients victimes.

3.3.3 Une coopération interinstitutionnelle pour le développement des services de confiance en ligne

La mise en place du référentiel de l'Arcom a permis de renforcer la coopération interinstitutionnelle entre les pouvoirs publics, notamment la Banque de France, l'Arcom et la Direction interministérielle du numérique (Dinum), sur les enjeux de sécurité des moyens de paiement, de l'utilisation et de la finalité des cartes et de l'authentification forte. Cela confirme les besoins à court et moyen terme de développer et promouvoir des services de confiance, techniquement fiables et adaptés aux usages, qui permettent de vérifier des attributs d'identité tels que l'âge. La protection des mineurs à l'égard des contenus pornographiques constitue ainsi un excellent vecteur de développement des solutions d'identité numérique, que l'OSMP appelait de ses vœux dans le cadre de son étude de veille sur l'identité numérique et la sécurité des paiements *(cf. rapport annuel de 2021)*.

3.4 Le suivi des actions et recommandations de l'Observatoire contre la fraude au chèque

Les recommandations de l'Observatoire sur la sécurité des paiements par chèque ont été publiées en juillet 2021 dans le rapport annuel 2020. Depuis, certaines dispositions ont montré leur efficacité, à l'image des dispositifs de surveillance mis en place par les banques pour renforcer le contrôle des chèques à l'encaissement (par exemple, temporisation au moyen d'un compte de réserve), comme en témoignent les 195 millions d'euros de fraude déjouée en 2024. À l'inverse, d'autres dispositions attendent leur mise en œuvre effective, comme l'accès des banquiers présentateurs de chèque au Fichier national des chèques irréguliers (FNCI) [16], ou peinent parfois à être encore pleinement appliquées.

Deux recommandations font notamment l'objet d'un suivi plus rapproché depuis 2023, en raison de leur caractère stratégique dans la lutte contre la fraude au chèque : i) la sécurisation de l'envoi des chéquiers par voie postale et ii) la simplification des procédures de mise en opposition d'un chéquier ou d'un chèque pour perte ou vol.

L'Observatoire relève que, en 2024, 89 % des cas de fraude sur le chèque correspondent à des chèques perdus ou volés. Pour y remédier, il faut, en prévention, assurer un meilleur contrôle des envois postaux. Si malgré ces précautions le vol intervient, le FNCI reste le principal outil de la Place pour bloquer l'utilisation des chèques volés. Cela suppose qu'il soit alimenté avec diligence et également consulté de manière large.

En effet, la mise en opposition pour vol, qui entraîne automatiquement la déclaration du chèque ou du chéquier au FNCI, permet bien souvent d'éviter les cas de fraude subséquents. Malheureusement, lorsque les vols de chéquiers interviennent dans les circuits postaux, plusieurs jours peuvent s'écouler avant la mise en opposition.

Par ailleurs, l'accès des banquiers présentateurs de chèque au FNCI, qui est actuellement envisagé par une proposition de loi, permettrait aussi de lutter plus efficacement contre la fraude au chèque. En effet, les fraudeurs ciblent de plus en plus les banques, en cherchant à encaisser directement les chèques volés, et relativement moins les commerçants dont la propension à accepter les chèques tend à diminuer.

L'Observatoire souligne que des efforts ont été réalisés depuis 2021 pour sécuriser l'envoi du chéquier au domicile du client ainsi que pour faciliter la mise en opposition.

Afin d'avoir un impact encore plus significatif et durable sur la fraude au chèque, l'Observatoire appelle toutefois les PSP à augmenter leurs efforts et les investissements sur ces deux recommandations issues du rapport annuel 2020.

3.4.1 Protection du chèque lors de l'acheminement chez le 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 doit se faire sans frais pour le client), ii) sécuriser par tout moyen l'acheminement des chéquiers par voie postale jusqu'à ce qu'il soit entre les mains du client et iii) adopter en ce domaine un dispositif de vigilance permanente assurant une réaction rapide en cas de perte ou de vol.

En 2024, le groupe de travail a constaté que l'envoi postal, utilisé par défaut, reste le canal privilégié d'acheminement des chéquiers chez le client, à l'exclusion du premier chéquier qui est généralement délivré en mains propres dans les établissements qui disposent d'agences bancaires. L'envoi postal correspond en outre à un souhait de la part de nombreux clients, qui, depuis la crise sanitaire du Covid, se rendent de moins en moins en agence bancaire. Néanmoins, le choix du retrait du chéquier en agence doit rester possible sur demande du client.

De même, si quelques établissements ont fait le choix de ne plus proposer le renouvellement automatique du chéquier, permettant d'adapter une dotation de chéquiers à la demande du client en fonction de ses besoins, la plupart des établissements ont opté pour ce service « par défaut ». Ce système de renouvellement automatique s'effectue souvent à partir d'un seuil de consommation du chéquier défini (par exemple, lors de l'utilisation du 35e chèque ou au-delà, pour un chéquier de 50 formules).

13 Cf. DSA : le règlement sur les services numériques ou *Digital services act* | vie-publique.fr. eIDAS – *Electronic Identification, Authentication and Trust Services*, identification, authentification et services électroniques de confiance).

14 Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.

15 C'est le cas par exemple d'un service qui avait fait l'objet d'une décision de blocage de la Cour d'appel de Paris le 17 octobre 2024, dans le cadre d'un recours introduit par des associations de protection des mineurs. Depuis, la Cour d'appel a prononcé la levée du blocage du service (à la suite d'un recours en tierce opposition de celui-ci).

16 Une proposition de loi, déposée par M. le député Daniel Labaronne, pourrait prochainement répondre à cette recommandation de l'Observatoire : il s'agit de la proposition de loi, adoptée le 31 mars 2025 par l'Assemblée nationale, visant à renforcer la lutte contre la fraude bancaire, n° 496.

Bien que l'Observatoire appelle chacun à privilégier le retrait du chéquier en agence, il n'est pas opposé aux modalités de l'envoi postal du chéquier sous réserve que celui-ci soit sécurisé.

La grande majorité des acheminements est réalisée en lettre simple, sans suivi particulier, ne permettant pas de tracer les éventuels pertes ou vols qui pourraient avoir lieu. Les établissements ont toutefois mis en place des mécanismes de sécurité qui sont assez hétérogènes :

- Les expéditions en lettre simple sont souvent accompagnées d'un mécanisme d'alerte par la communication d'un message au client l'informant de l'envoi de son chéquier par le fabricant.
- D'autres établissements ont fait le choix de ne pas alerter le client de l'envoi postal du chéquier, mais de l'avertir lorsque le premier chèque issu du nouveau chéquier est tiré. S'il n'en est pas l'auteur, il lui est demandé de contacter son conseiller bancaire pour s'opposer au paiement.
- Certains établissements, plus avancés, ont également renforcé la sécurité de l'acheminement des chéquiers en demandant à leur client, par le biais de l'espace « chèque » de leur application bancaire, d'accuser réception de leur carnet de chèque. À défaut d'accuser réception, un message de suspicion de fraude leur sera notifié à chaque chèque tiré issu de ce nouveau chéquier.

Bien que ces modalités démontrent la volonté des établissements bancaires de se conformer aux recommandations de l'OSMP, les pratiques en la matière restent trop hétérogènes et bien souvent incomplètes. **Afin d'accélérer la mise en œuvre de cette recommandation, l'Observatoire propose d'en préciser le contenu ci-après.**

Précisions sur la recommandation n° 4, issue du rapport annuel 2020 :

Renforcer les interactions avec le client dans le cadre d'un envoi postal de chéquier

L'Observatoire demande aux établissements bancaires de :

1) **Laisser de manière explicite le choix du mode de réception d'un chéquier au client :** en agence ou par courrier lorsqu'un mécanisme de traçabilité de l'expédition est associé à l'envoi (lettre premium, suivie, recommandée, etc.). **À ce titre, les chéquiers ne doivent plus être acheminés au client en lettre simple.**

De plus, lorsque le client fait le choix de recevoir son chéquier par courrier postal, l'établissement bancaire procède à :

2) **L'envoi d'un premier message au client, lui annonçant qu'un chéquier vient de lui être envoyé par voie postale ;**

…/ …

3) **L'envoi d'un deuxième message, après un délai raisonnable, précisant au client que :** i) il est censé avoir reçu son chéquier et ii) si ce n'est pas le cas, il doit prendre contact avec son établissement bancaire dans les plus brefs délais en raison des risques de fraude, à défaut d'opposition.

Le canal emprunté pour envoyer ces messages doit être adapté à chaque profil de client et répondre à des objectifs de sécurité et d'impact, maximisant la vigilance et la réactivité du client sur la bonne réception du chéquier.

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

Quelques établissements bancaires ont récemment mis en œuvre la recommandation n° 5 de l'OSMP en permettant la mise en opposition des chèques perdus ou volés par voie électronique, notamment sur les espaces de banque en ligne. Cette procédure permet de raccourcir les délais de mise en opposition et de conserver la trace des confirmations conformément à l'article L. 131-35 [17] du Code monétaire et financier. En effet, celui-ci précise que « *le tireur doit immédiatement confirmer son opposition par écrit, quel que soit le support de cet écrit* », le tireur étant le client détenteur du compte sur le chèque est tiré.

En revanche, quatre ans après la publication des recommandations de l'Observatoire contre la fraude au chèque, des procédures anciennes de mise en opposition se faisant par téléphone et nécessitant une confirmation par écrit en agence perdurent au sein de nombreux établissements.

Précisions sur la recommandation n° 5, issue du rapport annuel 2020 :

Possibilité pour le client de mettre un chéquier/chèque en opposition directement en ligne

L'Observatoire demande aux établissements bancaires de laisser la possibilité au client de mettre en opposition un chéquier/chèque volé ou perdu directement par le biais des outils numériques dont dispose la banque (banque en ligne, application mobile). Ces outils doivent permettre aux clients de déclarer et de confirmer l'opposition de bout-en-bout, dans le respect des dispositions légales.

En outre, l'Observatoire demande que les dispositifs de mise en opposition s'appuyant sur des supports non numériques soient également fluides et rapides.

Les établissements bancaires transmettront à la Banque de France, d'ici fin 2025, les plans d'action détaillant la mise en place de ces deux recommandations complétées de leurs précisions.

3.5 Rappel des principales recommandations de l'Observatoire sur les sujets de veille technologique et sur les instruments SEPA

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 récapitulées dans cette section.

3.5.1 Rappel des recommandations de l'Observatoire concernant la fraude aux paiements SEPA

Les nouvelles tendances de fond dans l'évolution de l'usage du virement au sein du grand public, favorisées par la volonté des pouvoirs publics d'accélérer le développement du virement instantané, constituent de nouveaux défis pour la lutte contre la fraude.

En effet, avec le virement instantané, le temps d'intervention possible pour l'émetteur est de fait réduit. Ce mode de virement ne bénéficie pas par nature du délai d'exécution d'un jour ouvrable existant dans le cas d'un virement SEPA « classique », réduisant d'autant la possibilité de réagir lorsqu'une irrégularité est constatée, et ce aussi bien au niveau de l'utilisateur que du prestataire de service de paiement (PSP). Ce dernier ne dispose que de quelques millisecondes pour détecter une opération suspecte avant transmission vers le système de paiement.

Le prélèvement est, quant à lui, moins affecté par la fraude. Néanmoins, la multiplication des fuites de données incluant souvent des coordonnées bancaires (IBAN) et les récentes affaires de prélèvement abusifs ont mis en lumière l'importance d'une vigilance accrue de la part des prestataires de services de paiement et de leurs clients sur ce moyen de paiement. La souplesse des règles SEPA a permis de faciliter l'usage du prélèvement dans la vie courante, mais elle expose aussi ce moyen de paiement à des scénarios de fraude et d'escroquerie de plus en plus industrialisés, et cela malgré les mesures mises en œuvre par la communauté bancaire et les moyens à disposition des payeurs.

Compte tenu de ce contexte, il s'avère nécessaire de doter les PSP d'outils complémentaires pour améliorer leur capacité à identifier proactivement des opérations potentiellement frauduleuses. De plus, rappeler aux utilisateurs des services de paiement les règles de vigilance relatives à l'usage du virement et du prélèvement est également primordial.

Dans le cadre de ses 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 1.

17 Article L. 131-35 du Code monétaire et financier dispose qu'il « *n'est admis d'opposition au paiement par chèque qu'en cas de perte, de vol ou d'utilisation frauduleuse du chèque, de procédure de sauvegarde, de redressement ou de liquidation judiciaires du porteur. Le tireur doit immédiatement confirmer son opposition par écrit, quel que soit le support de cet écrit* ».

T1 Recommandations de l'Observatoire relatives aux virements et prélèvements SEPA

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 À noter : une proposition de loi visant à renforcer la lutte contre la fraude bancaire a été adoptée en première lecture par l'Assemblée nationale le 31 mars 2025. Si cette proposition était définitivement adoptée, elle répondrait à la recommandation de l'OSMP.
Alerter et sensibiliser le public aux risques liés aux techniques de manipulation directe de l'utilisateur de services de paiement. 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 l'émission d'un virement, d'autant plus s'il s'agit d'un virement instantané : • N'effectuez un virement que lorsque vous êtes certain de l'identité du bénéficiaire et de son IBAN. • À partir d'octobre 2025, 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 s'il est supposé vous avoir 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.	Utilisateurs des services de paiement, qu'ils soient professionnels ou issus du grand public

…/…

T1 Recommandations de l'Observatoire relatives aux virements et prélèvements SEPA (suite)

Recommandations	Destinataires
• 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, soyez attentif aux informations et avertissements relatifs à l'opération qui sont affichés par votre prestataire de service de paiement.	
Rappeler les principes de fonctionnement du prélèvement bancaire et les risques associés. Ces actions de sensibilisation devraient en particulier décrire le rôle du créancier et du débiteur 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, 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 par les clients. • 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, en rappelant les délais réglementaires durant lesquels le détenteur de compte 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.), en sa possession dans les systèmes d'information et équipements informatiques détenus, compte tenu des usages frauduleux pouvant survenir en cas de fuite de données.	Créanciers (entreprises, associations, administrations) Grand public

Source : Observatoire de la sécurité des moyens de paiement.

3.5.2 Recommandations relatives à l'informatique quantique et la sécurité des systèmes de paiement par carte bancaire

L'informatique quantique offre des perspectives prometteuses dans des secteurs d'activité variés (en finance, logistique, météorologie, chimie, etc.), mais un cas d'usage bien identifié est problématique : le déchiffrement des communications électroniques sécurisées, dont les paiements, à un horizon de 10 à 20 ans. Il s'agit d'une menace sérieuse vis-à-vis de la sécurité nationale qui est déjà prise en compte par les autorités publiques (par exemple le mémorandum de sécurité nationale aux États-Unis de mai 2022, ou loi française de programmation militaire d'août 2023). **Toutefois, le secteur des paiements est invité à s'en saisir dès maintenant et à haut niveau en raison des cycles de vie des matériels et logiciels de paiement par carte (puces, terminaux de paiement électroniques, serveurs, etc.).**

La confidentialité et l'intégrité des paiements par carte sont assurées par deux types d'algorithmes : les algorithmes de chiffrement asymétrique (RSA, ECC, etc.) et les algorithmes de chiffrement symétrique (AES, Triple DES, etc.). L'étude de l'OSMP a réalisé un recensement de l'utilisation des algorithmes dans le dispositif de paiement par carte. Sans action de résilience, les risques à terme les plus importants sont :

- le vol de données privées, voire confidentielles, chez les commerçants piratés,
- la génération de paiements frauduleux par la fabrication de « *Yes Card* » pour les paiements dits « hors ligne »,
- la perte de confiance dans les infrastructures de paiement,
- et la prise de conscience par le public de ces risques qui pourrait provoquer une crise de confiance généralisée menaçant ainsi la stabilité de nos économies.

L'étude montre que des solutions techniques existent, mais qu'elles ne sont pas triviales, particulièrement dans le cas des algorithmes de chiffrement asymétrique.

T2 Recommandations relatives à l'informatique quantique et la sécurité des systèmes de paiement par carte bancaire

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.

3.5.3 Recommandations relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette

Les recommandations relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette ont été publiées dans le rapport annuel 2022.

Dans son rapport annuel 2016, l'Observatoire avait réalisé une étude sur l'acceptation des paiements par carte en situation de mobilité. Cette étude s'était principalement intéressée à deux solutions d'acceptation : le terminal autonome et le terminal m-POS (*mobile Point of Sale*). Le développement des terminaux m-POS est toutefois resté marginal puisqu'ils ne représentent en 2024 que moins de 1 % du parc de terminaux déployés en France. Plusieurs motifs ont incité l'Observatoire à étudier de nouveau en 2022 la sécurité des solutions de paiement en mobilité :

- les travaux de normalisation,
- le regain d'intérêt pour ces solutions d'acceptation de la part des acteurs historiques et technologiques issus du secteur mobile,
- et les évolutions rapides du marché.

Cette étude a porté plus précisément sur les solutions d'acceptation de paiement sur *smartphone* ou tablette, dite SoftPOS (*Software Point of Sale*). Il s'agit d'une application installée sur un appareil mobile non conçu pour l'acceptation des paiements par carte, de type *smartphone* ou tablette, pourvu de la technologie NFC (*near field communication*, communication en champ proche). L'Observatoire la perçoit en effet comme une alternative aux terminaux de paiement électroniques (TPE) traditionnels pour l'acceptation des paiements par carte, mais aussi comme une solution foncièrement différente puisqu'elle repose entièrement sur du logiciel.

T3 Recommandations de l'Observatoire relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette

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

…/…

T3 Recommandations de l'Observatoire relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette (suite)

Recommandations	Destinataires
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.

3.5.4 Recommandations relatives à l'identité numérique et la sécurité des paiements

Les recommandations relatives à l'identité numérique et la sécurité des paiements ont été publiées dans le rapport annuel 2021.

Les phénomènes d'usurpation d'identité, associés parfois à des techniques de fraude documentaire, peuvent mettre à mal la sécurité générale des moyens de paiement. En particulier, l'Observatoire relève et distingue trois phénomènes de fraude : i) les usurpations d'identité au moment de l'entrée en relation, ii) les usurpations de l'identité du payeur au moment de l'acte d'achat et iii) les usurpations de l'identité du bénéficiaire d'un paiement. Certains schémas de fraude reposent toujours sur l'usurpation d'identité de personnes morales. Toutefois, les risques d'usurpation d'identité portent principalement sur l'identité de personnes physiques.

En cherchant à lutter contre les risques d'usurpation d'identité dans la sphère numérique, les solutions d'identité numérique et les services de confiance sécurisés, comme la signature et le cachet électroniques, peuvent aider à améliorer la sécurité générale des moyens de paiement. L'Agence nationale de la sécurité des systèmes d'information a publié en 2021 un référentiel d'exigences destiné aux prestataires de vérification d'identité à distance (PVID). Parallèlement, la réglementation européenne eIDAS sur l'identification électronique et les services de confiance a été révisée en 2024 pour compléter le cadre européen relatif à une identité numérique [18]. L'Observatoire invite donc les acteurs du paiement à lutter contre les usurpations d'identité en recourant aux services d'identité numérique conformes aux exigences PVID ou eIDAS.

T4 Recommandations de l'Observatoire relatives à l'identité numérique et la sécurité des paiements

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

…/…

T4 Recommandations de l'Observatoire relatives à l'identité numérique et la sécurité des paiements (suite)

Recommandations	Destinataires
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.

3.5.5 Recommandations relatives à la sécurité des paiements en temps réel

Les recommandations relatives à la sécurité des paiements en temps réel ont été publiées dans le rapport annuel 2020.

Dans un contexte de développement rapide du virement instantané, qui pourrait progressivement se substituer au virement classique, voire à d'autres moyens de paiement, l'Observatoire reste particulièrement attentif à la sécurité des paiements en temps réel. En 2024, le virement instantané représentait 10 % du nombre total de virements et 0,7 % des montants échangés par virement (hors virements de gros montant traités par les systèmes de paiement de montant élevé). Le nombre de virements instantanés a encore progressé de 62 % par rapport à 2023. Le développement des virements instantanés devrait se poursuivre dans les prochaines années, soutenu par les stratégies nationales et européennes relatives aux moyens de paiement et par les initiatives législatives des pouvoirs publics européens, notamment l'équivalence tarifaire des virements instantanés par rapport aux virements classiques. En matière de sécurité, l'Observatoire note que le taux de fraude sur les virements instantanés (0,046 % en 2024) est proche de celui de la carte. Toutefois, avec 107 millions d'euros de fraude sur le virement instantané en 2024, soit près de 30 % du total de la fraude recensée sur les virements, l'Observatoire renouvelle son appel à destination des industriels des paiements à poursuivre leurs efforts et leurs investissements pour renforcer la sécurité des virements instantanés. De plus, l'Observatoire réitère ses recommandations visant à assurer un développement rapide et sécurisé de ce nouveau moyen de paiement.

18 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS – *Electronic IDentification Authentication and trust Services*), modifié par le règlement (UE) n° 2024/1183 du 11 avril 2024 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.

T5 Recommandations de l'Observatoire relatives à la sécurité des paiements en temps réel

Recommandations	Destinataires
Mettre en œuvre, dans les conditions fixées par la DSP 2, 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)

…/…

T5 Recommandations de l'Observatoire relatives à la sécurité des paiements en temps réel (suite)

Recommandations	Destinataires
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.

3.5.6 Recommandations relatives à la sécurité des données de paiement

Les recommandations relatives à la sécurité des données de paiement ont été publiées dans le rapport annuel 2019.

Le développement d'usages numériques intégrant les données de paiement – qu'il s'agisse de l'intégration dans des applications mobiles, dans des objets connectés ou pour utiliser des services de conseil budgétaire personnalisé – a pour conséquence une dissémination de ces données, désormais partagées avec divers acteurs (banques, commerçants, Fintech, etc.) dans différents environnements.

Dans ce contexte, la mise en œuvre de la DSP 2 a permis de renforcer la sécurité des usages dits de « banque ouverte » (*open banking*). Des acteurs tiers supervisés peuvent ainsi accéder aux comptes de paiement des utilisateurs en vue de fournir des services d'agrégation des informations ou d'initiation de paiement, au travers d'interfaces sécurisées dédiées qui ne nécessitent pas la communication des identifiants personnels de connexion. Le niveau de sécurité et de performance offert par ces interfaces et leur capacité à préserver la confidentialité des données seront des facteurs déterminants pour le développement des services d'*open banking* dans des conditions optimales de confiance et de fluidité pour l'utilisateur.

L'Observatoire rappelle le rôle central que jouent les utilisateurs dans la protection de leurs propres données de paiement. Il les invite à adopter les bons réflexes en veillant à protéger ces données et à ne les partager qu'au sein d'environnements de confiance.

T6 Recommandations de l'Observatoire relatives à la sécurité des données de paiement

Recommandations	Destinataires
Recourir, dans les conditions fixées par la DSP 2 (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

…/…

T6 Recommandations de l'Observatoire relatives à la sécurité des données de paiement (suite)

Recommandations	Destinataires
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 : DSP 2, deuxième directive européenne sur les services de paiement.
Source : Observatoire de la sécurité des moyens de paiement.

3.5.7 Recommandations relatives à la sécurité des paiements par mobile

Les recommandations relatives à la sécurité des paiements par mobile ont été publiées dans le rapport annuel 2018.

Le paiement par carte au point de vente par l'intermédiaire d'une solution mobile a connu un net développement ces quatre dernières années, porté par la crise sanitaire et la possibilité de payer sans contact dans la limite de cinquante euros. En 2024, le nombre de paiements par mobile représente 15 % du nombre de paiements par carte de proximité, contre respectivement 0,5 % avant la crise sanitaire.

Dans le même temps, le taux de fraude des paiements sans contact par mobile, qui s'établissait à 0,021 % en 2023, a continué de diminuer en 2024 pour atteindre 0,016 %. Cela traduit un renforcement des outils de maîtrise du risque de fraude, notamment au moment de l'enrôlement de l'utilisateur dans la solution, que l'Observatoire appelle à poursuivre. Pour éviter les risques d'enrôlement de numéros de carte usurpés par les fraudeurs dans ce type de solution, la mise en œuvre d'une authentification forte du porteur, prévue par la DSP 2 au titre des opérations sensibles, est impérative.

T7 Recommandations de l'Observatoire relatives à la sécurité des paiements par mobile

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

.../...

T7 Recommandations de l'Observatoire relatives à la sécurité des paiements par mobile (suite)

Recommandations	Destinataires
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.

4

L'APPORT DE L'INTELLIGENCE ARTIFICIELLE (IA) DANS LA LUTTE CONTRE LA FRAUDE : ENJEUX ET PERSPECTIVES

4.1 Propos introductif

De manière générale, les dispositifs de lutte contre la fraude aux moyens de paiement reposent sur quatre piliers fondamentaux, consacrés par la deuxième directive européenne sur les services de paiement (DSP 2 [1]) :

1. L'authentification des parties prenantes à la transaction, permettant de s'assurer de la légitimité du payeur et du payé ;
2. La capacité des acteurs de la chaîne des paiements à détecter les transactions présentant un risque de fraude élevé ;
3. La sécurité physique et logique des instruments et infrastructures de paiement, visant à assurer que les données de paiement sont protégées à tout moment contre les risques de compromission ou de réutilisation à des fins de fraude ;
4. La sensibilisation des utilisateurs, afin d'assurer qu'ils veillent à protéger leurs instruments et leurs données de paiement et qu'ils sachent réagir en cas de tentative de fraude.

Si ces quatre piliers constituent aujourd'hui un socle solide en matière de lutte contre la fraude, l'habileté des fraudeurs à inventer de nouveaux procédés frauduleux appelle les acteurs de la chaîne des paiements à tirer parti du progrès technologique pour développer de nouvelles capacités en matière de lutte contre la fraude. C'est le cas, en particulier, pour le renforcement des mécanismes de détection des transactions à risque (point 2 ci-dessus). Ces dispositifs de surveillance, qui sont l'objet de la présente étude, sont principalement des modèles de notation des transactions de paiement (en anglais modèles de *scoring*). Ceux-ci s'appuient sur des algorithmes sophistiqués, développés par des équipes de modélisation et d'analyse exploratoire de données. Leur rôle est d'analyser automatiquement et en temps réel les caractéristiques des transactions afin d'émettre des alertes en cas de suspicion de fraude. La transaction peut ainsi être bloquée le temps que des analystes procèdent à des contrôles. L'introduction de modules d'intelligence artificielle (IA) dans ces dispositifs permet d'accroître significativement les performances des modèles de détection.

Ces dispositifs peuvent être déployés à différents niveaux de la chaîne des paiements :

- Soit de façon complètement autonome, au niveau de l'un des acteurs de la chaîne des paiements :
  - Par exemple, un prestataire de services de paiement peut caractériser le profil d'utilisation de chacun de ses clients, fondé sur ses habitudes de paiement, et évaluer le risque de fraude d'une transaction en fonction de son caractère atypique (écart par rapport aux habitudes du client). Ainsi, pour un client qui n'utilise sa carte qu'en proximité pour des petits montants ou des retraits, l'émission d'un paiement de montant élevé sur internet vers l'étranger doit être considérée comme plus risquée que pour un utilisateur qui utiliserait régulièrement sa carte pour des paiements vers des sites étrangers ;
  - Autre exemple : un commerçant en ligne peut considérer, pour un client habituel, qu'un changement d'adresse de livraison est un facteur de risque qui peut nécessiter un appel de vérification ou une demande d'authentification forte au moment du paiement ;

- Certains mécanismes de *scoring* sont partagés entre les différents acteurs de la chaîne des paiements, via les réseaux de paiement par carte (tels que Cartes bancaires, Visa ou Mastercard) ou les infrastructures de paiement (telles que STET ou ABE Clearing). Ces réseaux et infrastructures de paiement ont en effet pour caractéristique de centraliser les flux de paiement d'un grand nombre d'établissements, y compris les informations relatives aux mécanismes de

1 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

rappel des fonds ou de remboursement des cas de fraude. Le traitement de ces données permet d'émettre une note sur le niveau de risque d'une transaction donnée, qui est partagée avec le prestataire de services de paiement du payeur. Celui-ci peut ainsi ajuster, s'il le juge opportun, sa propre appréciation du risque.

En mettant en échec les tentatives de fraude, ces modèles contribuent directement au maintien et à l'amélioration de la confiance dans les moyens de paiement et, par extension, à la stabilité du système bancaire et financier. Ils favorisent en outre la fluidification des parcours client. En effet, leur utilisation permet à certaines transactions de déroger à l'obligation d'authentification forte dès lors que le niveau de risque afférent est jugé faible (exemption relative à l'analyse des risques liés à l'opération [2]).

En conséquence, l'objet de cette étude est de présenter les principaux types de modèles utilisés ainsi que les enjeux associés à leur utilisation, leur intégration dans les processus métiers des acteurs de la chaîne des paiements et le respect des cadres règlementaires en vigueur.

4.2 Les enjeux techniques relatifs à l'optimisation de la performance des modèles

La qualité des données utilisées en entrée est essentielle pour la performance des modèles. Les acteurs du paiement sont à cet égard confrontés à un double défi : i) celui d'améliorer en continu la qualité des données ; ii) tout en intégrant rapidement de nouvelles données d'entraînement reflétant les dernières techniques de fraude identifiées. À cela s'ajoute la nécessité de trouver un bon équilibre entre l'impératif de disposer de modèles performants et le risque d'une multiplication importante des « faux positifs », c'est-à-dire les transactions qui sont à tort identifiées comme suspectes, car elles sont une source de gêne pour les clients.

4.2.1 Les données d'entraînement

La nature des données utilisables dans les dispositifs de surveillance des transactions de paiement est précisée par le règlement délégué relatif à l'authentification forte du client complétant la DSP 2. Il s'agit notamment des habitudes du client dans l'utilisation de son instrument de paiement, d'opérations de paiement, de la localisation du payeur et du bénéficiaire, des dispositifs techniques et des logiciels utilisés par le payeur ou des signes d'infection par un logiciel malveillant. Des négociations ont lieu pour faire évoluer ce cadre réglementaire dans un règlement européen sur les services de paiement (RSP) [3]. Ce projet de règlement autoriserait toujours l'utilisation des données actuelles pour les dispositifs de surveillance des transactions, mais serait enrichi des données relatives à la session applicative (adresses IP, etc.) et de façon générale, de tous les éléments d'information permettant de reconnaître un utilisateur légitime qui agit conformément à ses habitudes de paiement.

4.2.1.1 La qualité des données d'entraînement

Dans le domaine de l'apprentissage automatique, le jeu de données d'entraînement est semblable à la fondation d'une construction : c'est ce qui détermine la force et la stabilité de tout modèle d'IA. Pour garantir un modèle robuste dans le temps, les données doivent être fiables (c'est-à-dire des données avec des valeurs cohérentes, au bon format, avec peu de valeurs manquantes et non logiques), non biaisées, disponibles dans le temps et représentatives de la population à laquelle s'applique le modèle.

Une grande partie de ces données est renseignée, transmise et collectée dans les champs des messages d'authentification et d'autorisation par chacun des acteurs de la chaîne des paiements jusqu'au système d'information (SI) du prestataire de services de paiement (PSP) émetteur. Dans le cadre de l'autorisation technique du paiement, les données obligatoires sont standardisées dans les règles de fonctionnement des instruments de paiement (*rulebook*), à l'instar des numéros de carte (PAN, *primary account number*) pour les systèmes de carte (*card schemes*, réseaux d'échange de transactions par carte de paiement) ou des identifiants uniques (IBAN) pour les systèmes de paiement SEPA [4] (SEPA *payment schemes*). D'autres champs sont prévus pour enregistrer des données considérées comme optionnelles (par exemple, adresse de livraison, numéro Siret du marchand, etc.), mais ni leur disponibilité ni leur qualité ne sont garanties en l'absence de standards de Place.

Les développements et les intégrations de logiciels nécessaires pour assurer la qualité des données ainsi échangées représentent un coût parfois difficile à assumer par certains acteurs, tels que les petits commerçants par exemple. Par ailleurs, les pratiques en matière de collecte et de transmission de données chez les PSP restent souvent hétérogènes, particulièrement si une des parties à la transaction n'est pas localisée en France ni dans l'Union européenne.

➡ La complétude et l'exactitude des données d'entraînement sont ainsi directement affectées par la longueur de la chaîne des paiements et l'insuffisance de standards correctement définis et appliqués. Le renforcement des standards de Place en matière de qualité des données tout au long de la chaîne des paiements bénéficierait à l'ensemble de l'écosystème et augmenterait l'efficacité des dispositifs de lutte contre la fraude.

Pour renforcer la qualité des données, les PSP réalisent, ou bien délèguent à des *start-ups* spécialisées, la fiabilisation des données notamment en croisant diverses sources. Des modules d'IA exécutent potentiellement cette tâche. Par exemple, lorsque les données de commerçants sont enrichies des horaires d'ouverture et de la géolocalisation des différents points de vente, des alertes de fraude seront émises en cas d'incohérences détectées. En effet, les paiements par carte de proximité réalisés sur des terminaux de paiement électroniques (TPE) en-dehors des heures ou de la localisation habituelles engendreront une alerte.

Par ailleurs, la panoplie des typologies de fraude aujourd'hui observée est très large : fraude par manipulation, fraude au moyen du piratage de la banque en ligne, fraude par carte initiée par un faux « marchand » qui se trouve en réalité être un fraudeur, contestation abusive par le client lui-même, etc. Leur détection appelle donc des jeux de données différents dans chaque cas de figure.

➡ La segmentation des données disponibles est une technique souvent adoptée en divisant le jeu de données disponibles en plusieurs ensembles, à partir de critères objectifs, pour développer un modèle de détection optimisé pour chaque typologie de fraude.

4.2.1.2 Le déséquilibre de la classe des transactions fraudées

En statistique, une classe est un groupe de valeurs dans lequel les données sont classées pour le calcul d'une distribution de fréquence. D'après les statistiques de l'Observatoire de la sécurité des moyens de paiement, en 2023, le nombre de transactions frauduleuses représentait 0,0337 % du nombre total des transactions sur les cartes et 0,0016 % sur les virements.

➡ Ces très faibles proportions posent des difficultés en matière de modélisation statistique car il est difficile d'entraîner des modèles à détecter des fraudes sur des échantillons de taille aussi petite.

Deux techniques statistiques peuvent être employées pour remédier à ce problème :

- **Le sur-échantillonnage** : cette technique statistique consiste à dupliquer aléatoirement des observations de la classe minoritaire (les opérations frauduleuses) jusqu'à obtenir la proportion souhaitée. L'effet est donc de reconstituer un jeu d'observations dans lequel la part d'observations frauduleuses est plus importante ;
- **Le sous-échantillonnage** : cette technique consiste à supprimer aléatoirement des observations de la classe majoritaire (les opérations non frauduleuses) jusqu'à obtenir la proportion souhaitée de la classe minoritaire.

Ces techniques d'ajustement statistique peuvent toutefois induire des effets indésirables :

- **Dans le cas du sur-échantillonnage** : au-delà des problématiques de stockage de données et de temps de calcul accru, cette technique duplique des données existantes et, ce faisant, les erreurs d'observations associées. Cette méthode comporte également un risque de « surajustement du modèle » pouvant conduire ce dernier à ne détecter que les cas de fraude dont les caractéristiques sont identiques à celles comprises dans l'échantillon d'entraînement **;**
- **Dans le cas du sous-échantillonnage :** le nombre absolu de cas de fraude étant par nature très réduit, l'accroissement de leur part dans le total de l'échantillon implique une réduction considérable du nombre total de transactions de l'échantillon d'entraînement. Or, un nombre minimum d'observations est requis pour calibrer et entraîner pertinemment un modèle. Par ailleurs, comme le volume des transactions légitimes a été significativement réduit, il existe un risque que le modèle ne voie plus l'ensemble des typologies de paiement légitime, conduisant ainsi à lever trop d'alertes (les « faux positifs »).

➡ La mutualisation des données entre établissements, par exemple par le biais des systèmes et réseaux interbancaires, peut également constituer une réponse à la faible proportion des cas de fraude dans les échantillons. Cette solution permet d'augmenter le nombre de cas réels de fraude sans avoir à recourir à des méthodes statistiques qui peuvent être source de distorsions.

4.2.2 Les trois grandes familles de modèles

4.2.2.1 Les modèles experts

Les modèles experts (ou modèles heuristiques) sont constitués de règles automatiques, appelées scénarios, que les experts élaborent à partir de l'analyse des données de transactions frauduleuses. Ces règles sont donc adaptées aux modèles d'affaires des établissements et aux caractéristiques des

2 Cette exemption à l'authentification forte est prévue à l'article 18 du règlement délégué (UE) 2018/389 de la Commission européenne du 27 novembre 2017, complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de règlementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

L'Observatoire avait rappelé les principes applicables en la matière dans son rapport annuel 2022 (partie 4.1.3).

3 Cf. Commission européenne, proposition de règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, 28 juin 2023.

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

habitudes de paiement de leurs clients. Voici quelques exemples de règles courantes qui permettent de lever une alerte :

- une opération dont le montant est disproportionné, dépassant des seuils prédéfinis par rapport aux montants habituels des transactions d'un client, en entrée comme en sortie de son compte ;
- une opération atypique réalisée avec une contrepartie localisée à l'étranger, notamment dans certaines zones géographiques ou auprès d'établissements identifiés à risque ;
- des opérations correspondant à l'utilisation de comptes de « mule » [5] se traduisant par l'alimentation du compte par de nombreux débiteurs sur une période relativement courte suivis de multiples retraits en espèces, alors même que l'ouverture du compte est récente.

Les modèles heuristiques présentent l'avantage d'être adaptables rapidement pour appréhender les modifications d'habitudes des clients et des fraudeurs. Par exemple, certaines règles pourront être levées si le client déclare à son PSP un déplacement à l'étranger. Ces modèles sont également facilement interprétables : la cause du déclenchement d'une alerte est simple à identifier.

➡ À rebours des modèles heuristiques, les modèles plus sophistiqués fondés sur des modules d'IA peuvent être moins réactifs et souvent plus difficiles à interpréter tout en offrant des perspectives plus larges de détection de la fraude dans un environnement où les fraudes tendent également à être de plus en plus sophistiquées.

4.2.2.2 Les modèles statistiques d'IA

Différents types de modèles d'IA existent, mais ceux qui ont la détection de la fraude comme objet appartiennent majoritairement à la catégorie des modèles dits « supervisés ». À partir de données en entrée, ils ont pour but de reproduire une réponse connue, par exemple la temporisation ou le blocage de la transaction identifiée comme potentiellement frauduleuse. Voici les modèles statistiques d'IA les plus utilisés dans ce cadre :

- **La régression logistique** estime la probabilité qu'un événement se produise sur la base d'un jeu de variables indépendantes. Il s'agit d'un modèle qui produit une cote $f(x)$, assimilable à une probabilité comprise entre 0 et 1, sur la nature frauduleuse d'une transaction, définie à partir de ses caractéristiques propres x_i et de leurs pondérations respectives w_i dans la cote finale. C'est un modèle linéaire généralisé [6] utilisant une fonction logistique [7] comme fonction de lien.

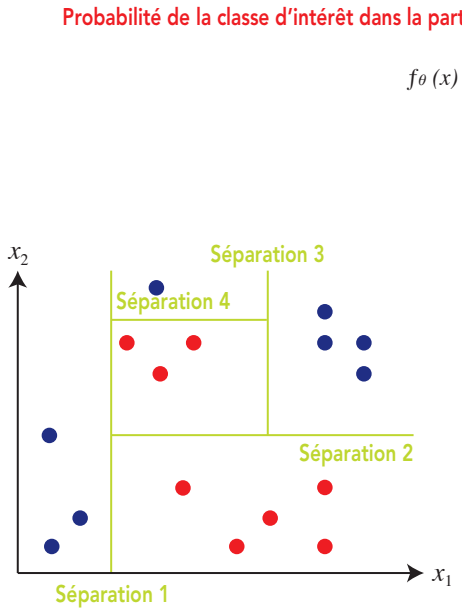
  Ainsi, tout le problème de classification par régression logistique apparaît alors comme un simple problème d'optimisation où, à partir de données, les experts tentent d'obtenir le meilleur jeu de paramètres w_i permettant à la courbe sigmoïde de coller au mieux aux données.
- **L'arbre de décision** est un algorithme d'apprentissage automatique (*machine learning,* ML) qui permet de faire une prédiction ou un classement. Il s'agit de modèles de partitionnement de l'espace pour isoler les cas de fraude (couleur rouge dans le schéma 1) en fonction de règles de logique simples et en succession s'appliquant aux caractéristiques des transactions, résumées dans le schéma 1 aux deux variables x_1 et x_2. Ces modèles sont faciles à interpréter et à entraîner. Contrairement à la régression logistique, ils permettent d'identifier des relations non linéaires, et donc plus complexes, entre les différentes caractéristiques d'une transaction frauduleuse.
- **La forêt aléatoire d'arbres décisionnels *(Random Forest)*** est un algorithme qui combine les résultats de plusieurs arbres de décision entraînés sur des sous-ensembles de données légèrement différents pour obtenir un résultat unique.

  ➡ L'arbre de décision est l'une des meilleures formes d'algorithme de *machine learning* (ML). Il offre une grande facilité d'interprétation et permet d'améliorer les modèles prédictifs avec précision. Toutefois, pour la détection de la fraude, certains professionnels considèrent qu'une régression logistique pourrait être plus performante qu'un arbre de décision et qu'une forêt d'arbres décisionnels serait plus performante qu'une régression logistique, car les relations entre les données ne seraient pas linéaires.

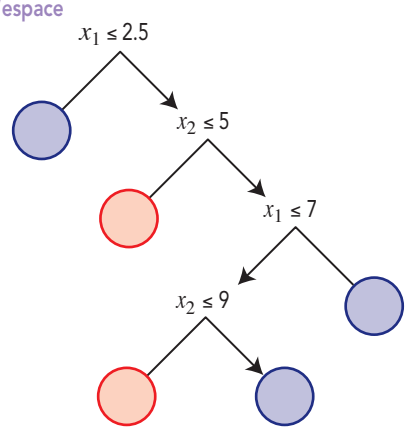
- **Le *boosting*** améliore la précision et les performances prédictives des modèles de ML en convertissant plusieurs modèles d'apprentissage faibles (à faible capacité de prédiction) en un seul modèle d'apprentissage fort (dont la précision de prédiction est plus élevée). Bien qu'il existe de nombreuses variations dans la mise en œuvre, les scientifiques des données utilisent souvent le *boosting* avec des algorithmes d'arbre de décision. Un modèle d'ensemble est créé en combinant plusieurs arbres de décision faibles de manière séquentielle. Les scientifiques de données attribuent des poids à la sortie des arbres individuels, et accordent ensuite aux classifications incorrectes du premier arbre de décision un poids plus élevé, puis modifient le poids en entrée dans l'arbre suivant pour corriger ces erreurs. Après de nombreux cycles, la méthode de *boosting* combine ces règles faibles en une règle unique de prédiction forte.

S1 Principe statistique de l'arbre de décision

a) Exemple de partitionnement de l'espace



b) Arbre de décision associé au partitionnement



Source : Observatoire de la sécurité des moyens de paiement.

➡ Ces modèles sont très performants pour capter les schémas de fraude complexes, mais nécessitent des techniques d'interprétabilité adaptées telles que le graphique de dépendance partielle (*partial dependence plots*, PDP) ou l'effet local accumulé (*accumulated local effect*, ALE).

- **Les réseaux de neurones (*deep learning*)** sont des modèles d'analyse statistique avec apprentissage automatique qui utilisent des nœuds ou neurones interconnectés. Il s'agit d'un sous-ensemble du *machine learning* où les algorithmes sont des variantes d'un algorithme de ML nommé réseau de neurones.

➡ Bien que ces modèles devraient en théorie mieux tirer parti des très nombreuses données disponibles, dans la pratique ils se montrent moins performants sur les données structurées de paiement que dans les approches plus traditionnelles [8]. Ils manquent en particulier de transparence dans l'explication de la notation des transactions.

4.2.2.3 Les modèles d'IA de type réseau de neurones en graphe (*Graph Neural Network*, GNN)

L'apparition de nouveaux types de données et la multiplication de données non structurées ont conduit à la création de nouveaux modèles d'apprentissage automatique capables de s'adapter à des données non structurées comme des graphes [9]. C'est le cas par exemple des réseaux de neurones en graphe (GNN). Ils constituent ainsi un prolongement des réseaux de neurones conventionnels issus du *deep learning* qui sont utilisés pour traiter des données structurées.

➡ Les GNN permettent de combiner l'application de scénarios, à l'instar des modèles experts, avec une approche statistique. Ce modèle permet d'obtenir des notations précises des transactions, ainsi qu'une meilleure exploitabilité des résultats.

5 Comptes d'intermédiaires, souvent manipulés par le fraudeur, pour permettre le transfert d'argent du compte des victimes vers celui du fraudeur.

6 La fonction $f(x)$ est déterminée par une combinaison linéaire pondérée : $f(x) = \sum_{i=1}^{n} w_i f(x_i)$.

7 En mathématiques, les fonctions logistiques sont les fonctions ayant pour expression : $f(t) = \frac{k}{1+ae^{-rt}}$ où k et r sont des réels positifs et a un réel. Ces fonctions renvoient uniquement des valeurs comprises entre 0 et 1 pour la variable dépendante, quelles que soient les valeurs de la variable indépendante.

8 Cf. « Why do tree-based models still outperform deep learning on tabular data? », Léo Grinsztajn (Soda), Édouard Oyallon (Institut des systèmes intelligents et de robotique, ISIR, et Centre national de la recherche scientifique, CNRS), Gaël Varoquaux (Soda), juillet 2022.

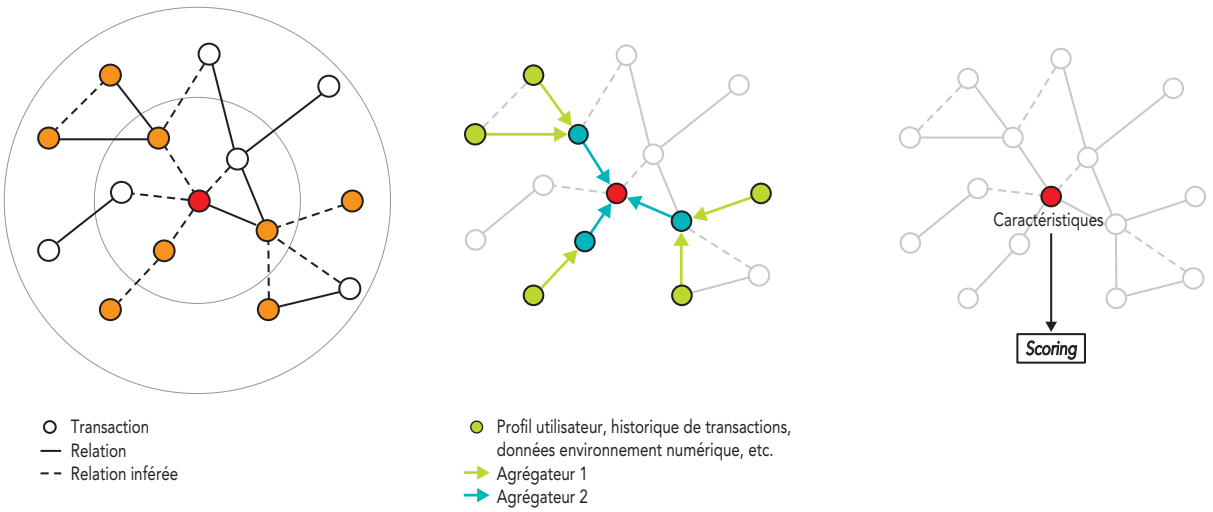
9 Un graphe est une structure de données complexe utilisée pour représenter des objets et des relations entre eux. Un graphe est constitué d'un ensemble de nœuds (*nodes*) et d'arêtes (*edges* ou *links*).

S2 Illustration d'un réseau de neurones en graphe appliqué au paiement

a) Analyser le « voisinage »

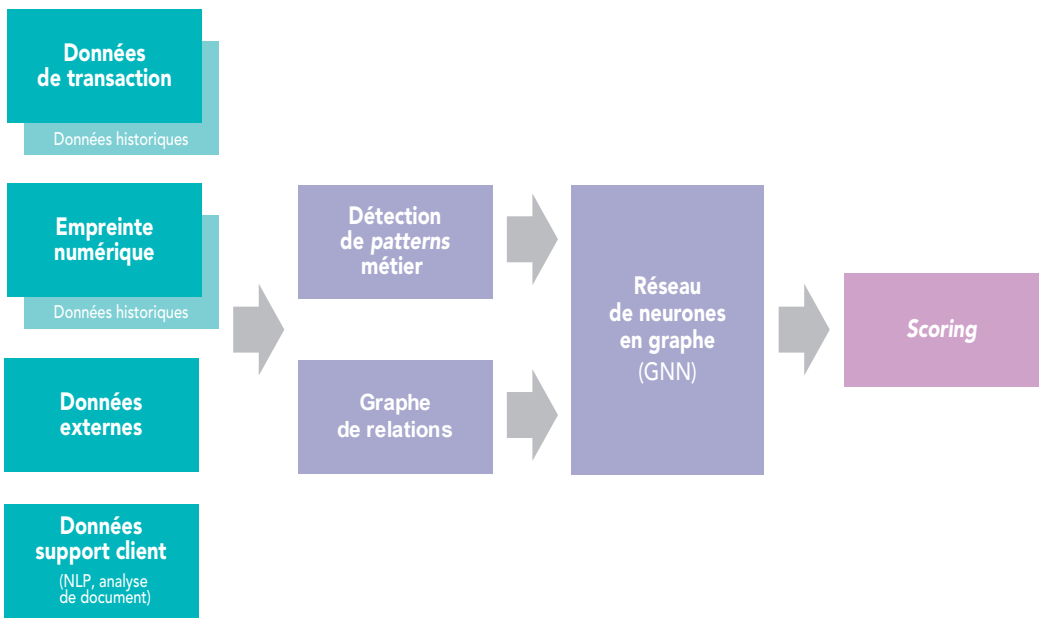
b) Agréger les renseignements à partir des nœuds voisins

c) Déterminer le *scoring* à partir des données agrégées (classification de nœud)



Source : Observatoire de la sécurité des moyens de paiement.

S3 Architecture simplifiée des modèles de réseau de neurones en graphe associés à des scénarios métier



Note : GNN, *Graph Neural Network*, réseaux de neurones en graphe ; NLP, *Natural Language Processing*, traitement du langage naturel.

Source : Observatoire de la sécurité des moyens de paiement.

➡ De manière générale, les modèles d'apprentissage automatique sont puissants mais également difficiles à interpréter. L'exploitabilité des résultats peut être facilitée en développant des méthodes d'interprétation, à l'instar de l'outil SHAP [10] (*SHapley Additive exPlanations*), du graphique de dépendance partielle (*Partial Dependence Plots*, PDP) ou de l'effet local accumulé (*Accumulated Local Effect*, ALE). Ces différentes méthodes permettent d'interpréter les modèles non linéaires à la manière de modèles linéaires (somme de poids des facteurs) et de mieux comprendre l'effet des caractéristiques du modèle sur les prédictions.

4.2.3 Les performances statistiques de détection de la fraude

4.2.3.1 Les outils de mesure de performance des modèles

La capacité des modèles de détection de la fraude à générer des alertes pertinentes ne peut s'apprécier qu'à l'aune d'indicateurs spécifiques.

Une autre manière d'exprimer les faux positifs est d'exprimer le nombre de transactions légitimes remontées comme alertes par le modèle pour finalement détecter un seul cas réel de fraude : **la courbe ROC** (*Receiver Operating Characteristic*, caractéristique de fonctionnement du récepteur) **est l'une des mesures les plus répandues en modèle de détection**.

Pour représenter la courbe ROC, il faut dans un premier temps classer toutes les transactions d'un échantillon, soit légitimes soit frauduleuses, par ordre de notation renvoyée par le modèle. À partir d'une certaine note, aussi appelée seuil de classification, les transactions font l'objet d'une alerte.

Le taux de vrais positifs, appelé **taux de détection** dans le tableau 1, est égal au nombre de vrais positifs divisé par la somme du nombre de vrais positifs et de faux négatifs. Les vrais positifs sont les transactions qui sont correctement classées comme frauduleuses, et les faux négatifs sont celles qui sont incorrectement classées comme légitimes.

Le **taux de faux positifs** est égal au nombre de faux positifs divisé par la somme du nombre de faux positifs et de vrais négatifs. Les faux positifs sont les transactions indûment classées comme frauduleuses et les vrais négatifs sont celles correctement classés comme légitimes.

10 Cf. « A unified approach to interpreting model predictions », Scott Lundberg et Su-In Lee, conférence scientifique en intelligence artificielle et neurosciences computationnelles NeurIPS (*Neural Information Processing Systems*), 2017.

T1 Principales mesures de performance utilisées dans le cadre des modèles de détection de la fraude en temps réel

Taux de rappel (ou de détection) : cible à 100 %

$$\frac{\textit{Nombre de transactions frauduleuses ayant fait l'objet d'une alerte}}{\textit{Nombre de transactions frauduleuses}}$$

1/3

Un taux de rappel de 33 % signifie que 1 fraude sur 3 a été détectée par le modèle.

Taux de précision : cible à 100 %

$$\frac{\textit{Nombre de transactions frauduleuses ayant fait l'objet d'une alerte}}{\textit{Nombre d'alertes levées par le modèle}}$$

1/2

Un taux de précision de 50 % signifie que 1 alerte sur 2 est un cas réel de fraude.

F-score (ou F-mesure) : cible à 100 %

$$F = 2 * \left(\frac{\textit{Taux de précision} * \textit{taux de rappel}}{\textit{Taux de précision} + \textit{taux de rappel}} \right)$$

Le F-score (ou F1 score) est une sorte de moyenne entre la précision et le rappel, sachant que le taux de précision diminue lorsque le taux de rappel augmente. **Il s'agit d'une mesure communément utilisée pour les modèles de détection de la fraude dans les paiements.**

Taux de faux positifs : cible à 0 %

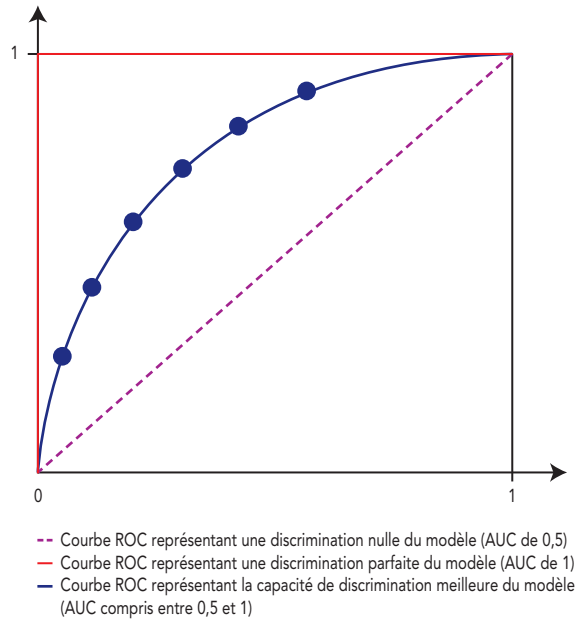
$$\frac{\textit{Nombre de transactions légitimes signalées à haut risque de fraude par le modèle}}{\textit{Nombre de transactions légitimes}}$$

1/6

Un taux de faux positifs de 16,6 % signifie que le modèle lève une alerte qui n'est pas un cas réel de fraude pour six transactions légitimes.

Source : Observatoire de la sécurité des moyens de paiement.

S4 Clés de lecture de la courbe ROC (axe horizontal : taux de faux positifs ; axe vertical : taux de détection)



Lecture : Un modèle parfait permet de repérer 100 % des cas réels de fraude pour un taux de faux positifs nul. Un modèle qui n'apporte pas de discrimination particulière détecte autant de transactions frauduleuses qu'il génère de faux positifs.
Pour comparer deux modèles, on peut comparer l'aire sous leurs courbes ROC respectives (AUC-ROC). Le modèle est parfait si son AUC est égale à 1.
Note : ROC, *Receiver Operating Characteristic*, fonction d'efficacité du récepteur ; AUC, *Area Under Curve*, aire sous la courbe ROC.
Source : Observatoire de la sécurité des moyens de paiement.

Pour chaque seuil, le taux de vrais positifs et le taux de faux positifs sont ainsi calculés et reportés sur la courbe ROC. La courbe ROC dessine l'évolution des cas réels de fraude détectés via les alertes du modèle, lorsque les x % des faux positifs ayant les notes les plus risqués sont pris en compte.

➡ Il existe une relation inverse entre l'amélioration du taux de rappel et celle du taux de précision, conduisant à un arbitrage entre le risque de ne pas détecter une opération frauduleuse (taux de rappel insuffisant) et le risque de générer trop d'alertes (taux de précision insuffisant).

➡ Par ailleurs, l'indicateur de précision est soumis à un paradoxe : dans le cas d'une baisse structurelle du taux de fraude dans un établissement donné, le taux de précision peut diminuer alors que le taux de rappel est constant, entraînant la chute du F-score. Pour autant, abandonner le modèle serait une erreur car en cas de recrudescence de la fraude, sa performance se redresserait.

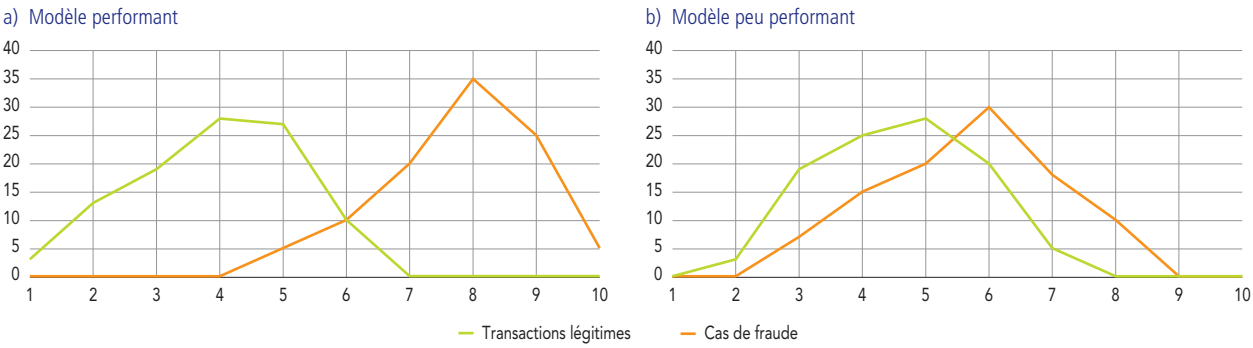
Au-delà de ces mesures, une approche directe s'appuyant sur l'étude des distributions statistiques peut s'avérer très complémentaire : la représentation graphique des scores attribués par le modèle aux transactions légitimes et aux cas de fraude permet d'apprécier très intuitivement sa performance à discriminer. Le graphique 1 illustre cette approche avec comme exemple un modèle qui discrimine sur 10 notes, de 1 à 10 (10 étant la note la plus risquée) : plus la zone de chevauchement entre les courbes représentant les cas de fraudes et les transactions légitimes est importante moins le modèle se montre efficace.

4.2.3.2 La complémentarité des modèles experts et de l'IA

La capacité prédictive des modèles experts et des modules d'IA est cumulative. En effet, la pratique a démontré qu'appliquer les modèles experts comme premier filtre de transaction et utiliser le résultat en entrée des modèles statistiques s'appuyant sur l'IA permet de détecter plus efficacement la fraude.

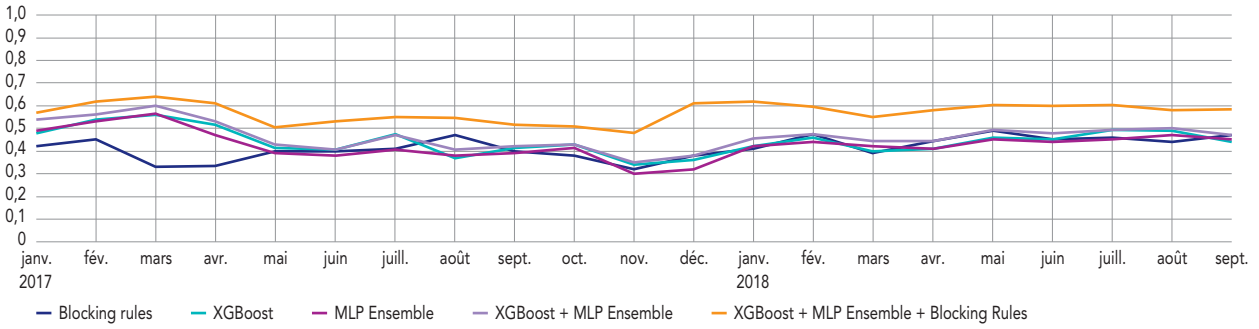
L'exemple représenté dans le graphique 2 illustre la valeur ajoutée de l'IA par rapport à un modèle expert déjà relativement performant sur la base des statistiques fournies par un contributeur de cette étude entre janvier 2017 et

G1 Deux cas de performance de modèle (en abscisse : notation du modèle, de 1 « peu risqué » à 10 « très risqué » ; en ordonnée : densité de probabilité en %)



Source : Observatoire de la sécurité des moyens de paiement.

G2 Performance de différents modèles de détection de fraude sur la carte (F-score calibré)



Note : *Blocking rules*, renvoyant au F-score du modèle expert ; XGBoost et MLP (*Multi-Layer Perceptron*), modèles d'intelligence artificielle.

Source : Observatoire de la sécurité des moyens de paiement.

septembre 2018. Le F-score du modèle expert (*Blocking Rules*) est comparable aux modèles d'IA XGBoost et MLP (*Multi-Layer Perceptron*). L'association des deux modèles d'IA ne permet toujours pas de dépasser significativement les performances du modèle expert. En revanche, l'association du modèle expert aux modèles d'IA (courbe orange) permet d'augmenter jusqu'à 50 % le F-score : ce dernier augmente ainsi de 40 % à 60 % entre novembre et décembre 2017.

4.2.3.3 Le *backtesting* et le réentraînement des modèles

Un modèle peut, après avoir été entraîné sur un ensemble de données spécifiques, s'être montré performant dans un certain contexte, puis se montrer moins efficace lorsqu'il se trouve appliqué à un environnement qui a évolué. Les types de dérives de modèles les plus couramment observés sont :

- **Le changement covarié** (*covariate shift,* aussi appelé *data drift*) : il s'agit du changement de distribution des données en entrée du modèle qui tendent à évoluer en fonction des habitudes de paiement des utilisateurs ainsi qu'avec les nouveaux procédés employés par les fraudeurs ;
- **La dérive conceptuelle** (*concept drift*) : en analyse prédictive et en apprentissage automatique, on parle de dérive conceptuelle lorsque les propriétés statistiques de la variable cible, que le modèle essaie de prédire, évoluent au cours du temps d'une manière imprévue. La relation entre la cible et les caractéristiques du modèle change et les prédictions deviennent moins exactes au fur et à mesure que le temps passe. Il s'agit d'un scénario dans lequel, par exemple, les contre-mesures mises en place par un PSP à la suite de la détection d'un nouveau schéma de fraude seraient contournées par certains fraudeurs.

Plusieurs leviers de résolution peuvent être mobilisés pour préserver la performance du modèle d'apprentissage automatique :

- si la dérive de modèle repose sur un changement covarié, corriger et améliorer la qualité des données permettront de corriger la situation ;
- en suivant régulièrement les performances des modèles par des processus de *backtesting*, il est possible d'engager des sessions de réentraînement du modèle.

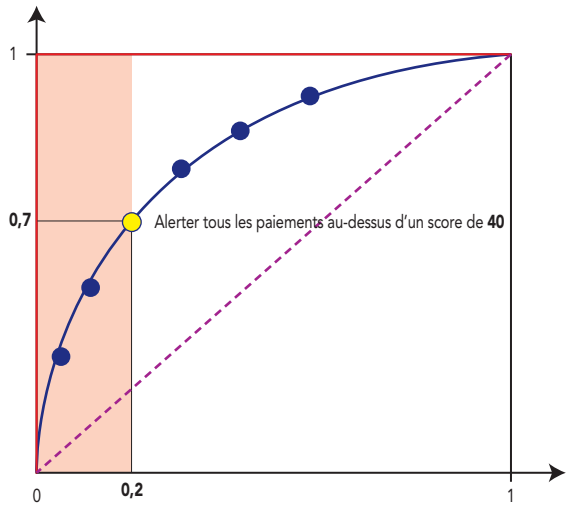
En revanche, si la correction des données ou le réentraînement ne suffit pas, il faudra alors envisager de construire un nouveau modèle.

4.3 Les enjeux métiers

La mise en place de mécanismes avancés de *scoring* nécessite une équipe de modélisateurs, qui peut soit être intégrée à l'entreprise, soit être externalisée auprès d'un prestataire spécialisé. Dans tous les cas, **il est essentiel que les équipes en charge de la modélisation et celles en charge de la gestion des opérations de paiement communiquent et coopèrent étroitement** dans le cadre de la conception et de la mise en œuvre de modèles performants.

➡ En règle générale, l'œil expert de l'humain sera plus rapide pour identifier un nouveau type d'attaque inopinée et proposer une contre-mesure adéquate. À l'inverse, dès que le type d'attaque est établi, les modèles de détection de fraude intégrant l'IA se montreront plus efficaces dans la détection des tentatives suivantes.

S5 Fixation du seuil de d'alerte en fonction du taux de *challenge* et du taux de rappel (axe des abscisses : taux de challenge ; axe des ordonnées : taux de rappel)



Lecture : Plus le seuil d'alerte est élevé, plus le point se déplace vers le bas de la courbe bleue. Dans cet exemple, fixer un seuil d'alerte à partir d'un score de 40/100 obligera le *back-office* à intervenir sur 20 % des commandes, permettant de couvrir 70 % des transactions frauduleuses.
Source : Observatoire de la sécurité des moyens de paiement.

S6 Approche Modelops

Note : Approche décrivant la gouvernance du cycle de vie d'un modèle d'intelligence artificielle.
Source : Observatoire de la sécurité des moyens de paiement.

4.3.1 Le choix du seuil de décision (ou seuil d'alerte)

Le **seuil de décision** est le seuil de notation à partir duquel les transactions feront l'objet d'une alerte. Afin de faciliter le choix par le métier, des outils adaptés aux enjeux opérationnels ont été développés. Un des outils métier les plus utilisés est directement inspiré de la courbe ROC *(cf. section 4.4.1)* et est présenté en schéma 5 :

- en abscisse, le taux d'intervention (taux de *challenge*) : il s'agit du pourcentage d'alertes à traiter par le *back-office* sur le nombre total de transactions ;
- en ordonnée, le taux de rappel : il correspond au nombre total de transactions frauduleuses ayant fait l'objet d'une alerte sur le nombre total de transactions frauduleuses.

4.3.2 La collaboration étroite entre les équipes de modélisation et le métier pour assurer l'agilité du dispositif

Face à l'évolution continue des techniques employées par les fraudeurs, une collaboration étroite est nécessaire entre les équipes en charge de la modélisation et celles en charge des opérations de paiement afin d'assurer l'agilité du dispositif de détection de la fraude.

Afin de rationaliser le développement et la mise en production de modèles pertinents, l'équipe de modélisation peut ainsi adopter les principes de l'approche *Modelops (cf. schéma 6)*. Conceptualisée par l'entreprise de recherche et de conseil Gartner, cette approche consiste à gérer le cycle de vie plus ou moins court des modèles. Les équipes de modélisation vont ainsi devoir acquérir les connaissances liées à la fraude. Il s'agit i) de comprendre les différents processus de paiement, l'origine et la signification des données disponibles ainsi que l'évolution des différentes techniques employées par les fraudeurs, et aussi ii) de communiquer efficacement avec le métier en charge des opérations.

En outre, afin de gérer au mieux la contrainte du temps, la proximité des équipes de modélisation avec le métier permet de fluidifier l'enrichissement des bases de données et de surveiller les performances des modèles. À la réception d'une nouvelle alerte, les analystes de *back-office* étudient la transaction pour déterminer s'il s'agit d'un cas réel de fraude. Si certains cas sont évidents, d'autres peuvent requérir des investigations plus approfondies. La complexité plus ou moins importante des modèles d'IA peut impliquer des demandes de renseignement récurrentes de la part des analystes vers l'équipe de modélisation afin de mieux comprendre l'origine des alertes.

Par ailleurs, dès la conception du modèle, et dans tous les cas avant sa mise en production, les équipes de modélisation doivent s'assurer auprès des services informatiques que les serveurs disposent des ressources nécessaires pour permettre le transport sécurisé de l'information et respecter les temps de calcul maximums de la note de risque qui dépendent des normes du secteur. En effet, le temps total de traitement informatique du paiement est encadré par des standards internationaux édictés par EMVco [11] pour les cartes et le Conseil européen des paiements [12] pour les instruments SEPA.

4.4 Les enjeux de conformité

La conformité des modèles de détection de la fraude en temps réel se situe au croisement de différentes réglementations et principalement : le règlement général de protection des données (RGPD) personnelles, le règlement sur l'intelligence artificielle, la directive sur les services de paiement (DSP 2) complétée par ses normes techniques de réglementation et les règles prudentielles relatives à la maîtrise des risques opérationnels [13].

4.4.1 L'absence de nouvelle contrainte règlementaire sur les processus opérationnels

La conformité au règlement européen sur la protection des données personnelles (RGPD) [14] est un enjeu essentiel pour le secteur des paiements. Son application aux données des modèles de détection de fraude en temps réel, si elle ne se fait pas sans mesures de précaution matérielle, ne soulève pas d'obstacle majeur sur le plan opérationnel :

- **La licéité de la collecte de données auprès des clients :**
  - L'article 6, paragraphe 1, point f) du RGPD précise que la collecte est licite si le « *traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement* […] » ;
  - En ce qui concerne le traitement des données sensibles (biométrie, données de paiement de prestations de santé, etc.), l'article 9, paragraphe 2, point *g*) du RGPD précise que leur utilisation n'est pas interdite si « *le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi* […] ».

  Dans les deux cas, la lutte contre la fraude constitue une finalité qui poursuit des intérêts légitimes. Cela est explicitement confirmé par la DSP 2 qui autorise dans son article 94 « *le traitement des données à caractère personnel par les systèmes de paiement et les prestataires de services de paiement lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements* » [15].

- **L'anonymisation des bases de données [16] :** le Comité européen de la protection des données (CEPD) considère que « *le traitement des données à caractère personnel strictement nécessaire à des fins de prévention de la fraude peut constituer un intérêt légitime du prestataire de services de paiement concerné, pour autant que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent pas sur ces intéressés* ».

  ➡ Les équipes de modélisation n'ont pas la nécessité de traiter des bases de données intégrant des données personnelles nominatives. Elles doivent donc être anonymisées en suivant les orientations de la Commission nationale de l'informatique et des libertés (CNIL).

- **L'autorisation de l'utilisation des données** : l'article 13, paragraphe 2, point f) du RGPD prévoit qu'au moment de la collecte des informations à caractère personnel auprès de la personne concernée, le responsable du traitement automatisé fournisse des informations sur la logique sous-jacente de l'algorithme, ainsi que l'importance et les conséquences prévues du traitement pour la personne visée. En cas de demande, seuls les grands principes doivent être expliqués, l'algorithme en lui-même pouvant demeurer confidentiel. Aussi, l'information aux personnes de l'utilisation de leurs données afin de détecter les tentatives de fraude est généralement précisée dans les contrats et conventions liés au compte et aux moyens de paiement.
- **La conservation des données** : selon le Comité européen de la protection des données (CEPD), le principe d'audibilité

11 EMVco a été créé en 1999 pour assurer au niveau mondial la gestion des spécifications EMV (Europay Mastercard Visa) qui sont des standards internationaux pour l'industrie des cartes de paiement et leur sécurité.

12 Le Conseil européen des paiements (*European Payment Council*, EPC) est une association créée en juin 2002 dans le cadre de la mise en œuvre et de la promotion du projet d'espace unique de paiement en euros (SEPA – *Single Euro Payments Area*) impulsé par l'Union européenne.

13 Selon l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement, les établissements sont tenus de maîtriser leurs risques opérationnels qui incluent notamment les risques de fraude interne et externe définis à l'article 324 du règlement (UE) n° 575/2013.

14 Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

15 L'article 94 de la DSP 2 a été transposé aux article L. 521-5 et L. 521-6 du Code monétaire et financier.

16 Comité européen à la protection des données, lignes directrices 06/2020 relatives à l'interaction entre le RGPD et la DSP 2, juin 2020.

des modèles de détection des opérations frauduleuses, exprimé par l'article 3 du règlement délégué 2018/389 de la Commission européenne en matière d'authentification forte [17], en raison de sa légitimité explicite, est « opposable » à l'article 17 du RGPD sur le droit à l'oubli et à l'article 18 du même texte sur la limitation du traitement des données à caractère personnel.

- **L'impact complet du règlement européen sur l'intelligence artificielle du 13 juin 2024** n'a pas encore été totalement appréhendé, mais aucune prévention majeure relative à l'utilisation des algorithmes de notation des transactions de paiement n'a été relevée par les contributeurs à la présente étude de l'Observatoire.

4.4.2 Les enjeux issus de la DSP 2

La DSP 2 incite les PSP à mettre en œuvre des modèles de détection de la fraude en temps réel, notamment pour pouvoir appliquer une exemption à l'authentification forte. Dans son projet de règlement sur les services de paiement (RSP), la Commission européenne souhaite également conforter et préciser cette incitation. Pour cela, des mécanismes de contrôle des opérations, la Commission en fait un pilier indispensable de la sécurité des paiements et complémentaire de l'authentification forte [18]. Aussi, le futur règlement européen pourrait-il faciliter le partage de données liées à des cas de fraude entre les PSP, aujourd'hui contraint par certains aspects du RGPD et de la loi sur le secret bancaire [19]. Ce partage de données entre les PSP pourrait ainsi enrichir les modèles respectifs de détection de la fraude.

4.4.2.1 La dérogation à l'authentification forte comme facteur de fluidification des paiements

Dans le cadre de l'application de la DSP 2, une exemption à l'authentification forte nommée « analyse des risques liés à l'opération » (*Transaction Risk Analysis*, TRA) est prévue par l'article 18 du règlement délégué 2018/389 de l'Autorité bancaire européenne (ABE), sous réserve que le PSP qui sollicite l'application de l'exemption présente un taux de fraude inférieur à un seuil défini en annexe du même règlement. Les conditions exactes de mise en œuvre de l'exemption TRA ont été rappelées par l'Observatoire dans son rapport annuel 2022 *(cf. section 4.1.3)*.

➡ Les analyses TRA à des fins d'exemption à l'authentification forte peuvent notamment être réalisées à partir de modules d'intelligence artificielle par certains acteurs et ont pour conséquence concrète de fluidifier l'exécution des transactions par les clients dans un cadre sécurisé.

4.4.2.2 Le partage de l'annotation de fraude relative aux transactions soumises à authentification forte par le PSP émetteur

La DSP 2 confère au PSP du payeur la responsabilité de la sécurité des opérations de paiement, avec notamment la responsabilité de remboursement en cas d'opération non autorisée. À ce titre, l'appréciation d'un faible niveau de risque est une condition nécessaire pour accorder une exemption à l'authentification forte, et doit pouvoir s'appuyer sur les informations relatives à l'opération transmises par le commerçant et son accepteur.

➡ Les PSP émetteurs doivent veiller, dans la mesure du possible, à informer les autres acteurs de la chaîne des paiements, notamment les accepteurs et les commerçants, des cas de fraude qui les concernent directement afin que ceux-ci puissent améliorer la performance de leurs propres modèles de détection de la fraude. Cette coopération peut aussi inciter les accepteurs et les commerçants à surveiller la qualité des données véhiculées dans les flux de paiement aux PSP.

4.5 Recommandations

À la suite de cette étude de veille, l'Observatoire de la sécurité des moyens de paiement émet les trois recommandations suivantes concernant l'utilisation des modules d'intelligence artificielle dans les dispositifs de lutte contre la fraude des acteurs de la chaîne des paiements.

17 Règlement délégué (UE) 2018/389 de la Commission européenne du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de règlementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

18 Considérant (100) de la proposition de règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) n° 1093/2010 (RSP), 28 juin 2023.

19 Le secret bancaire désigne l'obligation légale, à laquelle est tenue une banque, de ne pas divulguer à des tiers les données qu'elle détient sur son client. Le secret bancaire a été instauré en France par la loi n° 84-46 du 24 janvier 1984, dite « loi bancaire », et aujourd'hui repris à l'article L. 511-33 du Code monétaire et financier.

Recommandation n° 1 :

Explorer à des fins de lutte contre la fraude l'apport de modules d'intelligence artificielle pour les modèles de contrôle et de notation des opérations de paiement

L'Observatoire appelle les différents acteurs de la chaîne des paiements à évaluer l'opportunité d'intégrer des technologies d'intelligence artificielle dans leurs dispositifs d'analyse des risques de fraude en temps réel, en complément de leur approche préexistante.

Recommandation n° 2 :

Optimiser le périmètre de données utilisées dans les modèles de contrôle et de notation des opérations de paiement

L'Observatoire enjoint aux acteurs de la chaîne des paiements de valoriser l'ensemble des données exploitables dans leurs dispositifs d'analyse de risque :

- i) en veillant en particulier à la qualité et à l'exhaustivité des données échangées dans les messages de paiement, dans le respect des standards applicables (EMVco, *European Payment Council* – EPC, etc.) ;
- et ii) en prenant en compte les informations issues de mécanismes de partage existants (par exemple les notations de risque issues des systèmes de paiement interbancaires, ou les informations fournies au moyen d'interfaces communes par les opérateurs téléphoniques) ou à venir (telles que le service de vérification du bénéficiaire ou les mécanismes de partage de données de fraude prévus dans les futures règlementations nationales et européennes).

Recommandation n° 3 :

Instaurer un pilotage des modèles de contrôle et de notation des opérations de paiement reposant sur l'IA

L'Observatoire appelle les acteurs de la chaîne des paiements à évaluer par des méthodes de *backtesting*, au moins une fois par an, l'efficacité de leurs modèles de notation intégrant des modules d'IA en s'appuyant sur des indicateurs quantitatifs (du type de ceux proposés en partie 2.3), ainsi que sur une expertise qualitative complémentaire faisant intervenir les analystes en charge des opérations. À ce titre, il est essentiel de veiller à ce que les méthodologies, les évaluations et les contrôles associés aux modèles soient documentés, intelligibles et explicables.

ANNEXES

A1	Conseils de prudence pour l'utilisation des moyens de paiement	75
A2	Missions et organisation de l'Observatoire	88
A3	Liste nominative des membres de l'Observatoire	90
A4	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux	93
A5	Dossier statistique sur l'usage et la fraude aux moyens de paiement	103

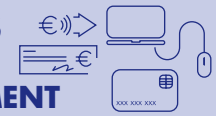
A1 CONSEILS DE PRUDENCE POUR L'UTILISATION DES MOYENS DE PAIEMENT

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 principales typologies de fraude rencontrées 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

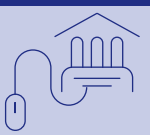


▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

- 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

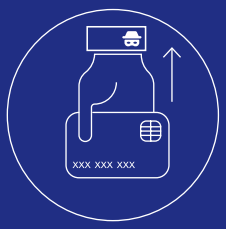
- Pour accéder à votre banque en ligne, choisissez un navigateur internet connu, un moteur de recherche de confiance et pour les accès sur *smartphone* téléchargez l'application bancaire sur les magasins officiels d'applications.
- N'accédez pas à votre banque en ligne depuis un ordinateur public ou 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*

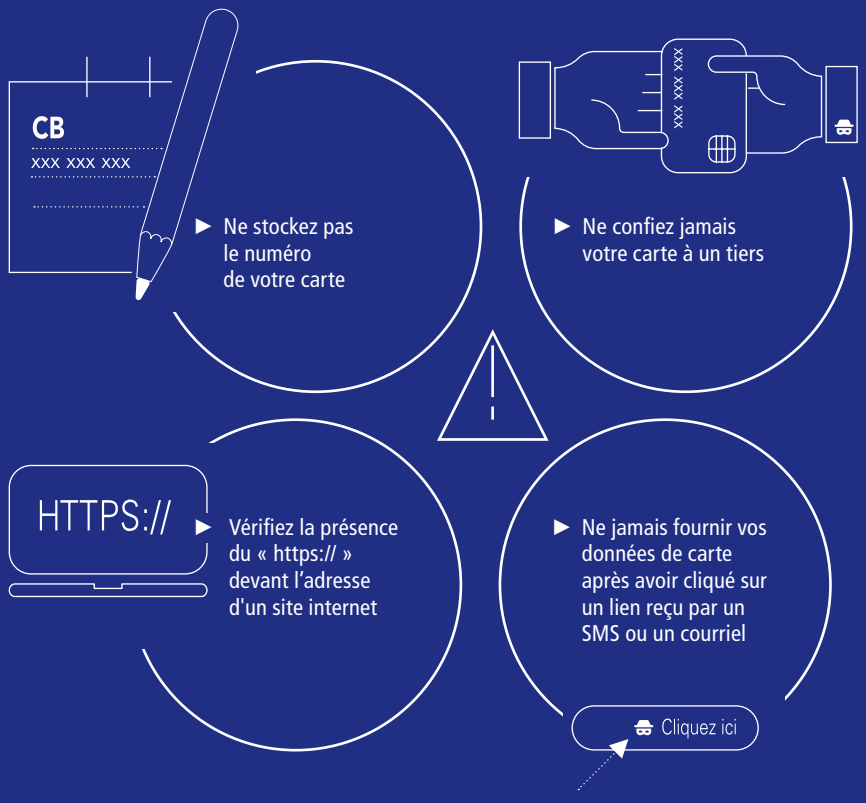


Vol de carte

Manipulation psychosociale

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

CONSEILS À DESTINATION DES UTILISATEURS



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.

▷ 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 votre litige au médiateur** désigné par votre banque à partir de deux mois après la date de votre première demande 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 à votre banque, au médiateur ou votre avocat, de la même manière que vous le feriez pour les forces de l'ordre.

FICHE 4

CONSEILS APPLICABLES AUX VIREMENTS

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Ingénierie sociale

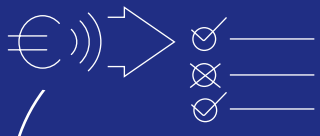
Logiciels malveillants

Campagnes
de *phishing* et *smishing*

CONSEILS À DESTINATION DES UTILISATEURS

► N'ajoutez que les personnes de confiance comme bénéficiaire sur votre espace de banque en ligne

► 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.
- 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 optionnels 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.).

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 et à mettre à jour dans votre espace de banque en ligne la liste des créanciers autorisés (appelée aussi « liste blanche ») ou interdits (appelée aussi « liste noire »).

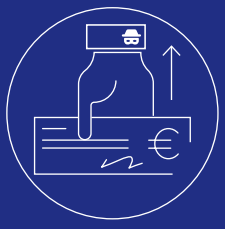
- Faites preuve de vigilance sur la communication de votre IBAN en la réservant à vos créanciers de confiance.

- 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

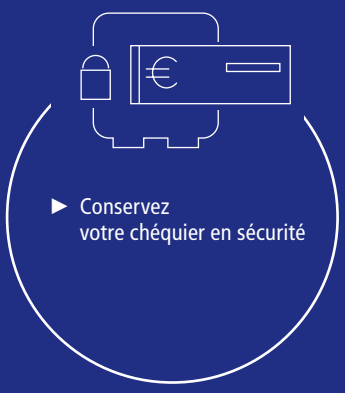
Falsification
d'un chèque

Contrefaçon
d'un chèque

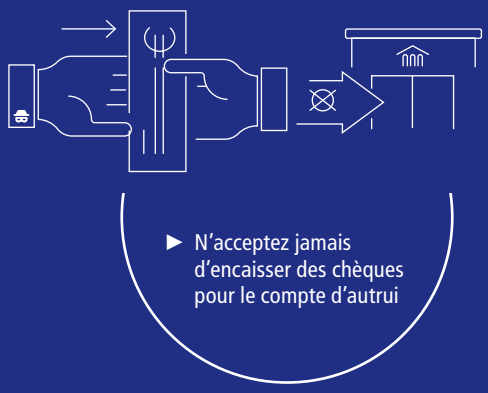
Fraude à la « mule »

CONSEILS À DESTINATION DES UTILISATEURS

► Privilégiez la remise de chéquiers en agence

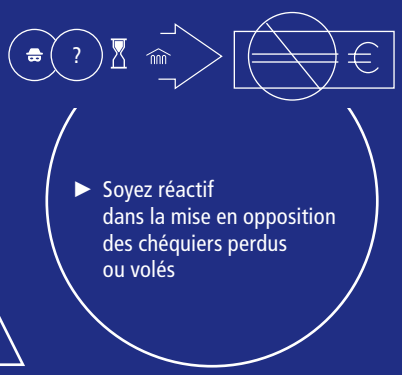


► Conservez votre chéquier en sécurité



► 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 lui-même (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

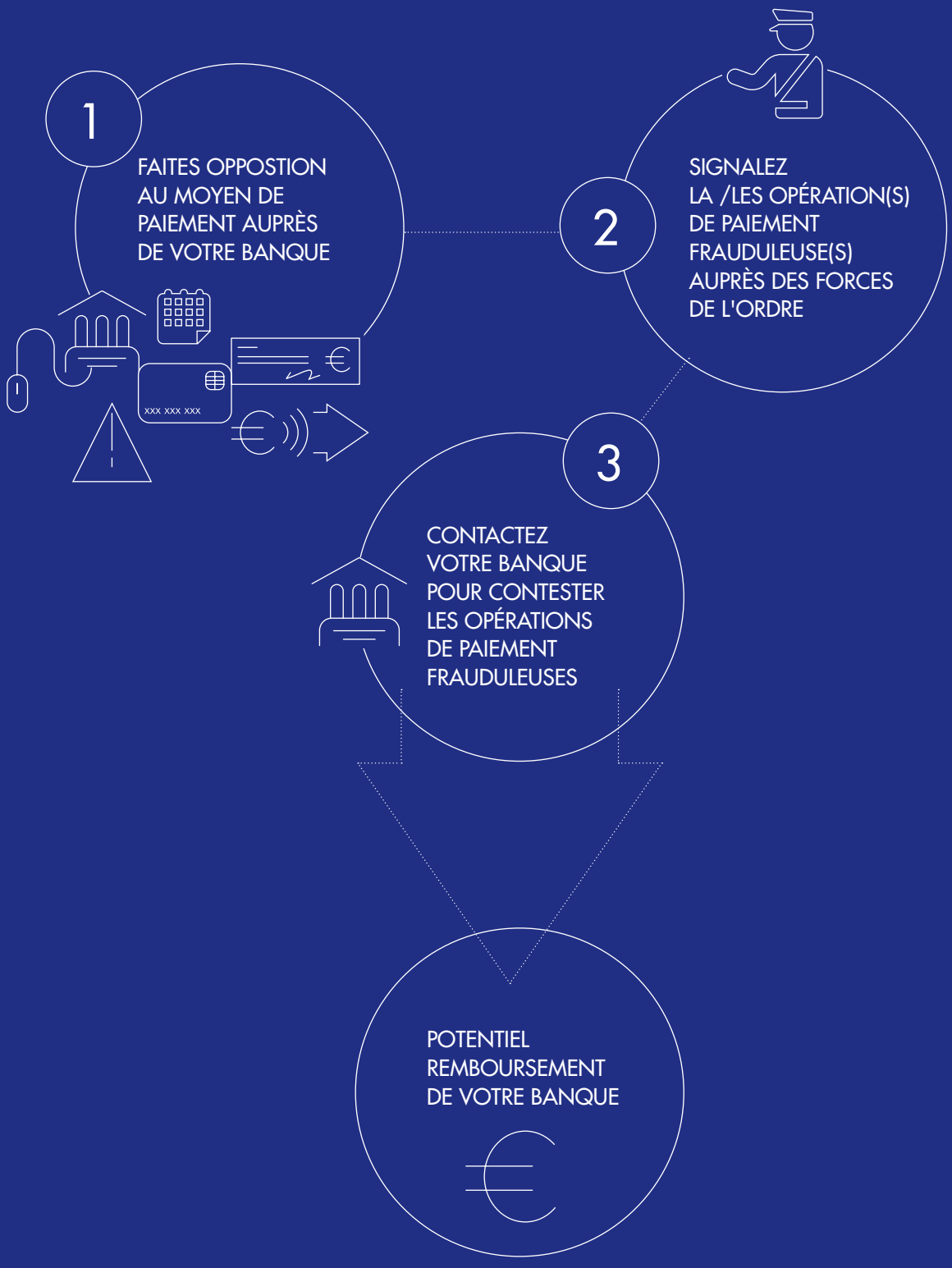
- Remise de chèques frauduleux à des bénéficiaires légitimes contre la remise de biens et de services (commerçants, sociétés de location, etc.)
- Processus de « cavalerie » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement d'un décaissement des fonds par 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 »).

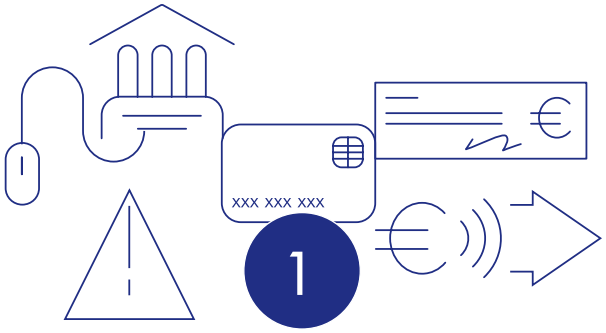
▷ CONSEILS À DESTINATION DE TOUS LES UTILISATEURS DE CHÈQUES

- 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.


1
FAITES OPPOSTION AU MOYEN DE PAIEMENT AUPRÈS DE VOTRE BANQUE
xxx xxx xxx
2
SIGNALEZ LA /LES OPÉRATION(S) DE PAIEMENT FRAUDULEUSE(S) AUPRÈS DES FORCES DE L'ORDRE
3
CONTACTEZ VOTRE BANQUE POUR CONTESTER LES OPÉRATIONS DE PAIEMENT FRAUDULEUSES
POTENTIEL REMBOURSEMENT DE VOTRE BANQUE



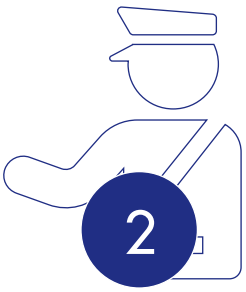
FAIRE OPPOSITION

- **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 les démarches sur les plateformes Perceval pour les fraudes à la carte bancaire sur internet et Thésée [1] pour les autres arnaques et escroqueries sur internet, notamment dans le cas des fraudes au virement.

- **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.**

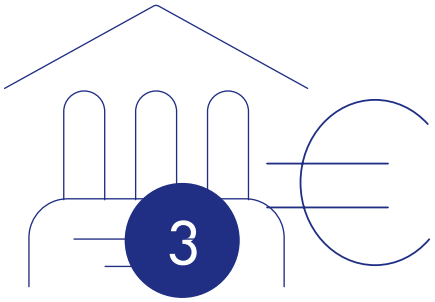
  Toutefois, l'utilisateur peut aussi porter plainte auprès d'un commissariat de police ou d'une unité de gendarmerie en cas de vol de son moyen de paiement et en cas d'utilisation frauduleuse de celui-ci ou des données qui lui sont liées. Afin de gagner du temps lors du rendez-vous, une pré-plainte en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

.../...

1 Perceval – Plateforme électronique de recueil de coordonnées bancaires ;
Thésée – Traitement harmonisé des enquêtes et signalements pour les e-escroqueries.



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,
  - démarches Perceval ou Thésée (transmettre le récépissé),
  - le cas échéant, car non obligatoire, dépôt de plainte auprès des forces de l'ordre, etc.

▼ En pratique

- Allez sur les **plateformes en ligne Perceval** pour les signalements relatifs à une fraude à la carte de paiement sur internet **ou Thésée** pour signaler les escroqueries sur internet, notamment dans le cas de fraude au virement ;
- 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**.

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 [2] 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 pourrait 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 deux mois, sauf dispositions plus contraignantes [3].

En cas de réponse défavorable, vous pouvez gratuitement soumettre votre litige au médiateur de la consommation désigné par votre banque à partir de deux mois après la date de votre première demande et dans un délai d'un an.

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 votre litige au médiateur** désigné par votre banque à partir de deux mois après la date de votre première demande 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.

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

3 Recommandations 2022-R-01 du 9 mai 2022 de l'Autorité de contrôle prudentiel et de résolution (ACPR) sur le traitement des réclamations.

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 R. 141-1, R. 141-2 et R. 142-22 à R. 142-27 du Code monétaire et financier.

PÉRIMÈTRE CONCERNÉ

En application de l'article 65 de la loi n° 2016-1691 du 9 décembre 2016 et conformément à la stratégie nationale des moyens de paiement, l'article L. 141-4 du Code monétaire et financier a été modifié en élargissant la mission de l'Observatoire de la sécurité des cartes de paiement à l'ensemble des moyens de paiement scripturaux. La compétence de l'Observatoire de la sécurité des moyens de paiement couvre donc désormais, en plus des cartes émises par les prestataires de services de paiement ou par les institutions assimilées, tous les autres moyens de paiement scripturaux.

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 12 mai 2025.

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 :
  Nathalie AUFAUVRE

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) :
  Ivan ODONNAT
- 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 :
  Étienne LESTRELIN

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

Alexandra ZANA
Mastercard France

Philippe LAULANIE
Groupement des cartes bancaires

Romain BOISSON
Visa Europe France

Régis FOLBAUM
STET

Pierre-Emmanuel DEGERMANN
Worldline

Narinda YOU
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)

Vincent DEPRIESTER
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).

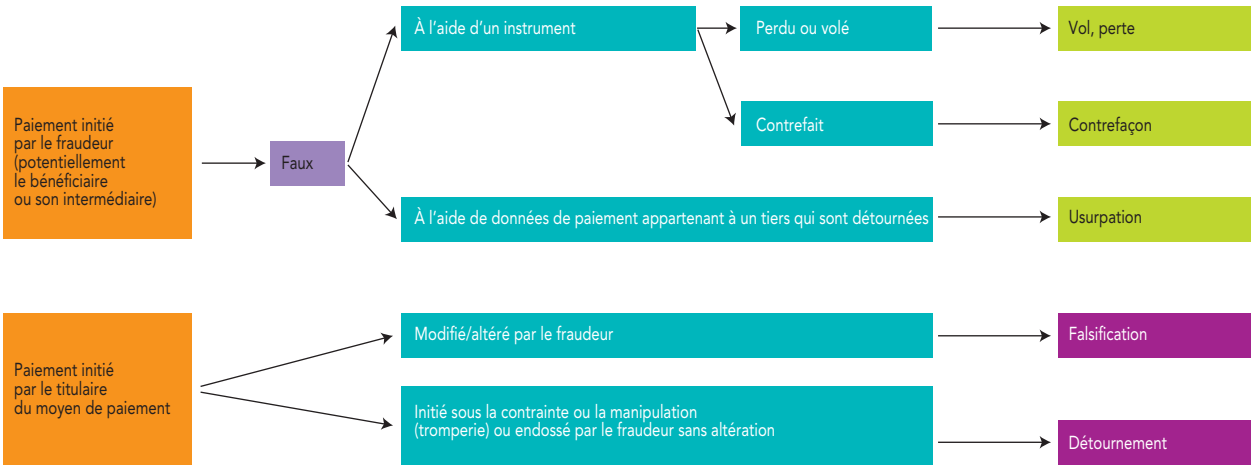
Par ailleurs, l'approche retenue pour évaluer la fraude est celle dite de la « fraude brute » qui consiste à retenir le montant initial des opérations de paiement sans prendre en compte les mesures qui peuvent être prises ultérieurement par les contreparties en vue de réduire le préjudice (par exemple, 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 « DSP 2 »).

Présentation schématique des différentes typologies de fraude



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 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 3D-Secure avec authentification forte	Paiement réalisé sur internet, en dehors de l'infrastructure 3D-Secure, avec une authentification forte déléguée à un tiers, conformément aux règles d'externalisation applicables dans le cadre de la DSP 2 (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 deuxième directive européenne sur les services de paiement (DSP 2) 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 (DSP 2) [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 DSP 2 : 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

Instruments de paiement couverts

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 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

Instruments de paiement couverts

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 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.

Origines 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.

Les totaux de fraude au chèque sont calculés d'après la nouvelle approche de fraude brute, qui prend en compte les fraudes déjouées après présentation du chèque au paiement. Toutefois, même à partir de 2021, les ventilations de fraude au chèque par typologie, quant à elles, sont effectuées à partir de l'ancienne approche de fraude brute.

Typologie de 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

Instruments de paiement couverts

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

Service de paiement couvert

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 (DSP 2). 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

Service de paiement couvert

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 DSP 2. 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

Instruments de paiement couverts

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/2025-09/rapport-osmp-2024_dossier-statistique_annexe-5.pdf

PANORAMA DES MOYENS DE PAIEMENT

T1 Cartographie des moyens de paiement scripturaux en 2024

(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
	2024	Variation 2024/2023	Part	2024	Variation 2024/2023	Part	
Paiement carte [a]	20 982	6,6	62,1	844	4,6	2,4	40
dont sans contact	*11 454*	*6,1*	*33,9*	*204*	*16,7*	*0,6*	*18*
dont paiement par mobile	*2 473*	*53,6*	*7,3*	*56*	*57,6*	*0,2*	*23*
Chèque	784	- 12,1	2,3	392	- 16,1	1,1	500
Virement	5 973	6,4	17,7	31 108	3,9	89,2	5 209
dont VGM [b]	*11*	*- 64,1*	*0,0*	*10 408*	*22,0*	*29,9*	*976 136*
dont virement instantané (SCT Inst)	*598*	*46,5*	*1,8*	*231*	*30,6*	*0,7*	*387*
Prélèvement	4 788	3,7	14,2	2 178	1,9	6,2	455
Effet de commerce	70	- 4,8	0,2	205	- 5,6	0,6	2 926
Monnaie électronique	98	11,2	0,3	1	25,9	0,0	13
Transmission de fonds	12	51,6	0,0	1	32,4	0,0	128
Total	**32 707**	**5,6**	**96,8**	**34 730**	**3,4**	**99,6**	**1 062**
Retrait par carte [a]	1 079	- 4,2	3,2	133	- 1,6	0,4	124
Total transactions	**33 787**	**5,2**	**100,0**	**34 864**	**3,4**	**100,0**	**1 032**

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 : 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)

	2017	2018	2019	2020	2021	2022	2023	2024
Carte	12 581	13 179	14 485	13 852	16 129	18 258	19 685	20 982
dont sans contact	*1 300*	*2 374*	*3 779*	*5 159*	*7 369*	*9 103*	*10 792*	*11 454*
dont par mobile	*5*	*11*	*48*	*129*	*357*	*845*	*1 609*	*2 473*
Chèque	1 927	1 747	1 587	1 175	1 106	1 008	891	784
Virement	3 870	4 038	4 269	4 483	4 843	5 158	5 613	5 973
dont virement instantané (SCT Inst)	*nd*	*0*	*14*	*45*	*107*	*198*	*408*	*598*
Prélèvement	4 091	4 211	4 370	4 622	5 020	4 914	4 616	4 788
Effet de commerce	81	81	78	71	75	75	74	70
Monnaie électronique	55	65	62	36	63	75	88	98
Transmission de fonds	18	16	16	15	2	3	8	12
Total paiements scripturaux	**22 605**	**23 320**	**24 851**	**24 238**	**27 238**	**29 491**	**30 975**	**32 707**
Retrait par carte	1 481	1 439	1 392	1 064	1 086	1 136	1 127	1 079
Total transactions	**24 086**	**24 759**	**26 243**	**25 302**	**28 324**	**30 627**	**32 102**	**33 787**

b) En montant

(en milliards d'euros)

	2017	2018	2019	2020	2021	2022	2023	2024
Carte	530	568	600	578	660	746	806	844
dont sans contact	*13*	*25*	*43*	*80*	*125*	*148*	*175*	*204*
dont par mobile	*0,1*	*0,2*	*1*	*3*	*8*	*18*	*36*	*56*
Chèque	1 002	891	814	614	589	540	467	392
Virement	24 069	24 296	25 164	32 712	38 723	38 895	29 942	31 108
dont virement instantané (SCT Inst)	*nd*	*0,086*	*7*	*27*	*50*	*119*	*177*	*231*
Prélèvement	1 579	1 645	1 711	1 684	1 895	2 041	2 139	2 178
Effet de commerce	260	252	232	197	212	222	218	205
Monnaie électronique	1	1	1	1	1	1	1	1
Transmission de fonds	1,6	2	2	2	1	1	1	1
Total paiements scripturaux	**27 440**	**27 653**	**28 522**	**35 786**	**42 081**	**42 445**	**33 574**	**34 730**
Retrait par carte	135	137	137	116	124	133	136	133
Total transactions	**27 575**	**27 789**	**28 658**	**35 902**	**42 204**	**42 578**	**33 710**	**34 864**

nd, non disponible.

Note : 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 2024

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

	Volume			Valeur			Taux de fraude	Montant moyen
	2024	Variation 2024/2023	Part	2024	Variation 2024/2023	Part	2024	
Paiement carte [a]	7 313 235	10,2	94,0	478 062 959	5,0	40,2	0,0567	65
dont sans contact	*746 923*	*1,8*	*9,6*	*22 648 147*	*20,6*	*1,9*	*0,0111*	*30*
dont par mobile	*129 052*	*17,2*	*1,7*	*9 023 196*	*23,7*	*0,8*	*0,0161*	*70*
Chèque (nouvelle approche) [b]	173 366	- 15,9	2,2	270 317 625	- 25,7	22,7	0,0689	1 559
Chèque (ancienne approche)	215 576	- 15,7	2,8	457 332 103	- 22,2	38,5	0,1166	2 121
Virement	132 298	46,3	1,7	350 992 884	12,3	29,5	0,0011	2 653
dont virement instantané (SCT Inst)	*80 394*	*65,3*	*1,0*	*105 718 759*	*53,2*	*8,9*	*0,0457*	*1 315*
Prélèvement	52 718	- 32,3	0,7	30 365 272	36,0	2,6	0,0014	576
Effet de commerce	350	929,4	0,0	18 037 208	1 291,1	1,5	0,0088	51 535
Monnaie électronique	3 232	3,1	0,0	95 876	- 45,6	0,0	0,0077	30
Transmission de fonds	86	- 15,7	0,0	17 796	- 67,8	0,0	0,0012	207
Total paiements	**7 675 285**	**9,4**	**98,6**	**1 147 889 620**	**- 0,7**	**96,6**	**0,0033**	**150**
Retrait par carte [a]	108 013	- 2,0	1,4	40 763 581	0,4	3,4	0,0306	377
Total transactions	**7 783 298**	**9,3**	**100,0**	**1 188 653 201**	**- 0,6**	**100,0**	**0,0034**	**153**

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 : 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)

	2017	2018	2019	2020	2021	2022	2023	2024
Carte	5 364 312	6 068 959	7 071 095	7 421 137	6 764 752	6 692 988	6 635 955	7 313 235
dont sans contact	*248 991*	*445 919*	*603 509*	*537 061*	*604 278*	*796 027*	*733 359*	*746 923*
dont par mobile	*22*	*2 070*	*3 494*	*33 761*	*83 266*	*162 869*	*110 133*	*129 052*
Chèque (nouvelle approche)	nd	nd	nd	190 001	232 277	218 122	206 197	173 366
Chèque (ancienne approche)	114 906	166 421	183 488	220 685	272 970	266 216	255 857	215 576
Virement	4 642	7 736	15 934	35 893	46 718	76 846	90 453	132 298
dont virement instantané (SCT Inst)	*nd*	*5*	*729*	*7 131*	*12 913*	*33 193*	*48 630*	*80 394*
Prélèvement	25 801	309 377	43 519	6 485	251 010	49 453	77 876	52 718
Effet de commerce	3	5	1	62	1	1	34	350
Monnaie électronique	nd	nd	nd	nd	2 001	1 945	3 135	3 232
Transmission de fonds	nd	nd	nd	nd	962	154	102	86
Total fraude paiements scripturaux	**5 509 664**	**6 552 498**	**7 314 037**	**7 684 262**	**7 297 721**	**7 039 509**	**7 013 752**	**7 675 285**
Retrait par carte	177 562	158 908	165 505	113 067	129 083	123 574	110 221	108 013
Total fraude transactions	**5 687 226**	**6 711 406**	**7 479 542**	**7 797 329**	**7 426 804**	**7 163 083**	**7 123 973**	**7 783 298**

nd, non disponible.
Note : 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.

b) En valeur
(en euros)

	2017	2018	2019	2020	2021	2022	2023	2024
Carte	344 962 084	401 604 986	428 249 931	439 489 315	421 410 285	420 585 823	455 204 894	478 062 959
dont sans contact	*2 748 790*	*5 234 852*	*8 479 354*	*11 292 261*	*16 274 668*	*23 047 180*	*18 786 086*	*22 648 147*
dont par mobile	*1 227*	*73 682*	*216 236*	*2 792 574*	*5 610 270*	*10 942 984*	*7 294 895*	*9 023 196*
Chèque (nouvelle approche)	nd	nd	nd	401 611 189	465 021 167	395 416 196	363 929 512	270 317 625
Chèque (ancienne approche)	296 072 847	450 108 464	539 215 175	538 059 139	625 703 442	556 796 815	588 194 101	457 332 103
Virement	78 286 492	97 327 128	161 642 174	266 969 099	287 264 068	313 163 442	312 487 450	350 992 884
dont virement instantané (SCT Inst)	*nd*	*29 800*	*2 203 240*	*10 562 419*	*22 406 942*	*52 768 218*	*69 003 730*	*105 718 759*
Prélèvement	8 726 403	58 346 253	10 990 025	1 891 051	25 318 677	19 853 012	22 320 813	30 365 272
Effet de commerce	153 100	226 217	74 686	538 918	12 079	12 079	1 296 652	18 037 208
Monnaie électronique	nd	nd	nd	nd	137 340	77 349	176 276	95 876
Transmission de fonds	nd	nd	nd	nd	246 362	77 162	55 333	17 796
Total fraude paiements scripturaux	**728 200 926**	**1 007 613 048**	**1 140 171 991**	**1 246 947 522**	**1 199 409 978**	**1 149 185 062**	**1 155 470 930**	**1 147 889 620**
Retrait par carte	42 038 924	37 630 659	41 651 788	33 950 879	42 950 169	43 148 054	40 608 913	40 763 581
Total fraude transactions	**770 239 850**	**1 045 243 707**	**1 181 823 779**	**1 280 898 401**	**1 242 360 147**	**1 192 333 116**	**1 196 079 843**	**1 188 653 201**

nd, non disponible.
Note : 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
(volume en milliers, montant en milliers d'euros)

	2019		2020		2021	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**12 171 755**	**459 066 750**	**11 193 795**	**424 105 649**	**12 935 438**	**475 079 750**
dont paiements sans contact (y compris paiements par mobile)	*3 778 756*	*42 903 452*	*5 159 657*	*79 664 370*	*7 368 699*	*125 082 420*
dont paiements par mobile	*47 885*	*850 983*	*129 105*	*2 734 667*	*357 355*	*7 596 769*
Paiements à distance (hors internet)	**77 150**	**4 838 911**	**134 114**	**7 567 877**	**76 931**	**7 995 010**
Paiements sur internet	**2 236 049**	**135 352 563**	**2 524 317**	**146 563 476**	**3 116 285**	**177 056 237**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*444 723*	*19 267 910*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*1 883 898*	*72 566 685*
Retraits	**1 391 930**	**136 507 651**	**1 064 095**	**115 958 207**	**1 086 289**	**123 867 648**
Total	**15 876 884**	**735 765 875**	**14 916 322**	**694 195 208**	**17 214 942**	**783 998 644**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T5 Paiements par carte émise en France (suite)
(volume en milliers, valeur en milliers d'euros)

	2022		2023		2024	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**14 868 338**	**537 503 850**	**15 903 747**	**570 896 450**	**16 742 186**	**586 501 562**
dont paiements sans contact (y compris paiements par mobile)	*9 102 931*	*148 006 593*	*10 792 452*	*174 706 103*	*11 453 514*	*203 943 905*
dont paiements par mobile	*845 223*	*17 937 091*	*1 609 423*	*35 539 253*	*2 472 705*	*56 018 195*
Paiements à distance (hors internet)	**105 781**	**16 994 865**	**96 368**	**15 880 261**	**95 683**	**14 871 495**
Paiements sur internet	**3 283 604**	**191 418 128**	**3 685 180**	**219 662 525**	**4 144 523**	**242 158 676**
dont paiements 3-D Secure avec authentification forte	*1 034 950*	*112 713 734*	*1 282 644*	*136 151 668*	*1 153 075*	*139 292 722*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*135 611*	*4 119 307*	*382 740*	*14 661 163*
dont paiements 3-D Secure sans authentification forte	*781 313*	*27 091 534*	*800 728*	*27 212 160*	*896 289*	*31 855 769*
dont paiements hors 3-D Secure sans authentification forte	*1 467 342*	*51 612 860*	*1 466 199*	*52 179 389*	*1 712 419*	*56 349 021*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*877 839*	*30 771 262*	*1 032 022*	*33 940 666*
dont paiements « one-leg »	*nd*	*nd*	*31 151*	*1 997 096*	*43 267*	*2 235 967*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*250 843*	*9 039 674*	*254 557*	*8 025 476*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*306 366*	*10 371 359*	*382 573*	*12 146 912*
Retraits	**1 135 675**	**132 879 066**	**1 127 043**	**135 511 148**	**1 079 441**	**133 312 840**
Total	**19 393 398**	**878 795 909**	**20 812 338**	**941 950 384**	**22 061 834**	**976 844 573**

nd, non disponible.

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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

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

	2019			2020			2021		
	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	**1 203 233**	**64 992 145**	**0,014**	**972 228**	**47 994 762**	**0,011**	**942 376**	**52 426 587**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	*603 509*	*8 479 354*	*0,020*	*537 061*	*11 292 261*	*0,014*	*604 278*	*16 274 668*	*0,013*
dont paiements par mobile	*3 494*	*216 236*	*0,025*	*33 761*	*2 792 574*	*0,102*	*83 266*	*5 610 270*	*0,074*
Paiements à distance (hors internet)	**409 319**	**31 806 788**	**0,657**	**411 344**	**26 899 103**	**0,355**	**124 596**	**22 193 382**	**0,278**
Paiements sur internet	**5 458 543**	**331 450 998**	**0,245**	**6 037 565**	**364 595 450**	**0,249**	**5 697 780**	**346 790 316**	**0,196**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*364 223*	*26 046 078*	*0,135*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*4 837 540*	*217 714 555*	*0,300*
Retraits	**165 505**	**41 651 788**	**0,031**	**113 067**	**33 950 879**	**0,029**	**129 083**	**42 950 169**	**0,035**
Total	**7 236 600**	**469 901 719**	**0,064**	**7 534 204**	**473 440 194**	**0,068**	**6 893 835**	**464 360 454**	**0,059**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T6 Transactions frauduleuses par carte émise en France (suite)

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

	2022			2023			2024		
	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	**1 055 575**	**62 861 464**	**0,012**	**966 134**	**61 618 923**	**0,011**	**943 105**	**62 951 625**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	*796 027*	*23 047 180*	*0,016*	*733 359*	*18 786 086*	*0,011*	*746 923*	*22 648 147*	*0,011*
dont paiements par mobile	*162 869*	*10 942 984*	*0,061*	*110 133*	*7 294 895*	*0,021*	*129 052*	*9 023 196*	*0,016*
Paiements à distance (hors internet)	**174 364**	**42 028 102**	**0,247**	**186 499**	**42 177 372**	**0,266**	**183 666**	**40 377 262**	**0,272**
Paiements sur internet	**5 463 049**	**315 696 257**	**0,165**	**5 483 322**	**351 408 599**	**0,160**	**6 186 464**	**374 734 072**	**0,155**
dont paiements 3-D Secure avec authentification forte	*624 473*	*124 258 815*	*0,110*	*722 396*	*132 754 198*	*0,098*	*676 055*	*128 822 135*	*0,092*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*159 680*	*8 966 661*	*0,218*	*189 142*	*11 192 865*	*0,076*
dont paiements 3-D Secure sans authentification forte	*625 296*	*25 695 176*	*0,095*	*593 808*	*22 929 848*	*0,084*	*449 128*	*17 294 653*	*0,054*
dont paiements hors 3-D Secure sans authentification forte	*4 213 280*	*165 742 266*	*0,321*	*4 007 438*	*186 757 892*	*0,358*	*4 872 139*	*217 424 419*	*0,386*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*1 995 881*	*87 685 148*	*0,285*	*2 487 438*	*106 598 193*	*0,314*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*416 116*	*30 632 806*	*1,534*	*651 446*	*43 751 776*	*1,957*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*553 018*	*16 515 229*	*0,183*	*516 679*	*13 485 307*	*0,168*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*1 042 423*	*51 924 709*	*0,501*	*1 216 576*	*53 589 143*	*0,441*
Retraits	**123 574**	**43 148 054**	**0,032**	**110 221**	**40 608 913**	**0,030**	**108 013**	**40 763 581**	**0,031**
Total	**6 816 562**	**463 733 877**	**0,053**	**6 746 176**	**495 813 807**	**0,053**	**7 421 248**	**518 826 540**	**0,053**

nd, non disponible.

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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 2024

(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	**641 803**	**68,1**	**37 605 552**	**59,7**	**9 883**	**1,0**	**1 434 341**	**2,3**	**112 006**	**11,9**	**8 507 879**	**13,5**
dont paiements sans contact (y compris paiements par mobile)	*532 917*	*71,3*	*13 271 574*	*58,6*	*3 916*	*0,5*	*83 663*	*0,4*	*86 689*	*11,6*	*4 810 958*	*21,2*
dont paiements par mobile	*53 737*	*41,6*	*3 769 237*	*41,8*	*287*	*0,2*	*16 688*	*0,2*	*40 215*	*31,2*	*3 308 416*	*36,7*
Paiements à distance (hors internet)	**17 076**	**9,3**	**3 683 722**	**9,1**	**76**	**0,0**	**8 922**	**0,0**	**618**	**0,3**	**174 492**	**0,4**
Paiements sur internet	**348 324**	**5,6**	**26 141 227**	**7,0**	**4 636**	**0,1**	**294 559**	**0,1**	**128 069**	**2,1**	**7 198 422**	**1,9**
dont paiements 3-D Secure avec authentification forte	*38 007*	*5,6*	*8 308 430*	*6,4*	*649*	*0,1*	*137 504*	*0,1*	*1 039*	*0,2*	*225 670*	*0,2*
dont paiements hors 3-D Secure avec authentification forte	*4 861*	*2,6*	*305 371*	*2,7*	*348*	*0,2*	*17 116*	*0,2*	*97*	*0,1*	*7 978*	*0,1*
dont paiements 3-D Secure sans authentification forte	*51 585*	*11,5*	*2 322 316*	*13,4*	*207*	*0,0*	*5 777*	*0,0*	*1 184*	*0,3*	*76 021*	*0,4*
dont paiements hors 3-D Secure sans authentification forte	*253 871*	*5,2*	*15 205 110*	*7,0*	*3 432*	*0,1*	*134 162*	*0,1*	*125 749*	*2,6*	*6 888 753*	*3,2*
dont paiements initiés par le commerçant (MIT)	*192 607*	*7,7*	*10 054 028*	*9,4*	*1 987*	*0,1*	*73 622*	*0,1*	*73 907*	*3,0*	*3 377 006*	*3,2*
dont paiements « one-leg »	*11 543*	*1,8*	*1 610 838*	*3,7*	*546*	*0,1*	*27 479*	*0,1*	*13 061*	*2,0*	*1 526 388*	*3,5*
dont paiements non 3-D Secure conformes à la DSP 2	*18 374*	*3,6*	*862 303*	*6,4*	*385*	*0,1*	*8 938*	*0,1*	*1 516*	*0,3*	*48 375*	*0,4*
dont paiements non 3-D Secure non conformes à la DSP 2	*31 347*	*2,6*	*2 677 941*	*5,0*	*514*	*0,0*	*24 123*	*0,0*	*37 265*	*3,1*	*1 936 984*	*3,6*
Retraits	**79 034**	**73,2**	**31 584 937**	**77,5**	**3 654**	**3,4**	**1 120 781**	**2,7**	**7 808**	**7,2**	**2 053 621**	**5,0**
Total	**1 086 237**	**14,6**	**99 015 438**	**19,1**	**18 249**	**0,2**	**2 858 603**	**0,6**	**248 501**	**3,3**	**17 934 414**	**3,5**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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 2024 (suite)

(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	**33 140**	**3,5**	**4 556 656**	**7,2**	**146 273**	**15,5**	**10 847 197**	**17,2**	**943 105**	**62 951 625**
dont paiements sans contact (y compris paiements par mobile)	*20 018*	*2,7*	*1 447 959*	*6,4*	*103 383*	*13,8*	*3 033 993*	*13,4*	*746 923*	*22 648 147*
dont paiements par mobile	*8 962*	*6,9*	*534 246*	*5,9*	*25 851*	*20,0*	*1 394 609*	*15,5*	*129 052*	*9 023 196*
Paiements à distance (hors internet)	**165 163**	**89,9**	**36 458 568**	**90,3**	**733**	**0,4**	**51 558**	**0,1**	**183 666**	**40 377 262**
Paiements sur internet	**5 665 079**	**91,6**	**337 167 693**	**90,0**	**40 356**	**0,7**	**3 932 171**	**1,0**	**6 186 464**	**374 734 072**
dont paiements 3-D Secure avec authentification forte	*633 888*	*93,8*	*118 930 572*	*92,3*	*2 472*	*0,4*	*1 219 959*	*0,9*	*676 055*	*128 822 135*
dont paiements hors 3-D Secure avec authentification forte	*181 129*	*95,8*	*10 653 401*	*95,2*	*2 707*	*1,4*	*208 999*	*1,9*	*189 142*	*11 192 865*
dont paiements 3-D Secure sans authentification forte	*392 920*	*87,5*	*14 671 798*	*84,8*	*3 232*	*0,7*	*218 741*	*1,3*	*449 128*	*17 294 653*
dont paiements hors 3-D Secure sans authentification forte	*4 457 142*	*91,5*	*192 911 922*	*88,7*	*31 945*	*0,7*	*2 284 472*	*1,1*	*4 872 139*	*217 424 419*
dont paiements initiés par le commerçant (MIT)	*2 208 720*	*88,8*	*92 770 543*	*87,0*	*10 217*	*0,4*	*322 994*	*0,3*	*2 487 438*	*106 598 193*
dont paiements « one-leg »	*613 780*	*94,2*	*39 489 357*	*90,3*	*12 516*	*1,9*	*1 097 714*	*2,5*	*651 446*	*43 751 776*
dont paiements non 3-D Secure conformes à la DSP 2	*492 159*	*95,3*	*12 374 463*	*91,8*	*4 245*	*0,8*	*191 228*	*1,4*	*516 679*	*13 485 307*
dont paiements non 3-D Secure non conformes à la DSP 2	*1 142 483*	*93,9*	*48 277 559*	*90,1*	*4 967*	*0,4*	*672 536*	*1,3*	*1 216 576*	*53 589 143*
Retraits	**902**	**0,8**	**159 379**	**0,4**	**16 615**	**15,4**	**5 844 863**	**14,3**	**108 013**	**40 763 581**
Total	**5 864 284**	**79,0**	**378 342 296**	**72,9**	**203 977**	**2,7**	**20 675 789**	**4,0**	**7 421 248**	**518 826 540**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2024

(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	**844 956**	**89,6**	**48 773 873**	**77,5**	**40 880**	**4,3**	**3 726 751**	**5,9**
dont paiements sans contact (y compris paiements par mobile)	*677 978*	*90,8*	*16 717 451*	*73,8*	*31 516*	*4,2*	*2 163 143*	*9,6*
dont paiements par mobile	*106 442*	*82,5*	*6 777 574*	*75,1*	*3 823*	*3,0*	*483 730*	*5,4*
Paiements à distance (hors internet)	**108 914**	**59,3**	**21 901 906**	**54,2**	**30 640**	**16,7**	**8 292 438**	**20,5**
Paiements sur internet	**1 698 767**	**27,5**	**140 961 462**	**37,6**	**2 843 968**	**46,0**	**140 451 519**	**37,5**
dont paiements 3-D Secure avec authentification forte	*243 803*	*36,1*	*64 612 099*	*50,2*	*333 371*	*49,3*	*51 411 372*	*39,9*
dont paiements hors 3-D Secure avec authentification forte	*29 664*	*15,7*	*2 723 581*	*24,3*	*133 819*	*70,8*	*6 709 739*	*59,9*
dont paiements 3-D Secure sans authentification forte	*269 807*	*60,1*	*11 345 394*	*65,6*	*134 624*	*30,0*	*4 434 507*	*25,6*
dont paiements hors 3-D Secure sans authentification forte	*1 155 493*	*23,7*	*62 280 388*	*28,6*	*2 242 154*	*46,0*	*77 895 901*	*35,8*
dont paiements initiés par le commerçant (MIT)	*911 249*	*36,6*	*46 970 926*	*44,1*	*1 028 521*	*41,3*	*39 736 426*	*37,3*
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 DSP 2	*82 250*	*15,9*	*3 895 661*	*28,9*	*431 126*	*83,4*	*9 281 176*	*68,8*
dont paiements non 3-D Secure non conformes à la DSP 2	*161 994*	*13,3*	*11 413 801*	*21,3*	*782 507*	*64,3*	*28 878 299*	*53,9*
Retraits	**97 042**	**89,8**	**38 795 063**	**95,2**	**2 824**	**2,6**	**808 281**	**2,0**
Total	**2 749 679**	**37,1**	**250 432 304**	**48,3**	**2 918 312**	**39,3**	**153 278 989**	**29,5**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2024 (suite)

(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	**57 269**	**6,1**	**10 451 001**	**16,6**	**943 105**	**62 951 625**
dont paiements sans contact (y compris paiements par mobile)	*37 429*	*5,0*	*3 767 553*	*16,6*	*746 923*	*22 648 147*
dont paiements par mobile	*18 787*	*14,6*	*1 761 892*	*19,5*	*129 052*	*9 023 196*
Paiements à distance (hors internet)	**44 112**	**24,0**	**10 182 918**	**25,2**	**183 666**	**40 377 262**
Paiements sur internet	**1 643 729**	**26,6**	**93 321 091**	**24,9**	**6 186 464**	**374 734 072**
dont paiements 3-D Secure avec authentification forte	*98 881*	*14,6*	*12 798 664*	*9,9*	*676 055*	*128 822 135*
dont paiements hors 3-D Secure avec authentification forte	*25 659*	*13,6*	*1 759 545*	*15,7*	*189 142*	*11 192 865*
dont paiements 3-D Secure sans authentification forte	*44 697*	*10,0*	*1 514 752*	*8,8*	*449 128*	*17 294 653*
dont paiements hors 3-D Secure sans authentification forte	*1 474 492*	*30,3*	*77 248 130*	*35,5*	*4 872 139*	*217 424 419*
dont paiements initiés par le commerçant (MIT)	*547 668*	*22,0*	*19 890 841*	*18,7*	*2 487 438*	*106 598 193*
dont paiements « one-leg »	*651 446*	*100,0*	*43 751 776*	*100,0*	*651 446*	*43 751 776*
dont paiements non 3-D Secure conformes à la DSP 2	*3 303*	*0,6*	*308 470*	*2,3*	*516 679*	*13 485 307*
dont paiements non 3-D Secure non conformes à la DSP 2	*272 075*	*22,4*	*13 297 043*	*24,8*	*1 216 576*	*53 589 143*
Retraits	**8 147**	**7,5**	**1 160 237**	**2,8**	**108 013**	**40 763 581**
Total	**1 753 257**	**23,6**	**115 115 247**	**22,2**	**7 421 248**	**518 826 540**

Note : *One-leg* signifie que l'acquéreur du paiement est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

T9 Paiements par carte émise et acceptée en France – Transactions nationales

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

	2019		2020		2021	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**11 774 183**	**437 193 670**	**10 978 602**	**413 760 411**	**12 611 966**	**460 274 895**
dont paiements sans contact (y compris paiements par mobile)	*3 690 364*	*41 558 002*	*5 081 519*	*78 386 853*	*7 202 992*	*121 694 861*
dont paiements par mobile	*45 249*	*794 288*	*126 945*	*2 687 300*	*348 251*	*7 390 633*
Paiements à distance (hors internet)	**34 859**	**2 773 069**	**60 243**	**5 428 918**	**56 236**	**5 540 339**
Paiements sur internet	**1 768 890**	**109 593 147**	**2 011 431**	**122 128 921**	**2 399 865**	**142 184 895**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*389 530*	*15 797 723*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*1 348 375*	*54 203 060*
Retraits	**1 339 625**	**130 198 441**	**1 038 647**	**112 337 533**	**1 056 936**	**119 485 544**
Total	**14 917 558**	**679 758 326**	**14 088 924**	**653 655 783**	**16 125 003**	**727 485 673**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T9 Paiements par carte émise et acceptée en France – Transactions nationales (suite)

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

	2022		2023		2024	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**14 340 211**	**514 159 801**	**15 252 122**	**543 567 354**	**16 006 233**	**556 741 575**
dont paiements sans contact (y compris paiements par mobile)	*8 781 813*	*141 160 469*	*10 357 439*	*164 920 568*	*10 909 977*	*190 761 361*
dont paiements par mobile	*808 622*	*17 132 553*	*1 533 084*	*33 773 794*	*2 350 573*	*53 025 223*
Paiements à distance (hors internet)	**87 602**	**13 259 829**	**82 700**	**12 227 259**	**81 806**	**11 294 926**
Paiements sur internet	**2 393 161**	**146 642 890**	**2 580 907**	**164 682 672**	**2 817 916**	**179 442 255**
dont paiements 3-D Secure avec authentification forte	*809 038*	*88 956 221*	*977 983*	*105 884 327*	*914 093*	*109 906 448*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*57 239*	*1 938 429*	*164 512*	*6 793 036*
dont paiements 3-D Secure sans authentification forte	*717 916*	*24 981 800*	*661 070*	*22 814 974*	*772 768*	*27 751 133*
dont paiements hors 3-D Secure sans authentification forte	*866 207*	*32 704 868*	*884 617*	*34 044 942*	*966 543*	*34 991 639*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*704 832*	*25 137 618*	*759 880*	*26 194 801*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*92 513*	*4 489 918*	*99 379*	*3 924 928*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*87 272*	*4 417 407*	*107 284*	*4 871 909*
Retraits	**1 101 989**	**128 161 781**	**1 085 417**	**129 282 806**	**1 038 313**	**126 861 199**
Total	**17 922 963**	**802 224 301**	**19 001 146**	**849 760 091**	**19 944 269**	**874 339 955**

nd, non disponible.

Note : MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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

(volume en unités valeur en euros taux en pourcentage)

	2019			2020			2021		
	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	**1 069 418**	**44 175 058**	**0,010**	**793 350**	**36 280 495**	**0,009**	**825 325**	**43 515 617**	**0,009**
dont paiements sans contact (y compris paiements par mobile)	*582 050*	*7 912 021*	*0,019*	*522 873*	*10 502 092*	*0,013*	*576 537*	*14 002 613*	*0,012*
dont paiements par mobile	*3 215*	*197 048*	*0,025*	*29 807*	*2 447 707*	*0,091*	*75 039*	*4 801 997*	*0,065*
Paiements à distance (hors internet)	**64 113**	**7 498 207**	**0,270**	**74 832**	**8 964 315**	**0,165**	**77 941**	**10 604 251**	**0,191**
Paiements sur internet	**2 630 697**	**183 067 879**	**0,167**	**2 847 769**	**212 962 645**	**0,174**	**2 577 337**	**191 873 234**	**0,135**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*159 344*	*11 208 886*	*0,071*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*2 150 437*	*111 120 015*	*0,205*
Retraits	**122 260**	**35 935 625**	**0,028**	**102 962**	**32 477 429**	**0,029**	**121 642**	**41 437 842**	**0,035**
Total	**3 886 488**	**270 676 769**	**0,040**	**3 818 913**	**290 684 884**	**0,044**	**3 602 245**	**287 430 944**	**0,040**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

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

(volume en unités valeur en euros taux en pourcentage)

	2022			2023			2024		
	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	**989 454**	**53 593 598**	**0,010**	**885 533**	**50 277 021**	**0,009**	**844 956**	**48 773 873**	**0,009**
dont paiements sans contact (y compris paiements par mobile)	*754 985*	*20 231 615*	*0,014*	*684 776*	*15 698 156*	*0,010*	*677 978*	*16 717 451*	*0,009*
dont paiements par mobile	*152 726*	*9 566 583*	*0,056*	*98 610*	*6 066 551*	*0,018*	*106 442*	*6 777 574*	*0,013*
Paiements à distance (hors internet)	**120 708**	**24 857 056**	**0,187**	**118 903**	**22 602 626**	**0,185**	**108 914**	**21 901 906**	**0,194**
Paiements sur internet	**1 874 565**	**145 299 292**	**0,099**	**1 913 224**	**152 815 486**	**0,093**	**1 698 767**	**140 961 462**	**0,079**
dont paiements 3-D Secure avec authentification forte	*314 967*	*72 922 674*	*0,082*	*314 857*	*72 017 359*	*0,068*	*243 803*	*64 612 099*	*0,059*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*36 576*	*2 353 042*	*0,121*	*29 664*	*2 723 581*	*0,040*
dont paiements 3-D Secure sans authentification forte	*342 714*	*17 460 124*	*0,070*	*258 701*	*12 634 204*	*0,055*	*269 807*	*11 345 394*	*0,041*
dont paiements hors 3-D Secure sans authentification forte	*1 216 884*	*54 916 494*	*0,168*	*1 303 090*	*65 810 881*	*0,193*	*1 155 493*	*62 280 388*	*0,178*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*1 044 582*	*49 260 633*	*0,196*	*911 249*	*46 970 926*	*0,179*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*70 590*	*4 496 448*	*0,100*	*82 250*	*3 895 661*	*0,099*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*187 918*	*12 053 800*	*0,273*	*161 994*	*11 413 801*	*0,234*
Retraits	**115 643**	**41 344 934**	**0,032**	**102 357**	**38 832 083**	**0,030**	**97 042**	**38 795 063**	**0,031**
Total	**3 100 370**	**265 094 880**	**0,033**	**3 020 017**	**264 527 216**	**0,031**	**2 749 679**	**250 432 304**	**0,029**

nd, non disponible.

Note : MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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 2024

(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	839 775 334	47 851 435 622	331 775	25 646 539	0,395	0,054
Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager, etc.)	167 243 767	7 480 671 089	301 261	14 058 213	1,801	0,188
Voyage, transport	326 985 440	30 154 845 761	163 659	21 327 646	0,501	0,071
Téléphonie et communication	409 511 562	15 409 913 699	262 287	19 961 503	0,640	0,130
Alimentation	34 103 581	2 614 453 637	10 090	1 060 996	0,296	0,041
Équipement de la maison, ameublement, bricolage	117 021 604	13 443 874 493	40 974	12 257 418	0,350	0,091
Assurance	14 109 505	2 838 800 127	5 752	818 359	0,408	0,029
Santé, beauté, hygiène	53 374 504	3 373 912 500	24 330	2 323 234	0,456	0,069
Services aux particuliers et aux professionnels	491 092 639	39 221 545 908	499 264	41 107 865	1,017	0,105
Approvisionnement d'un compte, vente de particulier à particulier	122 727 707	12 116 829 244	74 282	15 918 915	0,605	0,131
Jeux en ligne	159 189 679	4 864 731 237	66 173	4 375 325	0,416	0,090
Divers	164 587 463	11 366 167 820	27 834	4 007 355	0,169	0,035
Total	**2 899 722 785**	**190 737 181 137**	**1 807 681**	**162 863 368**	**0,623**	**0,085**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France

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

	2019		2020		2021	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**12 277 149**	**468 895 511**	**11 284 433**	**428 180 387**	**13 031 098**	**480 804 099**
dont paiements sans contact (y compris paiements par mobile)	*3 802 953*	*42 931 374*	*5 187 488*	*79 877 184*	*7 437 197*	*125 344 168*
dont paiements par mobile	*56 169*	*1 014 657*	*145 527*	*2 979 437*	*388 175*	*8 403 747*
Paiements à distance (hors internet)	**48 998**	**5 586 755**	**69 950**	**7 087 913**	**64 620**	**7 272 724**
Paiements sur internet	**1 906 065**	**121 920 272**	**2 158 226**	**132 554 575**	**2 565 276**	**155 816 405**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*409 008*	*18 152 505*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*1 448 074*	*59 013 071*
Retraits	**1 375 145**	**136 636 741**	**1 062 376**	**116 986 747**	**1 083 643**	**125 105 264**
Total	**15 607 358**	**733 039 279**	**14 574 985**	**684 809 622**	**16 744 636**	**768 998 491**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France (suite)

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

	2022		2023		2024	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**15 093 611**	**551 753 133**	**16 159 605**	**588 228 633**	**17 012 813**	**604 699 649**
dont paiements sans contact (y compris paiements par mobile)	*9 248 429*	*149 971 446*	*10 982 717*	*178 132 864*	*11 665 395*	*208 538 219*
dont paiements par mobile	*897 307*	*19 846 999*	*1 716 563*	*39 282 385*	*2 640 235*	*61 840 034*
Paiements à distance (hors internet)	**107 228**	**18 523 094**	**105 756**	**18 799 343**	**106 081**	**18 394 978**
Paiements sur internet	**2 589 260**	**166 197 062**	**2 821 038**	**190 607 365**	**3 093 897**	**209 248 154**
dont paiements 3-D Secure avec authentification forte	*871 961*	*99 937 461*	*1 049 797*	*120 158 448*	*983 884*	*125 202 674*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*86 343*	*3 228 632*	*207 164*	*8 955 485*
dont paiements 3-D Secure sans authentification forte	*748 083*	*27 403 752*	*707 064*	*26 605 058*	*824 916*	*32 032 178*
dont paiements hors 3-D Secure sans authentification forte	*969 216*	*38 855 848*	*977 834*	*40 615 228*	*1 077 933*	*43 057 816*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*730 327*	*26 600 426*	*799 769*	*28 458 565*
dont paiements « one-leg »	*nd*	*nd*	*13 616*	*1 740 365*	*18 288*	*2 203 462*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*101 735*	*5 110 587*	*108 621*	*4 746 678*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*132 156*	*7 163 850*	*151 255*	*7 649 111*
Retraits	**1 134 543**	**134 637 455**	**1 117 986**	**135 559 666**	**1 069 029**	**133 303 352**
Total	**18 924 643**	**871 110 743**	**20 204 386**	**933 195 008**	**21 281 820**	**965 646 133**

nd, non disponible.

Note : *One-leg* signifie que l'émetteur de la carte est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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

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

	2019			2020			2021		
	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	**1 170 399**	**64 448 538**	**0,0137**	**841 280**	**42 883 367**	**0,0100**	**874 166**	**49 441 754**	**0,0103**
dont paiements sans contact (y compris paiements par mobile)	*602 309*	*8 534 090*	*0,0199*	*538 313*	*12 238 895*	*0,0153*	*601 803*	*15 600 613*	*0,0124*
dont paiements par mobile	*3 890*	*307 230*	*0,0303*	*35 968*	*3 640 684*	*0,1222*	*84 421*	*5 793 427*	*0,0689*
Paiements à distance (hors internet)	**108 259**	**23 167 505**	**0,4147**	**105 972**	**17 644 315**	**0,2489**	**96 257**	**15 211 163**	**0,2092**
Paiements sur internet	**2 989 333**	**232 763 441**	**0,1909**	**3 176 400**	**248 966 265**	**0,1878**	**2 885 920**	**227 162 875**	**0,1458**
dont paiements 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*213 403*	*20 406 481*	*0,1124*
dont paiements hors 3-D Secure sans authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*2 366 252*	*129 864 761*	*0,2201*
Retraits	**127 005**	**37 354 814**	**0,0273**	**104 960**	**33 084 175**	**0,0283**	**124,077**	**42,256,276**	**0,0338**
Total	**4 394 996**	**357 734 298**	**0,0488**	**4 228 612**	**342 578 122**	**0,0500**	**3,980,420**	**334,072,068**	**0,0434**

nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T13 Transactions frauduleuses par carte acceptée en France (suite)

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

	2022			2023			2024		
	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	**1 084 701**	**67 409 965**	**0,0122**	**999 344**	**67 688 751**	**0,0115**	**936 033**	**60 704 064**	**0,0100**
dont paiements sans contact (y compris paiements par mobile)	*819 535*	*24 406 015*	*0,0163*	*769 979*	*21 899 061*	*0,0123*	*750 184*	*21 346 502*	*0,0102*
dont paiements par mobile	*170 752*	*12 007 511*	*0,0605*	*127 622*	*10 042 616*	*0,0256*	*132 824*	*9 630 052*	*0,0156*
Paiements à distance (hors internet)	**144 965**	**35 446 137**	**0,1914**	**142 763**	**32 984 939**	**0,1755**	**142 032**	**33 542 430**	**0,1823**
Paiements sur internet	**2 252 283**	**190 461 573**	**0,1146**	**2 337 170**	**201 724 304**	**0,1058**	**2 244 306**	**203 744 409**	**0,0974**
dont paiements 3-D Secure avec authentification forte	346 366	80 959 973	0,0810	354 651	83 805 192	0,0697	267 924	73 737 188	0,0589
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*71 563*	*5 522 986*	*0,1711*	*44 498*	*4 443 794*	*0,0496*
dont paiements 3-D Secure sans authentification forte	*405 445*	*26 105 266*	*0,0953*	*342 878*	*20 687 862*	*0,0778*	*402 394*	*20 996 741*	*0,0655*
dont paiements hors 3-D Secure sans authentification forte	*1 500 472*	*83 396 334*	*0,2146*	*1 568 078*	*91 708 264*	*0,2258*	*1 529 490*	*104 566 686*	*0,2429*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*1 098 829*	*52 343 346*	*0,1968*	*1 013 164*	*53 073 094*	*0,1865*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*92 524*	*12 994 451*	*0,7467*	*134 338*	*20 595 974*	*0,9347*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*80 195*	*5 068 095*	*0,0992*	*92 684*	*4 512 752*	*0,0951*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*296 530*	*21 302 372*	*0,2974*	*289 304*	*26 384 866*	*0,3449*
Retraits	**120 217**	**42 811 637**	**0,0318**	**106 749**	**40 292 502**	**0,0297**	**100 323**	**40 070 346**	**0,0301**
Total	**3 602 166**	**336 129 312**	**0,0386**	**3 586 026**	**342 690 496**	**0,0367**	**3 422 694**	**338 061 249**	**0,0350**

nd, non disponible.

Note : *One-leg* signifie que l'émetteur de la carte est situé hors de l'Union européenne ; MIT, *Merchant Initiated Transaction* ; DSP 2, directive sur les systèmes 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 2024

T13 *quinquies* Répartition géographique de la fraude sur les cartes acceptées en France en 2024

CHÈQUE

T14 Chèques échangés

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

	2019	2020	2021	2022	2023	2024
Volume	1 586,5	1 175,5	1 105,8	1 008,0	891,5	783,8
Montant	814,5	614,2	588,6	539,8	467,3	392,2
Montant moyen	**513,4**	**522,5**	**532,3**	**535,5**	**524,1**	**500,4**

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

	2019	2020	2021	2022	2023	2024
Volume	**183 488**	**220 685**	**272 970**	**266 216**	**255 857**	**215 576**
Taux de fraude (‰)	0,116	0,188	0,247	0,264	0,287	0,275
Valeur	**539 215 175**	**538 059 139**	**625 703 442**	**556 796 815**	**588 194 101**	**457 332 103**
Taux de fraude (%)	0,066	0,088	0,106	0,103	0,126	0,117
Montant moyen	**2 939**	**2 438**	**2 292**	**2 092**	**2 299**	**2 121**

b) Nouvelle approche

	2019	2020	2021	2022	2023	2024
Volume	**nd**	**190 001**	**232 277**	**218 122**	**206 197**	**173 366**
Taux de fraude (‰)		0,162	0,210	0,216	0,231	0,221
Valeur	**nd**	**401 611 189**	**465 021 167**	**395 416 196**	**363 929 512**	**270 317 625**
Taux de fraude (%)		0,065	0,079	0,073	0,078	0,069
Montant moyen	**nd**	**2 114**	**2 002**	**1 813**	**1 765**	**1 559**

nd, non disponible.

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)

	2019		2020		2021		2022		2023		2024	
	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part
Volume												
Vol, perte	154 211	84,0	196 754	89,2	244 750	89,7	237 854	89,3	225 859	88,3	192 307	89,2
Falsification	16 459	9,0	13 894	6,3	18 074	6,6	18 885	7,1	20 583	8,0	14 260	6,6
Contrefaçon	9 574	5,2	7 207	3,3	5 119	1,9	5 969	2,2	5 720	2,2	6 249	2,9
Détournement, rejeu	3 244	1,8	2 830	1,3	5 026	1,8	3 508	1,3	3 695	1,4	2 760	1,3
Valeur												
Vol, perte	296 367 562	55,0	365 813 764	68,0	398 739 224	63,7	375 576 575	67,5	385 379 003	65,5	285 010 973	62,3
Falsification	145 881 745	27,1	102 801 337	19,1	100 395 756	16,0	93 152 894	16,7	103 932 879	17,7	89 327 982	19,5
Contrefaçon	76 511 582	14,2	32 340 420	6,0	33 725 041	5,4	32 648 566	5,9	29 927 137	5,1	44 088 111	9,6
Détournement, rejeu	20 454 286	3,8	37 103 618	6,9	92 823 421	14,8	55 418 781	10,0	68 955 081	11,7	38 905 037	8,5

Note : La ventilation par typologie de la fraude au chèque se fait en fonction de l'ancienne approche, qui couvre toute opération par chèque réglée et rejetée pour un motif de fraude.

Source : Observatoire de la sécurité des moyens de paiement.

T17 Virements émis par type de virement

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

	2019		2020		2021		2022		2023		2024	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4 251**	**25 879 217**	**4 483**	**32 713 128**	**4 843**	**38 722 734**	**5 158**	**38 894 879**	**5 613**	**29 942 161**	**5 973**	**31 108 348**
dont virements SEPA – SCT	*4 174*	*9 602 866*	*4 384*	*10 029 108*	*4 668*	*12 980 883*	*4 689*	*9 655 892*	*4 867*	*9 823 091*	*5 023*	*10 480 787*
dont virements SEPA instantanés – SCT Inst	*14*	*7 074*	*45*	*26 243*	*107*	*50 053*	*198*	*118 972*	*408*	*177 099*	*598*	*231 252*
dont virements de gros montants – VGM [a]	*9*	*12 266 316*	*9*	*19 042 030*	*9*	*19 661 685*	*19*	*15 907 892*	*30*	*8 533 346*	*11*	*10 407 612*
dont autres virements	*54*	*4 002 960*	*45*	*3 615 748*	*59*	*6 030 114*	*252*	*13 212 124*	*309*	*11 408 625*	*341*	*9 988 697*
Total – hors VGM	**4 242**	**13 612 900**	**4 474**	**13 671 098**	**4 834**	**19 061 050**	**5 138**	**22 986 988**	**5 583**	**21 408 815**	**5 962**	**20 700 736**

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

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

	2019			2020			2021		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**15 934**	**161 642 174**	**0,0006**	**35 893**	**266 969 099**	**0,0008**	**46 718**	**287 264 068**	**0,0007**
dont virements SEPA – SCT	*13 302*	*127 572 549*	*0,0013*	*25 254*	*191 474 396*	*0,0019*	*33 199*	*246 527 533*	*0,0019*
dont virements SEPA instantanés – SCT Inst	*729*	*2 203 240*	*0,0311*	*7 131*	*10 562 419*	*0,0402*	*12 913*	*22 406 942*	*0,0448*
dont virements de gros montants – VGM [a]	*15*	*15 476 053*	*0,0001*	*51*	*2 439 224*	*0,0000*	*5*	*1 539 120*	*0,0000*
dont autres virements	*1 888*	*16 390 332*	*0,0004*	*3 457*	*62 493 060*	*0,0017*	*601*	*16 790 473*	*0,0003*
Total – hors VGM	**15 919**	**146 166 121**	**0,0011**	**35 842**	**264 529 875**	**0,0019**	**46 713**	**285 724 948**	**0,0015**

a) Il s'agit des virements de gros montant effectués via Target2 ou Euro1.
Note : SEPA, *Single Euro Payment Area*, espace unique de paiment 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 (suite)

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

	2022			2023			2024		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**76 846**	**313 163 442**	**0,0008**	**90 453**	**312 487 450**	**0,0010**	**132 298**	**350 992 884**	**0,0011**
dont virements SEPA – SCT	*40 874*	*205 737 587*	*0,0021*	*38 591*	*202 417 172*	*0,0021*	*41 693*	*199 872 166*	*0,0019*
dont virements SEPA instantanés – SCT Inst	*33 193*	*52 768 218*	*0,0444*	*48 630*	*69 003 730*	*0,0390*	*80 394*	*105 718 759*	*0,0457*
dont virements de gros montants – VGM [a]	*49*	*1 934 774*	*0,0000*	*32*	*9 828 077*	*0,0001*	*20*	*3 496 816*	*0,0000*
dont autres virements	*2 730*	*52 722 863*	*0,0004*	*3 200*	*31 238 471*	*0,0003*	*10 191*	*41 905 143*	*0,0004*
Total – hors VGM	**76 797**	**311 228 668**	**0,0014**	**90 421**	**302 659 373**	**0,0014**	**132 278**	**347 496 068**	**0,0017**

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)

	2019	2020	2021	2022	2023	2024
Volume	**15 934**	**35 893**	**46 718**	**76 846**	**90 453**	**132 298**
Taux (‰)	0,0037	0,0080	0,0096	0,0149	0,0161	0,0222
Valeur	**161 642 174**	**266 969 099**	**287 264 068**	**313 163 442**	**312 487 450**	**350 992 884**
Taux (%)	0,0006	0,0008	0,0007	0,0008	0,0010	0,0011
Montant moyen	**10 144**	**7 438**	**6 149**	**4 075**	**3 455**	**2 653**

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)

	2019		2020		2021		2022		2023		2024	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**13 769**	**98 525 485**	**28 211**	**87 061 255**	**35 865**	**87 370 131**	**57 443**	**120 006 990**	**63 471**	**134 097 939**	**75 038**	**135 980 519**
Part	86,4	61,0	78,6	32,6	76,8	30,4	74,8	38,3	70,2	42,9	56,7	38,7
Falsification	**125**	**3 438 923**	**203**	**3 377 807**	**875**	**5 387 862**	**179**	**2 838 371**	**269**	**2 293 923**	**406**	**3 498 532**
Part	1,6	2,1	0,6	1,3	1,9	1,9	0,2	0,9	0,3	0,7	0,3	1,0
Détournement	**1 534**	**56 514 755**	**5 731**	**157 318 883**	**8 523**	**168 094 274**	**16 991**	**148 732 203**	**25 071**	**152 081 946**	**54 693**	**183 251 281**
Part	19,8	35,0	16,0	58,9	18,2	58,5	22,1	47,5	27,7	48,7	41,3	52,2
Autres	**506**	**3 163 011**	**1 748**	**19 211 154**	**1 455**	**26 411 801**	**2 233**	**41 585 878**	**1 642**	**24 013 643**	**2 161**	**28 262 553**
Part	3,2	2,0	4,9	7,2	3,1	9,2	2,9	13,3	1,8	7,7	1,6	8,1

Source : Observatoire de la sécurité des moyens de paiement.

T21 Prélèvements émis par type de mandat

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

	2019		2020		2021		2022		2023		2024	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4370**	**1710931**	**4622**	**1684258**	**5020**	**1895098**	**4914**	**2040963**	**4616**	**2138539**	**4788**	**2178198**
Prélèvements par type de mandat												
dont prélèvements consentis par mandat électronique	nd	nd	nd	nd	1106	430781	1357	1045754	1254	1021429	1228	1026955
dont prélèvements consentis par mandat papier	nd	nd	nd	nd	3914	1464317	3558	995210	3362	1117110	3560	1151243
Prélèvements par mode d'initiation												
dont prélèvements initiés dans un fichier/lot	4312	1672338	4560	1647504	4936	1819420	4645	1929438	4242	2009917	4479	2064694
dont prélèvements initiés sur la base d'un paiement unique	58	38593	61	36754	84	75678	269	111525	374	128622	310	113504

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)

	2019	2020	2021	2022	2023	2024
Volume	**43519**	**6485**	**251010**	**49453**	**77876**	**52718**
Taux de fraude (‰)	0,0100	0,0014	0,0500	0,0101	0,0169	0,0110
Valeur	**10990025**	**1891051**	**25318677**	**19853012**	**22320813**	**30365272**
Taux de fraude (%)	0,0006	0,0001	0,0013	0,0010	0,0010	0,0014
Montant moyen	**253**	**292**	**101**	**401**	**287**	**576**

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)

	2019		2020		2021		2022		2023		2024	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**14601**	**3961260**	**6011**	**1388326**	**250493**	**25201709**	**43788**	**14206533**	**70212**	**22003546**	**27476**	**29202487**
Part	33,6	36,0	92,7	73,4	99,8	99,5	88,5	71,6	90,2	98,6	52,1	96,2
Détournement	**26223**	**6677467**	**62**	**10720**	**517**	**116968**	**5665**	**5646479**	**7664**	**317267**	**25242**	**1162784**
Part	60,3	60,8	1,0	0,6	0,2	0,5	11,5	28,4	9,8	1,4	47,9	3,8

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.

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 service 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 service d'initiation de paiement (service 7 de l'article 314-1 du Code monétaire et financier)

Éditeur
Banque de France

Directeur de la publication
Érick 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, Julien Cisamolo, Caroline Corcy, Anne-Marie Fourel, Trân Huynh, Fatih Kurt, Isabelle Maranghi, Adrien Mocek, Ségolène Mure, Didier Névonnic, Cyril Ronfort, Marine Soubielle, Valérie Tallarita

Réalisation
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 2025
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*).

www.banque-france.fr