

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2022

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2022

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 François Villeroy de Galhau,
gouverneur de la Banque de France,
président de l'Observatoire de la sécurité
des moyens de paiement

JUILLET 2023

SOMMAIRE

SYNTHÈSE	5
2022 EN CHIFFRES	8
CHAPITRE 1	
ÉTAT DE LA FRAUDE EN 2022	11
1.1 Vue d'ensemble	12
1.2 État de la fraude sur la carte de paiement	14
1.3 État de la fraude sur le chèque	20
1.4 État de la fraude sur le virement	21
1.5 État de la fraude sur le prélèvement	22
CHAPITRE 2	
MODALITÉS DE REMBOURSEMENT DES OPÉRATIONS DE PAIEMENT FRAUDULEUSES	27
2.1 Contexte des travaux	27
2.2 Réglementation applicable aux contestations d'opérations de paiement	29
2.3 Recommandations générales applicables au traitement des contestations d'opérations de paiement	31
2.4 Recommandations applicables au traitement de cas spécifiques	31
2.5 Recommandations à l'attention des consommateurs et de leurs représentants	34
2.6 Recommandations visant à prévenir la fraude	36
2.7 Conditions d'application des recommandations	38

CHAPITRE 3	
LES SOLUTIONS D'ACCEPTATION DE PAIEMENT SUR <i>SMARTPHONE</i> OU <i>TABLETTE</i>	39
3.1	Introduction
	39
3.2	Panorama des solutions actuelles
	40
3.3	Les risques
	41
3.4	Les standards de sécurité
	42
3.5	La sécurité technique des solutions SoftPOS
	44
3.6	Les recommandations de l'Observatoire
	45
3.7	Conclusion
	46
CHAPITRE 4	
ACTIONS CONDUITES PAR L'OBSERVATOIRE EN 2022	49
4.1	L'authentification forte des paiements par carte
	49
4.2	Le suivi des actions et recommandations de l'Observatoire contre la fraude au chèque
	55
4.3	Rappel des principales recommandations de l'Observatoire sur les sujets de veille technologique
	60
ANNEXES	65
A1	Conseils de prudence pour l'utilisation des moyens de paiement
	67
A2	Missions et organisation de l'Observatoire
	80
A3	Liste nominative des membres de l'Observatoire
	82
A4	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux
	85
A5	Dossier statistique sur l'usage et la fraude aux moyens de paiement
	95

SYNTHÈSE

L'année 2022 confirme la progression générale de l'usage des moyens de paiement scripturaux (+ 8 %) observée depuis la crise sanitaire. Dans ce contexte dynamique, certains usages dématérialisés se sont durablement installés comme le paiement sans contact, représentant désormais plus de six paiements par carte sur dix en proximité, tandis que d'autres usages poursuivent leur croissance très soutenue, comme le paiement par carte sur mobile (+ 137 %, atteignant près de 6 % des paiements par carte de proximité) ou le virement instantané (+ 85 %).

Le chapitre 1 du rapport, qui présente les évolutions statistiques sur l'usage et la fraude, expose une amélioration générale de la sécurité des moyens de paiement scripturaux. Au total, et malgré la croissance des flux, la fraude recule de 4 % en volume comme en valeur, pour revenir à 1,19 milliard d'euros de préjudice. Les évolutions sont toutefois différenciées selon les moyens de paiement :

- **La carte, qui conforte encore davantage son statut de moyen de paiement principal du quotidien, voit son taux de fraude se contracter à 0,053 %** (contre 0,059 % en 2021), **soit le niveau le plus bas jamais enregistré par l'Observatoire.** Ce résultat historique est le fruit de l'amélioration sensible de la sécurité des paiements sur Internet, qui a bénéficié à plein régime et sur une année entière des règles d'authentification forte introduites par la deuxième directive européenne sur les services de paiement (DSP 2). Ainsi, par rapport à 2019 où ces règles n'étaient pas encore appliquées, le taux de fraude des paiements par carte sur Internet a baissé d'un tiers, à 0,165 %. Après les premières tendances observées en 2021, ces éléments confortent le bilan très positif de l'authentification forte pour la sécurité des paiements par carte sur Internet. En revanche, le rapport souligne le taux de fraude encore relativement élevé des paiements mobiles en proximité (0,061 %) qui, s'il est en baisse par rapport à 2021, reste six fois

supérieur à l'ensemble des paiements par carte de proximité. Ceci est dû principalement à des vulnérabilités dans les processus d'enrôlement dans les portefeuilles électroniques, qui ne mobilisent pas toujours une authentification forte du porteur de la carte sous le contrôle de l'établissement émetteur.

- **Le chèque enregistre également une baisse de son taux de fraude, à 0,073 %** (contre 0,079 % en 2021), **même si celui-ci reste encore le plus élevé parmi les différents moyens de paiement.** La baisse de la fraude, qui s'inscrit dans un contexte de chute des flux (– 8 %), matérialise les premiers résultats positifs du plan d'action de l'Observatoire décidé en 2021. Les dispositifs de surveillance des encaissements de chèque, qui sont déployés par les établissements bancaires depuis quelques années, y contribuent. Compte tenu des niveaux toujours élevés de fraude, les utilisateurs doivent rester vigilants et les efforts doivent être durablement poursuivis par les acteurs de la filière. Des progrès sont encore attendus dans la sécurisation de l'envoi des chèquiers par voie postale et la simplification des procédures de mise en opposition des formules de chèque perdues ou volées.
- **Le virement enregistre une nouvelle hausse annuelle des montants de fraude (9 %).** Le taux de fraude reste extrêmement bas (0,001 %) en raison de la valeur significative des montants échangés. En effet, le virement est le principal instrument utilisé par les entreprises et les administrations. Néanmoins, les montants de fraude liés au virement ont plus que triplé en cinq ans, passant de 78 millions d'euros en 2017 à 313 millions d'euros en 2022. Si les grandes entreprises et les administrations restent touchées, les particuliers et les petites entreprises sont les principales victimes en 2022. En effet, 70 % du montant de la fraude a ciblé les virements initiés depuis les interfaces de banque en ligne, principalement utilisées par les particuliers et les petites entreprises. L'Observatoire se félicite en revanche de la stabilité du taux de fraude

du virement instantané (0,044 %), inférieur à celui de la carte et dont l'usage est appelé à se développer dans les prochaines années. Pour répondre à ces nouveaux défis de sécurité, l'Observatoire va lancer, dès la rentrée de septembre 2023, des travaux visant à identifier des mesures complémentaires de lutte contre la fraude au virement et à accélérer leur mise en œuvre sur le marché français.

Dans la suite du rapport, l'Observatoire émet plusieurs recommandations qui apportent des réponses aux évolutions des usages de paiement et des techniques de fraude.

- **Au milieu de ces progrès d'ensemble, l'année 2022 a tout d'abord été marquée par le développement des techniques d'escroquerie et des modes opératoires reposant sur la manipulation, notamment celles reposant sur un appel téléphonique à la victime en usurpant l'identité du personnel bancaire.** Usant de différents moyens pour prendre l'emprise sur leur victime, les fraudeurs parviennent ainsi à obtenir une authentification forte de leurs opérations frauduleuses. Dans ces circonstances, les victimes ont pu rencontrer des difficultés à obtenir un remboursement. En réponse à ces fraudes, qui touchent tous les profils de clients, l'Observatoire a émis en mai 2023 un ensemble de treize recommandations qui visent à améliorer le remboursement des victimes tout en intensifiant les actions de prévention et de lutte contre la fraude de la part de tous les acteurs impliqués (chapitre 2). L'Observatoire assurera un suivi précis de leur mise en œuvre, avec l'appui de l'Autorité de contrôle prudentiel et de résolution (ACPR) au titre de son mandat de contrôle des pratiques commerciales. Un premier bilan sera dressé et publié à la fin de l'année 2024. Il est en effet essentiel que les consommateurs puissent avoir l'assurance d'un traitement rigoureux de leurs contestations, afin de conforter le sentiment qu'eux aussi bénéficient pleinement des progrès collectifs obtenus en matière de lutte contre la fraude.
- **Fort de son travail permanent de veille technologique, l'Observatoire émet par ailleurs quelques recommandations sur l'utilisation des terminaux destinés au grand public, tels que les téléphones mobiles ou les tablettes, comme terminaux d'acceptation des paiements par carte (chapitre 3).**

Ces solutions, très minoritaires, et encore souvent à l'état d'expérimentation, commencent à apparaître sur le marché français. En 2016, l'Observatoire soulignait que le téléphone mobile restait un maillon faible dans la sécurité des solutions de paiement en situation de mobilité. En 2022, la sécurité technique de ces nouvelles solutions d'acceptation paraît désormais possible, si elles sont dûment auditées et certifiées. L'Observatoire appelle toutefois les commerçants à rester particulièrement prudents, rigoureux et sélectifs dans le déploiement de ces nouveaux terminaux « grand public », afin de maintenir la même exigence que pour les terminaux dédiés aux paiements électroniques. Ces derniers ont en effet fait la preuve de leur sécurité, de leur robustesse et de leur capacité à être utilisés en situation de mobilité. Les commerçants qui utiliseraient ce type de terminaux « grand public » doivent en outre prévoir une alternative pour les personnes en situation de déficience visuelle, qui ne peuvent pas toujours utiliser les écrans tactiles et les claviers virtuels de ces solutions.

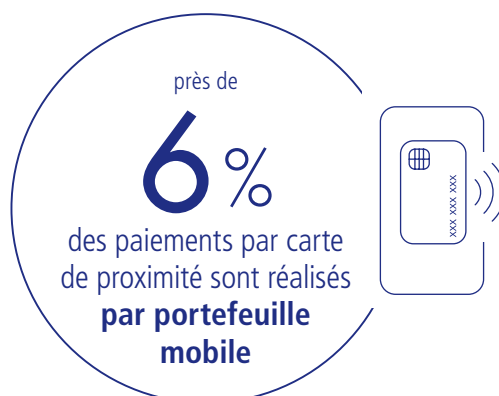
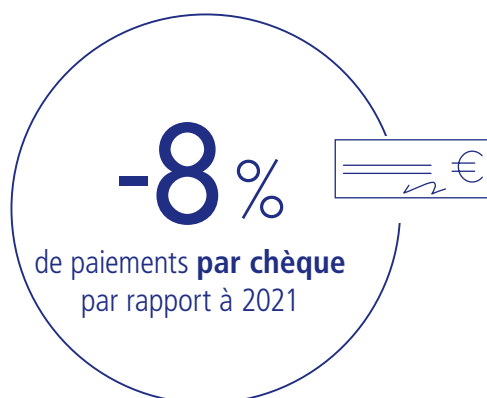
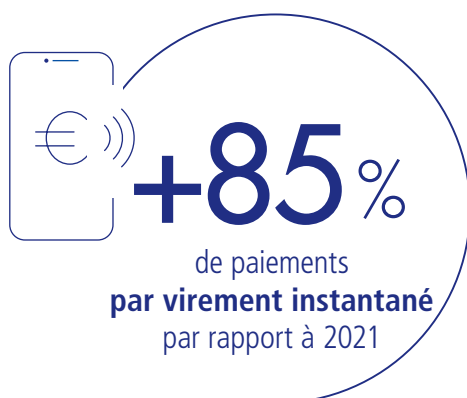
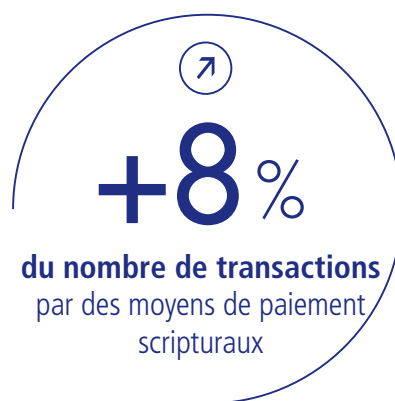
- **Les travaux de l'Observatoire menés en 2022 sur l'authentification forte des paiements en ligne sont repris dans le chapitre 4.** Le rapport restitue pour la première fois des données détaillées sur l'équipement des porteurs et les paiements sur Internet. Celles-ci mettent en lumière de nettes marges de progrès pour renforcer la sécurité des paiements sur Internet, notamment des opérations dites « MIT » (Merchant Initiated Transactions, c'est-à-dire des transactions initiées par un commerçant) et de certaines opérations exemptées d'authentification forte en dehors des protocoles d'authentification de type 3D-Secure. Les lignes directrices publiées dans ce rapport devraient concourir à un usage plus sécurisé et conforme de l'exemption à l'authentification forte fondée sur l'analyse des risques de la transaction.

Dans un contexte de rapide évolution des moyens de paiement et de renouvellement continu des menaces, l'Observatoire reste mobilisé pour veiller à la sécurité de l'ensemble des moyens de paiement. Ceci garantit à tous les utilisateurs, des particuliers aux entreprises, une authentique liberté de choix dans leurs usages au quotidien. Dans son programme de travail pour 2023-2024, l'Observatoire s'attachera en particulier à intensifier le dialogue avec le secteur des télécommunications, qui a un rôle clé à jouer pour prévenir les risques d'usurpation d'identité et ainsi contribuer à la lutte contre la fraude aux moyens de paiement.

2022 EN CHIFFRES

L'USAGE DES MOYENS DE PAIEMENT EN 2022

42 578 MDS €
échangés



L'ÉVOLUTION DE LA FRAUDE EN 2022

1,192 MD€
de préjudice

-4%

de fraude en volume
et en valeur

0,053%

de taux de fraude
sur la carte,
plus bas niveau historique

0,044%

de taux de fraude
des virements instantanés

près de
70%

de la fraude au virement
en valeur touche
**les interfaces de
banque en ligne**

-33%

du taux de fraude
**pour les paiements
par carte sur Internet
depuis 2019**

-15%

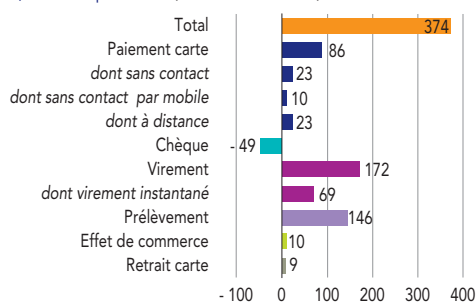
de fraude en valeur
sur le chèque
par rapport à 2021

ÉTAT DE LA FRAUDE EN 2022

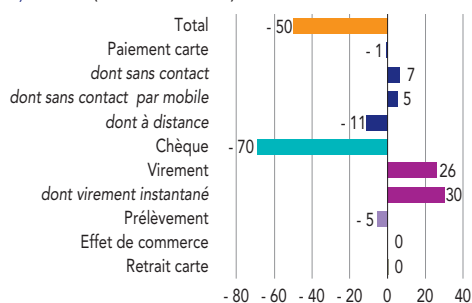
Données clés

G1 Évolution des moyens de paiement entre 2021 et 2022

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

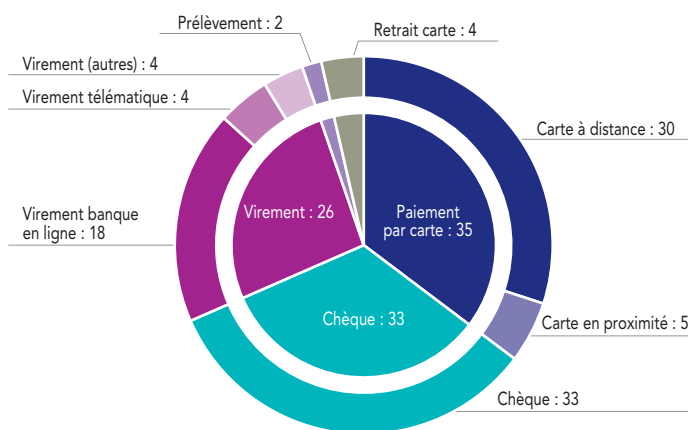


b) Fraude (en millions d'euros)



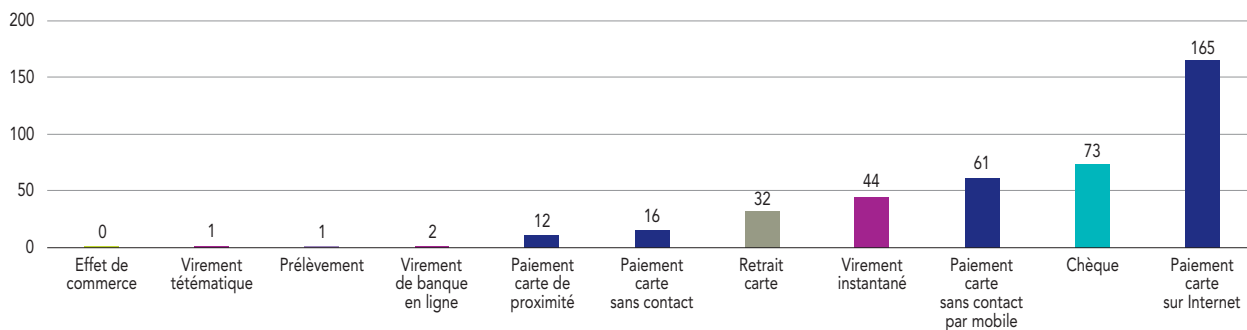
Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

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



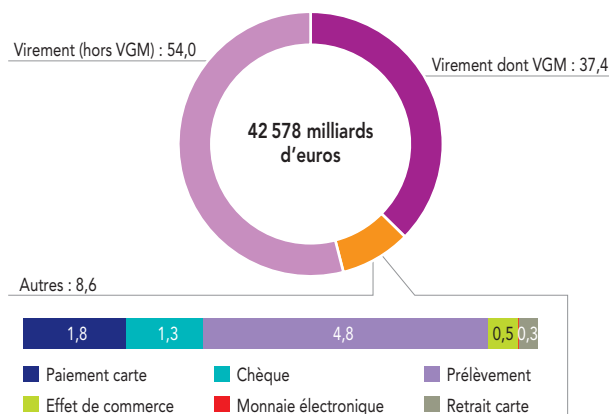
Source : Observatoire de la sécurité des moyens de paiement.

1.1 Vue d'ensemble

1.1.1 Cartographie des moyens de paiement

G4 Usage des moyens de paiement scripturaux en 2022 (en %)

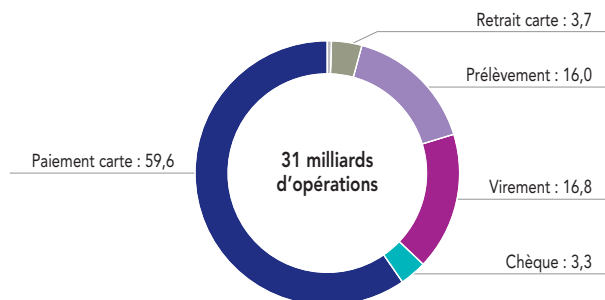
a) En montant



Note : VGM – virement de gros montant.

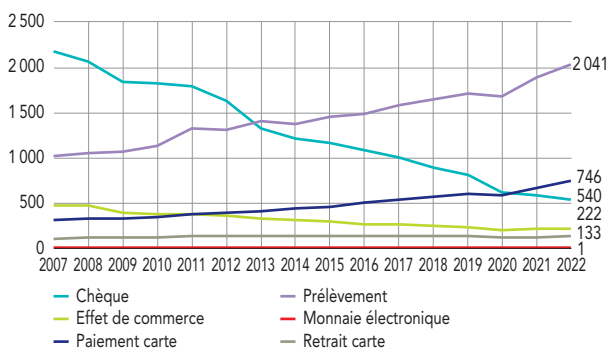
Source : Observatoire de la sécurité des moyens de paiement.

b) En volume



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

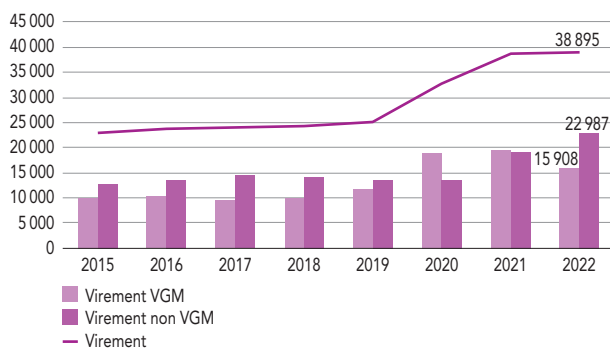
a) Par instrument (hors virement)



Note : VGM – virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

b) Par virement



Les opérations de paiement scripturales réalisées par les particuliers, les entreprises et les administrations ont atteint 30,6 milliards de transactions en 2022 (+ 8,1 % par rapport à 2021), pour un total de 42 578 milliards d'euros (+ 0,9 % par rapport à 2021).

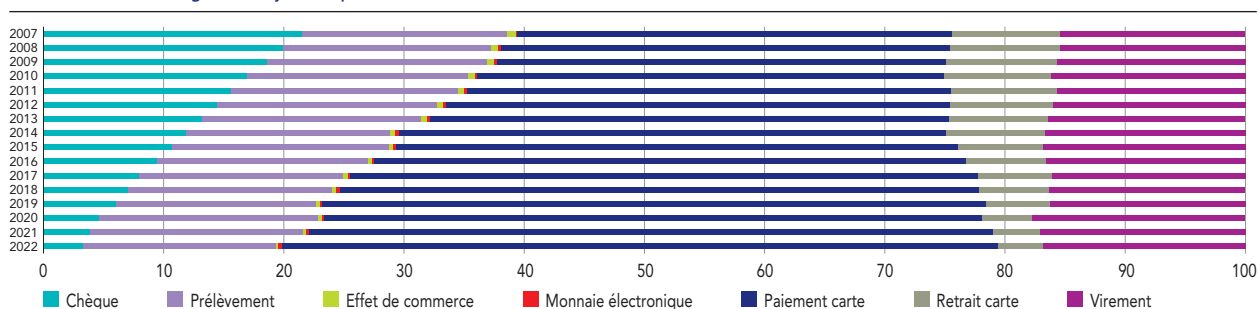
Le virement instantané poursuit sa rapide progression (+ 85 % en volume et + 138 % en valeur) pour représenter désormais 3,8 % des virements (contre 2,2 % en 2021).

La carte bancaire reste le moyen de paiement scriptural préféré des Français. Sa part, hors retraits, dans les volumes

de transactions est en constante augmentation puisqu'elle passe de 56,9 % en 2021 à 59,6 % en 2022. La croissance des flux en volume et en montant se retrouve aussi dans le paiement sans contact (61 % des paiements par carte de proximité, contre 57 % en 2021), et notamment parmi ceux-là dans les paiements par mobile (près de 6 % des paiements par carte de proximité, contre moins de 3 % en 2021).

Le chèque reste le seul moyen de paiement en repli à la fois en nombre de transactions (– 8,8 %) et en montant (– 8,3 %), tandis que les retraits d'espèces par carte se maintiennent (+ 4,5 % en volume et + 7,3 % en valeur).

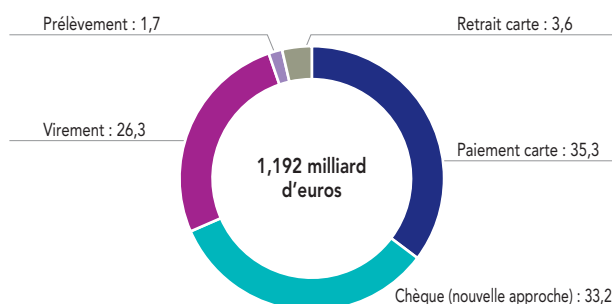
G6 Évolution de l'usage des moyens de paiements en volume (en %)



1.1.2 Panorama de la fraude aux moyens de paiement

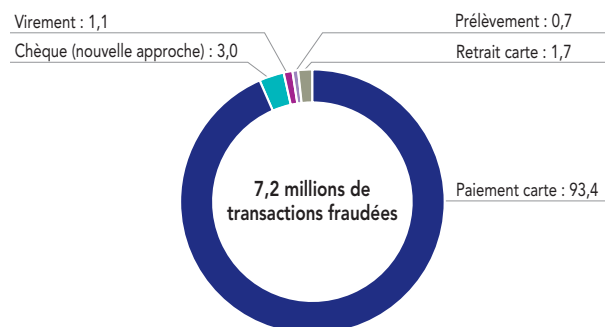
G7 Répartition de la fraude (en %)

a) En valeur

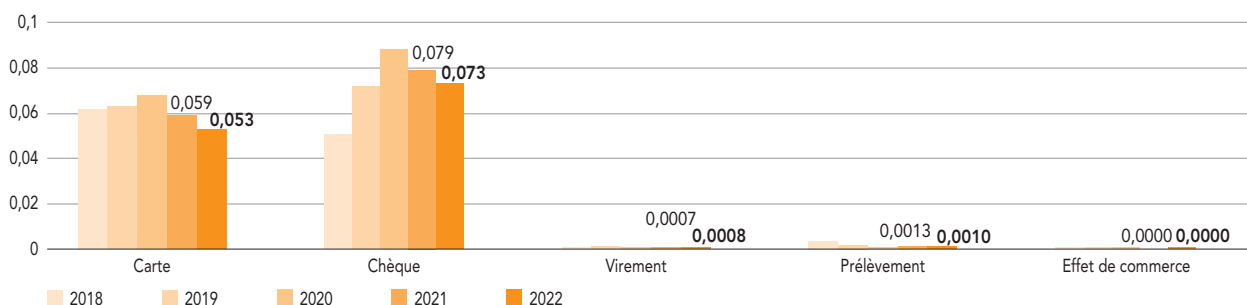


Source : Observatoire de la sécurité des moyens de paiement.

b) En volume



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



Note : En 2021 et 2022, le taux de fraude sur le chèque est calculé selon la nouvelle approche.

Source : Observatoire de la sécurité des moyens de paiement.

Dans un contexte de progression des transactions en volume comme en valeur, la fraude aux moyens de paiement scripturaux décroît. Elle atteint 7,2 millions d'opérations frauduleuses (– 3,6 % par rapport à 2021), pour un préjudice de 1,192 milliard d'euros (– 4 % par rapport à 2021).

Cette régression générale de la fraude est notamment entraînée par la baisse de la fraude à la carte (– 0,2 % en valeur), dont le taux de fraude atteint un plus bas historique à 0,053 %, et par la diminution de la fraude au chèque (– 15 % en valeur) qui est plus rapide que celle

des flux (– 8 % des montants échangés). La fraude sur le prélèvement, par nature assez erratique, fléchit (– 21,6 % en valeur) et sa part dans la fraude reste stable et modérée.

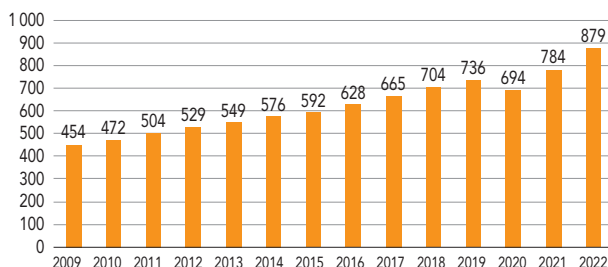
En revanche, même si le taux de fraude du virement reste extrêmement faible en raison des montants significatifs échangés (0,0008 %), la fraude au virement poursuit sa progression avec un préjudice total de 313,1 millions d'euros, en hausse de 9 % par rapport à 2021. Le virement représente 26,3 % des montants de fraude en 2022, contre 23,1 % en 2021.

1.2 État de la fraude sur la carte de paiement

1.2.1 Vue d'ensemble – Cartes émises en France

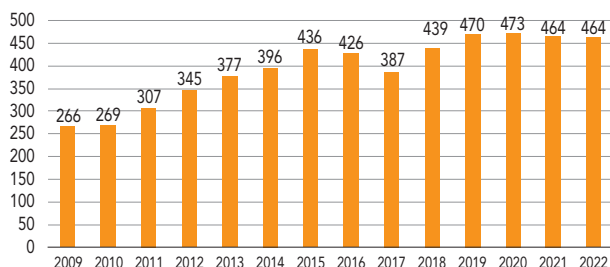
G9 Les cartes émises en France en 2022

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



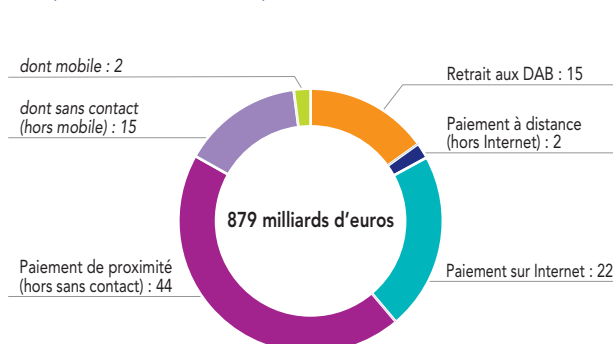
Source : Observatoire de la sécurité des moyens de paiement.

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



G10 Le canal d'utilisation des cartes émises en France en 2022 (en %)

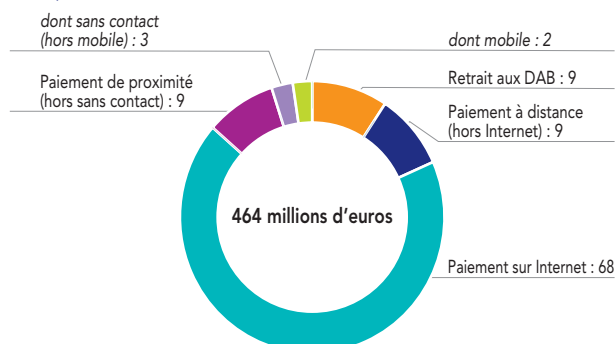
a) Répartition du montant des opérations



Note : DAB – distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

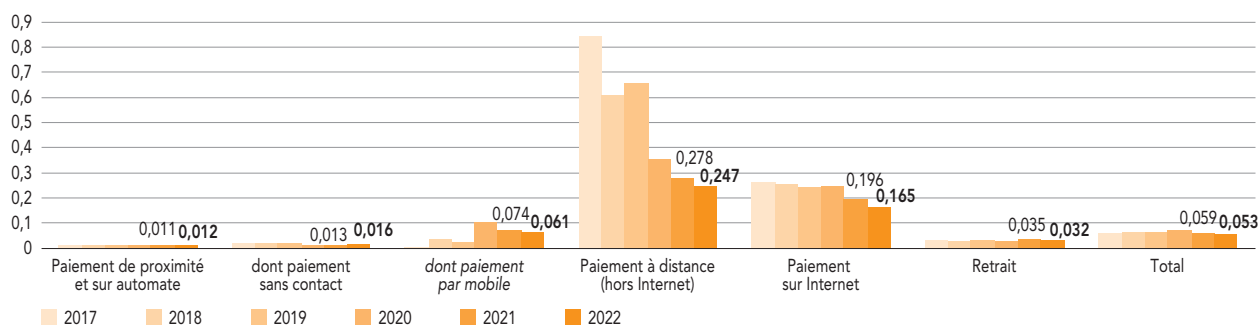
b) Répartition de la valeur de la fraude



La carte poursuit sa progression dans le paysage des moyens de paiement, avec des flux qui progressent en 2022 dans les mêmes proportions en volume comme en valeur (respectivement de 13 et 12 %). Dans ce contexte haussier, le montant total de la fraude sur les cartes émises en France se stabilise à 464 millions d'euros, tout spécialement grâce

à l'application sur l'ensemble de l'année 2022 des règles d'authentification forte pour les transactions réalisées sur Internet. Le paiement par carte sur Internet reste toutefois le principal canal exposé à la fraude : s'ils ne représentent que près d'un quart des flux (22 %), ils véhiculent encore 68 % des montants de fraude.

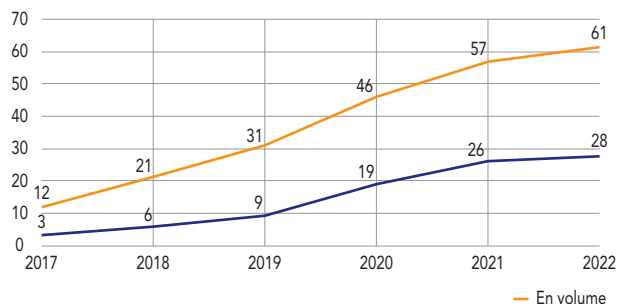
G11 Évolution des taux de fraude en valeur sur les cartes françaises par canal d'initiation (en %)



Source : Observatoire de la sécurité des moyens de paiement.

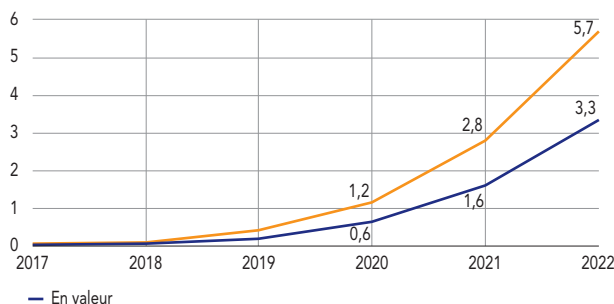
G12 Paiements par carte de proximité (en %)

a) Part des paiements sans contact



Source : Observatoire de la sécurité des moyens de paiement.

b) Part des paiements par mobile



Le taux de fraude sur les transactions par carte émise en France a sensiblement baissé de 0,059 % en 2021 à 0,053 % en 2022, soit une diminution de 10 % pour la deuxième année consécutive (13 % en 2021). Cette tendance se retrouve sur la plupart des canaux d'utilisation des cartes émises en France, avec des baisses plus substantielles sur :

- Les paiements sur Internet : leur taux de fraude continue de décroître de 0,196 % en 2021 à 0,165 % en 2022 (– 16 %), soit un nouveau plus bas historique. En cinq ans, ce taux de fraude aura ainsi chuté de 37 %, confirmant l'effet très positif des règles d'authentification forte de la DSP 2 et de l'amélioration des outils de mesure du risque par les acteurs de la monétique.
- Les paiements à distance hors Internet : leur taux de fraude encore très élevé chute néanmoins de 16 %. Ces paiements où le numéro de carte est communiqué

par courrier, téléphone ou courriel représentent moins de 1 % des paiements par carte.

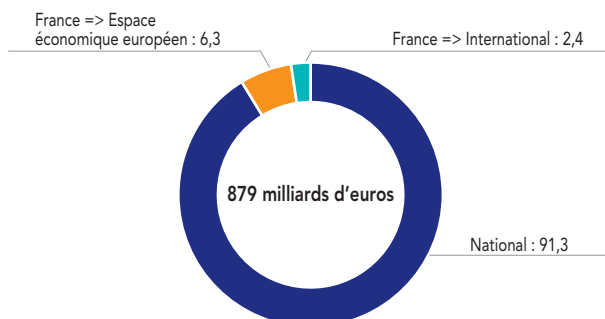
- Les paiements par mobile : leur taux de fraude reste six fois plus élevé que le reste des paiements par carte de proximité. Les enrôlements frauduleux de cartes usurpées dans des applications mobiles en sont le principal motif. Toutefois, leur taux de fraude fléchit à 0,061 % en 2022, quand bien même ce mode de paiement se développe rapidement (+ 137 % en volume, soit 5,7 % des paiements par carte de proximité).

Alors que le paiement sans contact en proximité consolide sa position de mode de paiement privilégié en proximité (61 % des transactions pour 28 % des montants), son taux de fraude progresse légèrement à 0,016 %, tout en restant à un niveau très faible. Cette légère hausse s'explique principalement par une recrudescence des vols de cartes utilisées pour quelques transactions inférieures au plafond de cinquante euros.

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

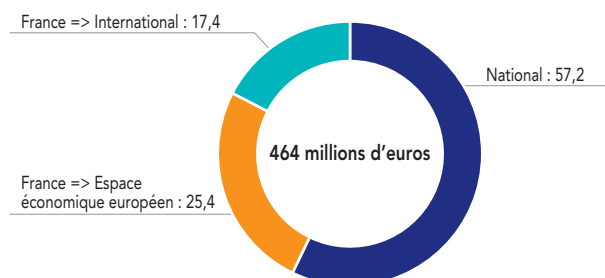
G13 Cartes émises en France par zone géographique (en %)

a) Répartition du montant des opérations

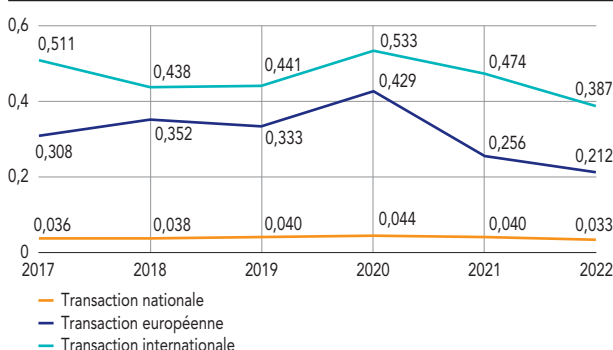


Source : Observatoire de la sécurité des moyens de paiement.

b) Répartition de la valeur de la fraude

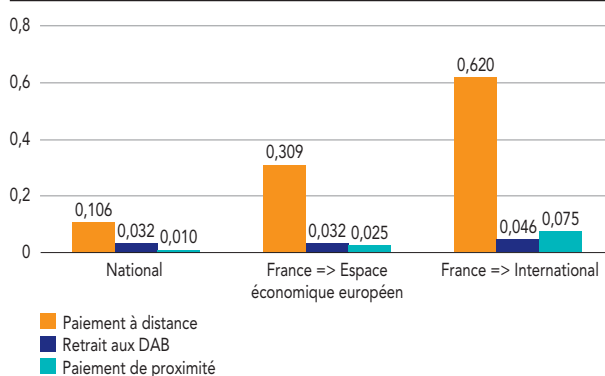


G14 Évolution des taux de fraude sur les cartes émises en France par zone géographique (en %)



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.

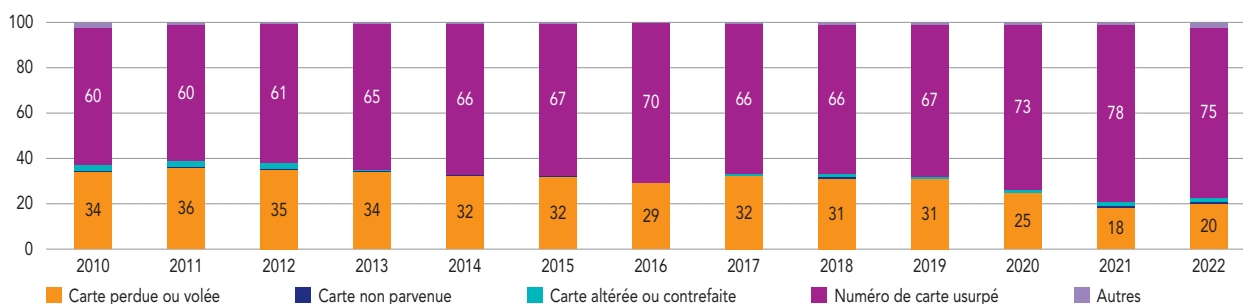
Dans les opérations réalisées au moyen de cartes émises en France, la part des transactions internationales (incluant les transactions vers l'Espace économique européen) demeure faible : que 9 % des transactions en 2022. En revanche, avec 198 millions d'euros de préjudice, celles-ci pèsent pour près de 43 % dans la fraude (contre 38 % en 2021).

Toutefois, si les transactions par carte à l'international sont structurellement plus sujettes à la fraude, car constituées pour l'essentiel de paiements à distance, leur taux de fraude continue de s'améliorer. Ainsi, le taux de fraude des transactions européennes, c'est-à-dire des cartes françaises auprès d'accepteurs européens, se contracte de 17 %, et celui des transactions internationales de 18 %.

Quelle que soit la zone géographique, les canaux dont les taux de fraude sont les plus élevés sont les paiements à distance, majoritairement constitués des paiements sur Internet. Le taux de fraude des paiements sur Internet au sein de l'Espace économique européen baisse de 15 %, grâce aux effets des règles d'authentification forte. Il reste cependant trois fois plus élevé que les paiements sur Internet au niveau national (0,309 %, contre 0,106 %). Les paiements de proximité à l'international sont plus exposés à la fraude, du fait de l'utilisation de technologies moins robustes. Ils sont donc plus vulnérables à la contrefaçon, comme la lecture de la piste magnétique ou la prise d'empreinte physique de la carte.

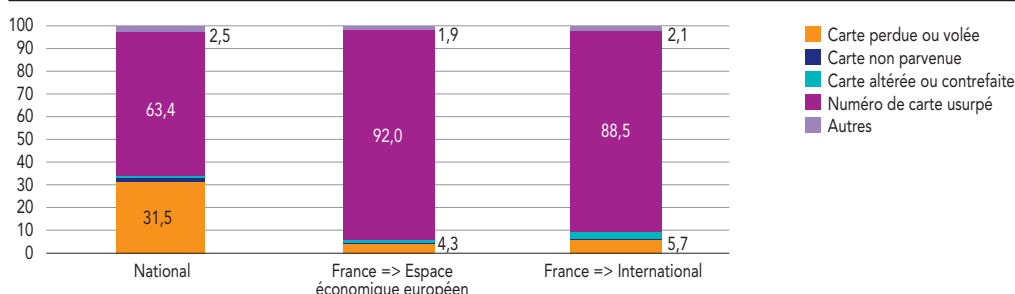
1.2.3 Répartition de la fraude par mode opératoire – Cartes émises en France

G16 Évolution des typologies dans la valeur de la fraude depuis 2010 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G17 Typologies dans la valeur de la fraude par zone géographique en 2022 (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, même si elle régresse légèrement : de 78 % en 2021 à 75 % en 2022. Les techniques de fraude associées à l'usurpation des numéros de carte restent l'hameçonnage par courriel ou par SMS.

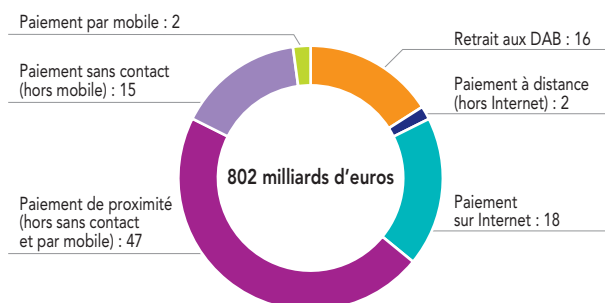
À l'inverse, la part de la fraude liée à la perte ou au vol de la carte augmente légèrement, et ce pour la première fois depuis 2017, tout en restant à un faible niveau (20 %).

Très logiquement, l'usage des cartes perdues ou volées se manifeste d'abord sur le territoire national (31,5 % de la fraude). La fraude par usurpation du numéro de carte, quant à elle, se concrétise d'abord sur Internet, quelles que soient les zones géographiques. L'usage des cartes altérées ou contrefaites se réalise principalement dans les pays extérieurs à l'Union européenne (4 % de la fraude dans cette zone géographique), où la distribution de la carte à puce n'est pas encore généralisée.

1.2.4 Répartition de la fraude sur les opérations nationales

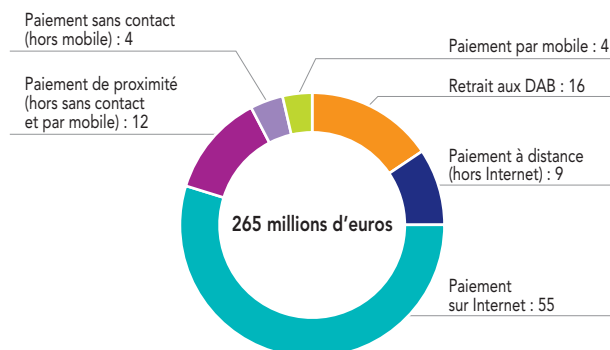
G18 Transactions nationales par carte en montant (en %)

a) Répartition des transactions

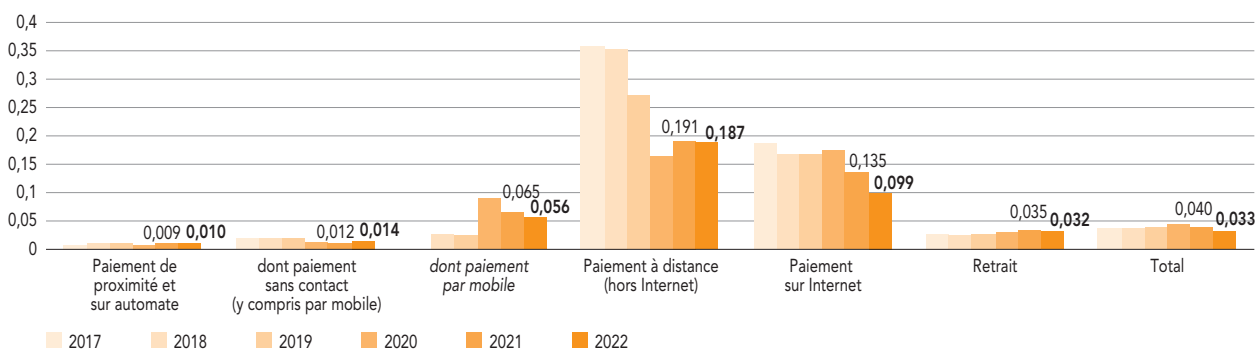


Note : DAB – distributeurs automatiques de billets.
Source : Observatoire de la sécurité des moyens de paiement.

b) Répartition de la fraude



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



Source : Observatoire de la sécurité des moyens de paiement.

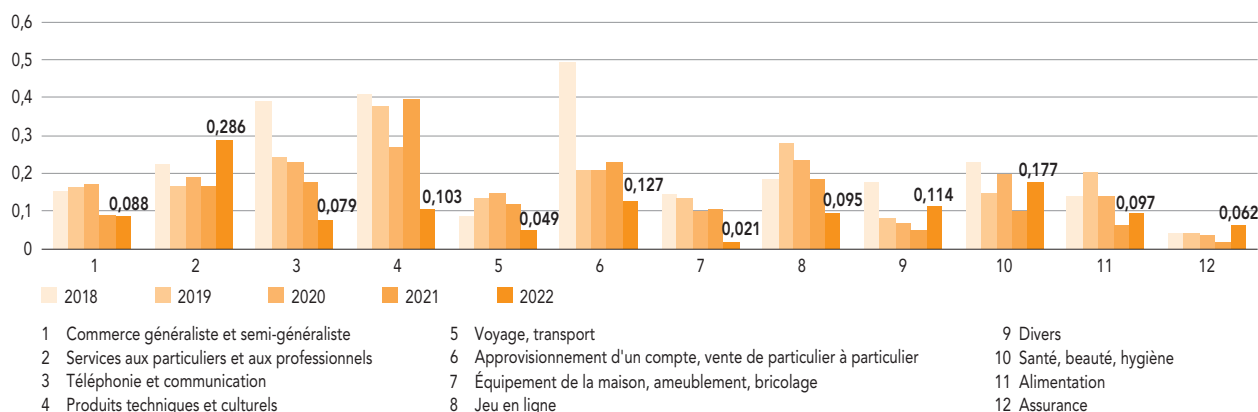
Les paiements à distance représentent de manière stable un cinquième des transactions nationales, dont l'essentiel sont des transactions sur Internet (92 %). Ils concentrent 64 % de la fraude (55 % pour les paiements sur Internet), mais enregistrent une baisse de 6 points par rapport à 2021. Toutefois, les paiements sur Internet bénéficient des effets de la généralisation de la mise en place de l'authentification forte en 2022. En effet, le taux de fraude de ces paiements chute de 27 % par rapport à 2021. Il se situe ainsi en dessous du seuil symbolique de 0,1 %, soit un nouveau plus bas niveau

historique. Par rapport à 2017, où les règles d'authentification forte de la DSP 2 n'étaient pas entrées en application, ce taux de fraude aura chuté de 47 %. En 2022, seuls les paiements de proximité et sur automates (y compris les paiements sans contact) voient leur taux de fraude très légèrement augmenter.

Au total, le taux de fraude des transactions nationales par carte se contracte. Sa baisse est substantielle : 18 % en 2022 pour s'établir à 0,033 %, après une première régression de 9 % en 2021.

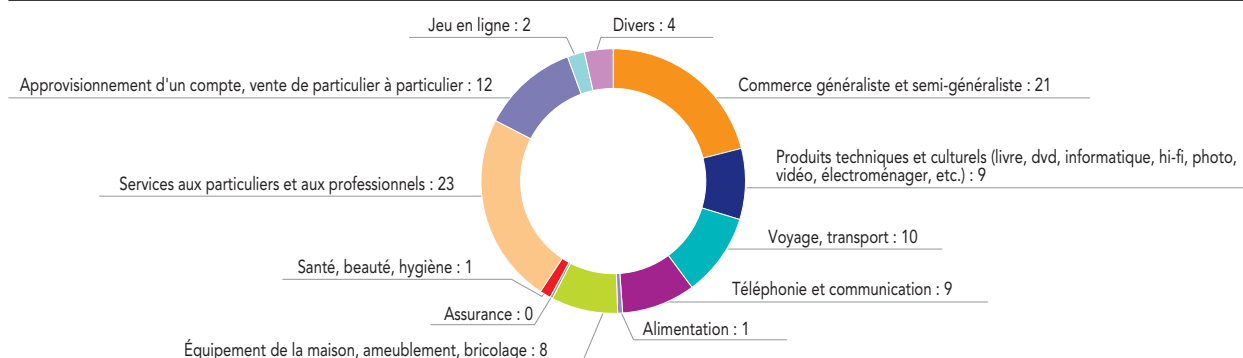
1.2.5 Focus sur la fraude aux paiements nationaux par carte sur Internet

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



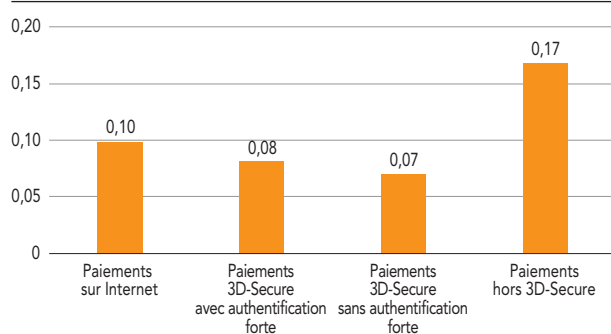
Source : Observatoire de la sécurité des moyens de paiement.

G21 Répartition de la fraude sur les paiements nationaux par carte sur Internet en valeur, par secteur en 2022 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

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



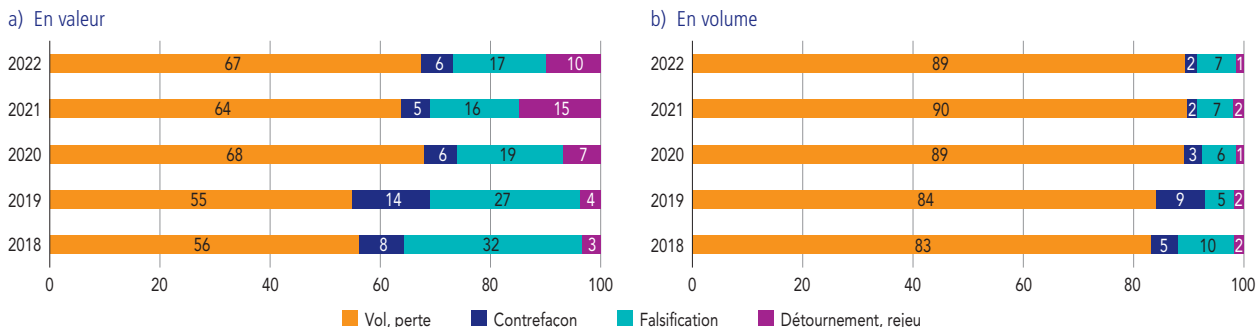
Source : Observatoire de la sécurité des moyens de paiement.

Au niveau national, les transactions sur Internet ayant recours au protocole d'échange 3D-Secure (ou protocole privatif équivalent) sont proportionnellement deux fois moins fraudées que celles qui s'en exonèrent. Parmi les transactions hors 3D-Secure, on retrouve principalement des paiements initiés par le commerçant (*Merchant Initiated Transactions* – MIT), qui s'apparentent à des prélèvements ayant la carte comme support (par exemple, abonnements, paiements différés ou réservations), ainsi que quelques transactions exemptées d'authentification forte.

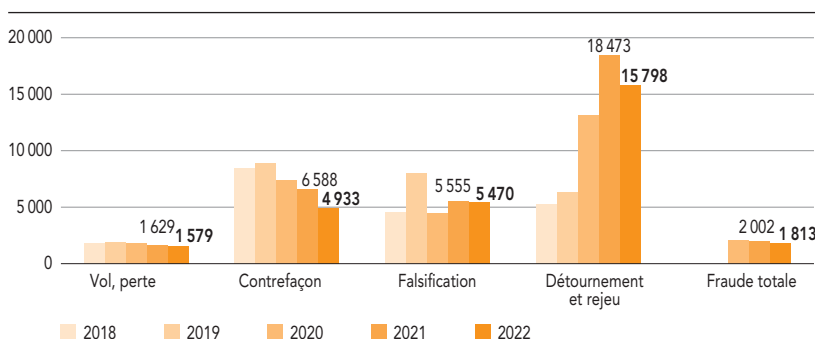
Par ailleurs, au niveau national, les exemptions à l'authentification forte sont appliquées de manière fiable. En effet, les transactions exemptées transitant par 3D-Secure ont un taux de fraude équivalent, voire légèrement inférieur aux transactions avec authentification forte (0,07 %, contre 0,08 %). Par conséquent, les exemptions sont ciblées sur les transactions les moins risquées.

1.3 État de la fraude sur le chèque

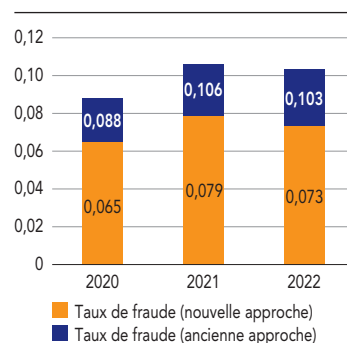
G23 Répartition de la fraude sur le chèque par typologie de fraude (en %)



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



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



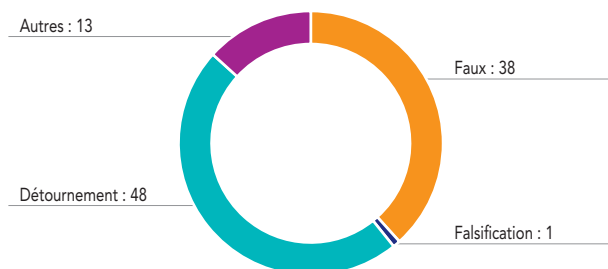
En 2022, le montant brut¹ des opérations frauduleuses par chèque fléchit à 395 millions d'euros (– 15 % par rapport à 2021). Les mécanismes de prévention contre la fraude, déployés par les banques, conformément à la feuille de route de l'Observatoire, et en particulier aux dispositifs de blocage ou de temporisation des remises de chèques, ont permis de neutraliser 161 millions d'euros de remises frauduleuses. Le taux de fraude baisse ainsi sensiblement de 0,079 % en 2021 à 0,073 % en 2022. La principale typologie de fraude reste, de loin, l'utilisation de chèques perdus ou volés directement remis à l'encaissement par le fraudeur ou utilisés comme moyen de règlement auprès des commerçants ou de particuliers (68 % des montants de fraude et 89 % des transactions frauduleuses). Le montant moyen de la fraude par chèque diminue globalement depuis 2020 pour atteindre 1 813 euros en 2022.

Ces bons résultats traduisent de façon plus visible les premiers effets du plan d'action décidée en 2021 par l'Observatoire contre la fraude au chèque. Le chèque reste toutefois le moyen de paiement affichant le taux de fraude le plus élevé. L'Observatoire appelle l'ensemble des acteurs à poursuivre leurs efforts et maintenir leur vigilance pour assurer le ralentissement du recours à ce moyen de paiement dans les meilleures conditions de sécurité possibles.

¹ À partir de 2020, la nouvelle approche de la fraude au chèque consiste à exclure les fraudes qui sont déjouées après remise de chèque à l'encaissement.

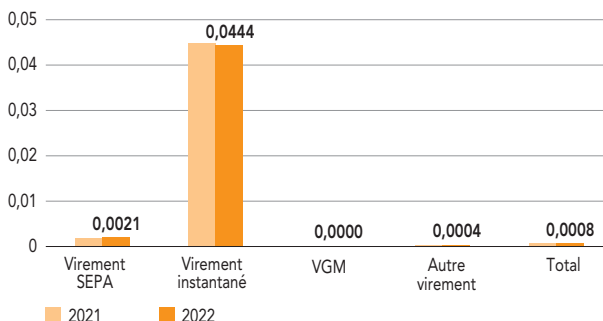
1.4 État de la fraude sur le virement

G26 Répartition de la fraude au virement en valeur par typologie de fraude en 2022 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

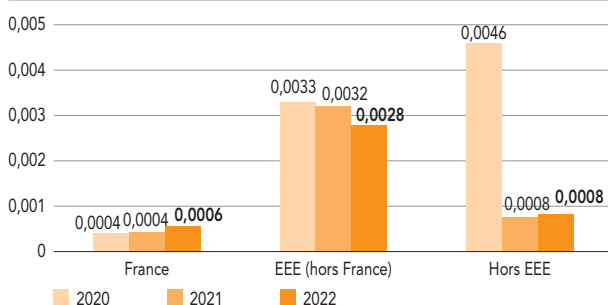
G27 Taux de fraude par type de virement (en %)



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

Source : Observatoire de la sécurité des moyens de paiement.

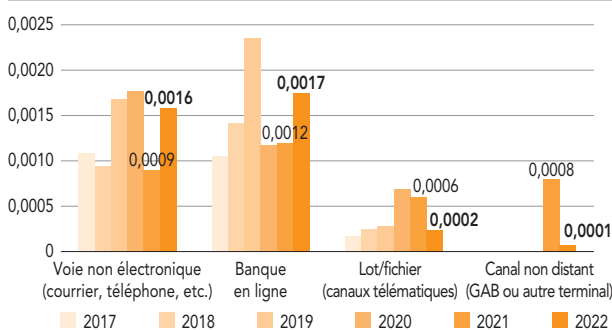
G28 Évolution du taux de fraude au virement par zone géographique (en %)



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 continue sa sensible progression. En cinq ans, le montant total de la fraude au virement a triplé passant de 98 millions d'euros en 2018 à 313 millions d'euros en 2022. En 2022, le nombre d'opérations frauduleuses a encore progressé de 64 % et de 9 % en valeur. Par conséquent, le montant moyen du virement fraudé baisse sensiblement, à environ 4 000 euros (contre environ 6 000 euros en 2021).

S'agissant du profil des victimes, la fraude au virement touche de plus en plus les particuliers et les professionnels, à la fois dans l'usage de leur banque en ligne (216 millions d'euros de fraude) et dans leurs virements initiés par voie non électronique (42 millions d'euros de fraude). À l'inverse, la sécurité des virements initiés par les entreprises et les administrations par les canaux télématiques s'améliore

nettement (53 millions d'euros de fraude, contre 92 millions en 2021).

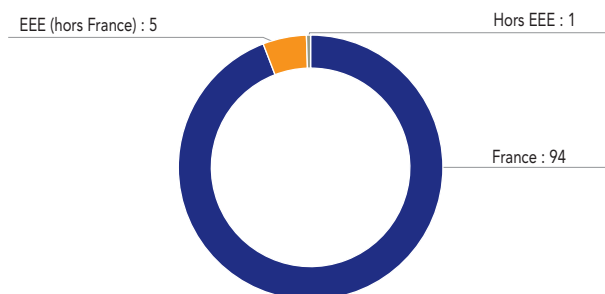
Les méthodes de la fraude au virement évoluent. Les fraudeurs utilisent davantage des comptes ouverts en France pour récupérer leurs fonds, même si les virements européens sont proportionnellement quatre fois plus fraudés que les virements nationaux. Par ailleurs, les fraudeurs mobilisent à la fois des techniques de récupération des accès à la banque en ligne par hameçonnage, et des techniques de manipulation par téléphone pour convaincre leurs victimes de fournir une donnée sensible ou valider une opération.

L'Observatoire se félicite néanmoins de la stabilité de la fraude sur le virement instantané, dont le taux de fraude se stabilise et reste inférieur à celui de la carte (0,044 %, contre 0,053 %).

1.5 État de la fraude sur le prélèvement

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

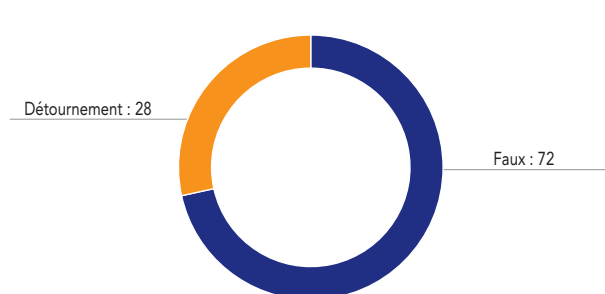
a) Par zone géographique



Note : EEE – Espace économique européen.

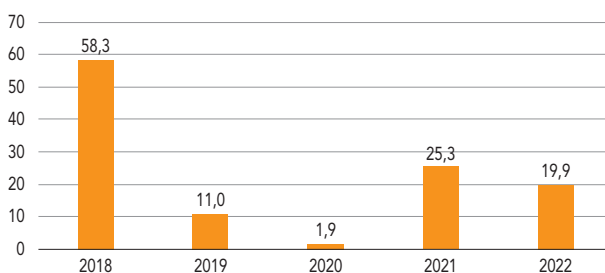
Source : Observatoire de la sécurité des moyens de paiement.

b) Par typologie de fraude



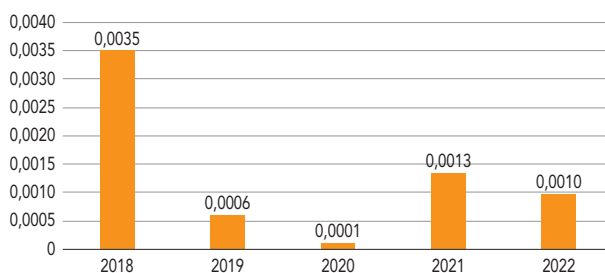
G31 Fraude au prélèvement

a) En valeur (en millions d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

b) Taux (en %)



La fraude au prélèvement est extrêmement volatile. L'année 2022 se termine par une légère diminution du montant de la fraude à 20 millions d'euros (contre 25 millions d'euros en 2021), ce qui transparaît dans son taux (0,0010 % en 2022, contre 0,0013 %). Il s'agit majoritairement de créanciers fraudeurs, qui émettent de faux ordres, sans disposer d'un mandat de prélèvement ni de relation économique avec la victime.

L'Observatoire relève toutefois trois évolutions notables par rapport à 2021 :

- tout d'abord, la fraude enregistrée par les établissements des créanciers touche très majoritairement des comptes ouverts en France (94 %), alors que les comptes ouverts dans un autre pays européen étaient principalement ciblés en 2021 (57 % en 2021),

- ensuite, le montant moyen de la fraude a été multiplié par quatre, ce qui indique une action plus ciblée des fraudeurs,
- enfin, la fraude par détournement, pour lequel le fraudeur débiteur usurpe l'identité et l'IBAN d'un tiers pour la signature d'un mandat de prélèvement, représente 28 % du montant total de la fraude, alors que cette typologie de fraude avait quasiment disparu depuis 2019.

①

Indicateurs, enseignements et préconisations des services du ministère de l'Intérieur sur la fraude aux moyens de paiement en 2022

Le ministère de l'Intérieur est représenté à l'Observatoire par le Service central de renseignement criminel (SCRC) de la Gendarmerie nationale et la Direction centrale de la police judiciaire (DCPJ) de la Police nationale. Comme chaque année, ces deux services ont communiqué en 2022 leurs principales observations sur les fraudes aux moyens de paiement constatées à l'Observatoire.

Les collectes statistiques du ministère de l'Intérieur sont fondées sur des approches méthodologiques différentes de celles de l'Observatoire. Toutefois, quand la comparaison est possible, les données font ressortir des évolutions cohérentes, ce qui renforce les constats de l'Observatoire sur l'évolution de la fraude aux moyens de paiement scripturaux.

1. Les fraudes à la carte bancaire : un taux de signalement en hausse et des chiffres cohérents avec ceux remontés par les acteurs des paiements à l'Observatoire

Les services de police et de gendarmerie comptabilisent les infractions se rapportant à l'utilisation frauduleuse d'une carte bancaire, que les captations des données aient été effectuées en France ou à l'étranger. Les forces de l'ordre s'appuient sur deux sources statistiques :

- les chiffres du Service statistique ministériel de la sécurité intérieure (SSMSI), répertoriant l'ensemble des données remontées par les services de police et de gendarmerie ;
- les chiffres provenant de recherches par nature d'infractions (NATINF), qui est un indicateur de qualification pénale des infractions produit par le ministère de la Justice.

Ces deux nomenclatures ne permettent pas de quantifier spécifiquement le nombre et le préjudice financier des fraudes à la carte bancaire. Toutefois, elles consolident un agrégat constitué de vols de cartes bancaires, d'usages frauduleux de cartes perdues, de falsifications et de contrefaçons. Les possibilités de rapprochement avec les données agrégées de l'Observatoire sont donc limitées.

En revanche, les rapprochements sont plus aisés avec les enregistrements sur la plateforme Perceval de la gendarmerie, qui est la plateforme nationale de recueil de signalement des usages frauduleux de cartes bancaires sur Internet, destinée à tous les usagers. Elle fait état de 304 923 signalements en 2022 (contre 324 594 en 2021, soit une baisse de 6,1 %) pour un préjudice total de 161 millions d'euros (contre 140 millions d'euros en 2021, soit une hausse de 14 %), soit un préjudice moyen par signalement de 529 euros (contre 431 euros en 2021, soit + 23 % en un an). Un signalement sur la plateforme Perceval peut, cependant, couvrir plusieurs transactions initiées frauduleusement à partir des mêmes données de carte usurpée.

La comparaison avec les statistiques de l'Observatoire fait ressortir un taux de signalement des fraudes en augmentation sur Perceval. En effet, 51 % de la fraude à la carte sur les paiements à distance telle que quantifiée par l'Observatoire aurait été signalée sur Perceval en 2022, contre 40 % en 2021. Les victimes ont tendance à ne déclarer que les fraudes les plus importantes : en 2022, le montant moyen par transaction frauduleuse est de 58 euros d'après les statistiques de l'Observatoire, contre 131 euros d'après Perceval.

T1 Nombre de faits de fraude à la carte bancaire recensés par la police et la gendarmerie (nombre en unités, variation en %)

	2018	2019	2020	2021	2022	Variation 2022/2021
Source SSMSI ^{a)}	57 796	67 366	61 235	74 706	78 373	4,91
Source NATINF	53 276	64 168	58 414	70 425	72 955	3,59

a) L'historique du nombre de faits de fraude peut augmenter d'une année sur l'autre, étant donné que les forces de l'ordre peuvent enregistrer des plaintes relatives à des cas de fraude sur les années antérieures.

Sources : Service statistique ministériel de la sécurité intérieure (SSMSI) et ministère de la Justice.

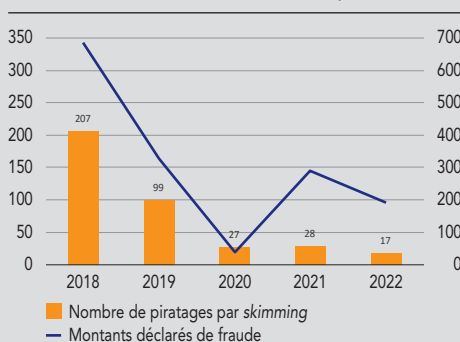
L'Observatoire rappelle l'utilité des déclarations de fraude sur la plateforme Perceval qui permettent aux forces de l'ordre de recouper les informations nécessaires aux démantèlements des réseaux de fraudeurs.

2. Les piratages de terminaux de paiement et de retrait : en baisse depuis plusieurs années, malgré quelques affaires ciblées

Les piratages peuvent cibler des automates de paiement ou de retrait d'argent (distributeurs de billets, distributeurs automatiques de carburant, automates d'autoroute, 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*¹ 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.

Nombre de piratages par *skimming* et montants déclarés de fraude en euros depuis 2018 (échelle de gauche : nombre en unités, échelle de droite : montants en milliers d'euros)



Sources : Groupement des cartes bancaires et Direction centrale de la police judiciaire (DCPJ).

Les chiffres des forces de l'ordre mettent en lumière une chute drastique des piratages par *skimming* sur ces dernières années.

Pour l'année 2022, 17 attaques ont été recensées pour un préjudice total de 190 000 euros (contre 290 000 euros en 2021, soit une baisse de 53 %), dont 3 attaques sur des distributeurs automatiques de billets (DAB), contre 15 en 2021, et 14 sur des distributeurs de carburant (DAC), contre 13 en 2021. Ces tendances sont cohérentes avec celles remontées par les acteurs des paiements à l'Observatoire. En 2022, l'Observatoire enregistre notamment une baisse de 64 % de la fraude liée à des cartes contrefaites utilisées pour des opérations de retrait en dehors de l'Europe, pour un préjudice total de 127 000 euros.

Néanmoins, les gestionnaires de stations-service, comme les gestionnaires de DAB, doivent rester vigilants pour prévenir les tentatives de substitution d'un terminal de paiement légitime par un terminal compromis ou toute installation par un tiers d'un dispositif externe frauduleux (lecteur, caméra, clavier, etc.). Les forces de l'ordre ont en effet constaté une activité toujours importante des fraudeurs. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) reçoit, via Interpol, un nombre croissant de demandes de gel des vidéos de surveillance des stations-service : 110 demandes en 2022, contre 91 en 2021 et 76 en 2020. Les cartes piratées en France, principalement des cartes carburant, seraient ensuite utilisées sur les péages autoroutiers en France ou en Europe centrale et orientale, notamment en Pologne, en République tchèque, en Slovaquie, en Slovaquie et en Bulgarie.

La fraude au *shimming*² repose sur des procédés similaires au *skimming* mais visant à récupérer les données contenues dans la puce de la carte. La complexité technique du dispositif limite encore les attaques. Le préjudice financier lié à ce type d'attaque n'avait pas été estimé en 2021, mais il s'approcherait des 50 000 euros en 2022.

¹ Matériel se glissant dans le lecteur de carte d'un automate tout en laissant de l'espace pour qu'une carte de paiement puisse y être insérée naturellement. Une copie des données de la piste magnétique sera alors réalisée par le matériel sans que cela ait une quelconque implication sur le bon fonctionnement de la carte bancaire.

² 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.

3. Les attaques par *jackpotting* contre les distributeurs automatiques de billets (DAB) : en baisse grâce au démantèlement des réseaux

Les forces de l'ordre continuent leurs investigations contre les attaques de distributeurs automatiques de billets par *jackpotting*. Il s'agit d'une attaque physique ou logique d'un DAB afin de pirater l'ordinateur intégré, d'en prendre le contrôle et ainsi d'actionner les mécanismes de délivrance des billets. Ces techniques très sophistiquées ne peuvent être mises en œuvre que par des réseaux organisés ou des délinquants spécialisés.

Les préjudices associés au *jackpotting* sont en baisse sensible : 22 faits ont été recensés en 2022 pour un montant total de 74 970 euros, contre 32 pour 335 370 euros en 2021 et 95 pour 681 170 euros en 2020. Ce type d'attaque n'est pas remonté dans les données de l'Observatoire, ces pertes étant comptabilisées en risque opérationnel par les gestionnaires des DAB, et non comme de la fraude sur les moyens de paiement en tant que telle.

La diminution nette de ce type de délinquance peut s'expliquer par l'action des forces de l'ordre (infiltration, exploitation des images de vidéosurveillance, mise sur écoute, etc.) qui permet de démanteler les réseaux : l'OCLCTIC a procédé à l'interpellation de douze « jackpoteurs » et au démantèlement de cinq équipes de malfaiteurs en 2021. De plus, en 2022, elles ont aussi interpellé un suspect connu de la Justice pour des faits similaires. L'affaire est en cours d'instruction.

Ces bons résultats sont également liés au renforcement de la sécurité des distributeurs par les gestionnaires de DAB. Toutefois, l'OCLCTIC note l'obsolescence du matériel et des logiciels, qui facilite encore trop souvent la réussite des attaques. Par conséquent, il préconise aux gestionnaires de DAB des mesures minimales de sécurité, en particulier de :

- procéder à une mise à jour systématique des systèmes d'exploitation,
- chiffrer le disque dur pour prévenir les attaques ne passant pas par le système d'exploitation,
- installer des capteurs anti-intrusion en mesure de mettre le DAB hors service en cas d'attaque,
- ou encore de renforcer la sécurité de la communication entre l'automate et les appareils dédiés à la maintenance.

4. Les faux ordres de virement : globalement stables, mais un point de vigilance pour les collectivités locales

Les escroqueries aux « faux ordres de virement » (FOVI) sont caractérisées par les forces de l'ordre comme une arnaque financière consistant à obtenir de la victime un virement imprévu vers un compte bancaire géré par l'escroc. Procédant généralement par téléphone ou par courriel et usant de techniques d'ingénierie sociale, les escrocs exploitent les vulnérabilités techniques, humaines et organisationnelles d'une entreprise ou d'une administration publique afin de faire réaliser des virements frauduleux.

La généralisation du télétravail depuis 2020 avait favorisé une recrudescence exponentielle des cas de FOVI. Le déploiement rapide de nouveaux modes de fonctionnement et d'organisation qui a ainsi permis l'exploitation de vulnérabilités nouvelles ou préexistantes par des acteurs malveillants. **En 2022, si le nombre de cas de FOVI augmente, le préjudice global est en baisse** : les forces de l'ordre ont relevé 670 affaires de FOVI pour un préjudice total de 64 millions d'euros, contre 517 affaires en 2021 pour un préjudice total de 101 millions d'euros, dont une seule fraude d'un montant exceptionnel de 33 millions d'euros.

Les entreprises du secteur privé ne sont pas les seules cibles des fraudeurs. **Les institutions publiques et notamment les collectivités locales (centres hospitaliers universitaires, théâtres municipaux, mairies, métropoles, communes, villes, départements, etc.) ont représenté en 2022 la moitié des faits connus de la Police judiciaire.**

Ces évolutions sont cohérentes avec les tendances générales remontées par les acteurs des paiements à l'Observatoire : la fraude au virement progresse sur les segments de la banque en ligne, concernant les particuliers et les professionnels, mais se stabilise sur les canaux touchant les entreprises et les administrations.

T2 Comparaison des données de fraude au virement impliquant une manipulation de la victime entre 2021 et 2022

(montant en euros, nombre en unités, variation et taux en %)

	Observatoire ^{a)}			FOVI de la Police nationale			Taux de signalement	
	2021	2022	Variation 2022/2021	2021	2022	Variation 2022/2021	2021	2022
Valeur totale de la fraude	168 094 274	148 732 203	- 12	101 200 000	64 000 000	- 37	60	43
Nombre d'opérations frauduleuses	8 523	16 991	+ 99	517	670	+ 30	6	4
Montant moyen d'une fraude	19 722	8 754	- 56	195 745	95 522	- 51	na	na

a) Dans la méthodologie de l'Observatoire, les FOVI peuvent être assimilés aux détournements de virement (cf. annexe 4 sur la méthodologie statistique). Toutefois, la comparaison est limitée par le fait que les chiffres de la Police nationale concernent essentiellement les entreprises et les administrations, tandis que les chiffres de l'Observatoire couvrent l'ensemble des utilisateurs, y compris les particuliers.

Note : FOVI – faux ordres de virement; na – non applicable.

Sources : Direction centrale de la police judiciaire et Observatoire de la sécurité des moyens de paiement.

MODALITÉS DE REMBOURSEMENT DES OPÉRATIONS DE PAIEMENT FRAUDULEUSES

2.1 Contexte des travaux

2.1.1 La mise en place de l'authentification forte du porteur pour sécuriser les paiements électroniques

Le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique est une disposition clé en matière de sécurité des paiements, qui a été introduite par la deuxième directive européenne sur les services de paiement (DSP 2)¹. Pour ce qui concerne les paiements par carte sur Internet, la mise en œuvre de cette disposition au niveau du marché français s'est appuyée sur un plan de migration adopté par l'Observatoire à l'automne 2019, et l'authentification forte a ensuite été déployée sur une période de deux ans environ.

Pour mémoire, l'authentification forte repose sur l'utilisation de deux éléments ou plus appartenant au moins à deux catégories différentes de facteurs d'authentification, parmi les trois catégories suivantes :

- « connaissance » : une information que seul l'utilisateur connaît, par exemple un code confidentiel, un mot de passe ou une information personnelle ;
- « possession » : un objet que seul l'utilisateur possède, et qui peut être reconnu sans risque d'erreur par le prestataire de services de paiement (PSP) comme une carte, un *smartphone*, une clé USB, un boîtier sécurisé, une montre ou un bracelet connecté, etc. ;
- « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique (empreinte digitale, visage, voix, etc.).

Lorsque l'enrôlement d'un élément de possession, c'est-à-dire l'association à un utilisateur d'un objet que seul cet utilisateur possède et qui servira de facteur d'authentification forte,

s'effectue à distance, alors cet enrôlement doit lui-même être validé par authentification forte.

La DSP 2 dispose que ces éléments doivent être indépendants : la compromission de l'un ne doit pas remettre en question la fiabilité des autres, de manière à préserver la confidentialité des données d'authentification. En outre, concernant les paiements à distance, la DSP 2 ajoute une exigence supplémentaire : les données d'authentification doivent être liées à l'opération de paiement, de sorte qu'elles ne peuvent être réutilisées pour une opération de paiement ultérieure. On parle de lien dynamique :

- le code d'authentification généré pour l'opération est spécifique au montant de l'opération et au bénéficiaire identifié ;
- toute modification du montant ou du bénéficiaire nécessite une nouvelle authentification.

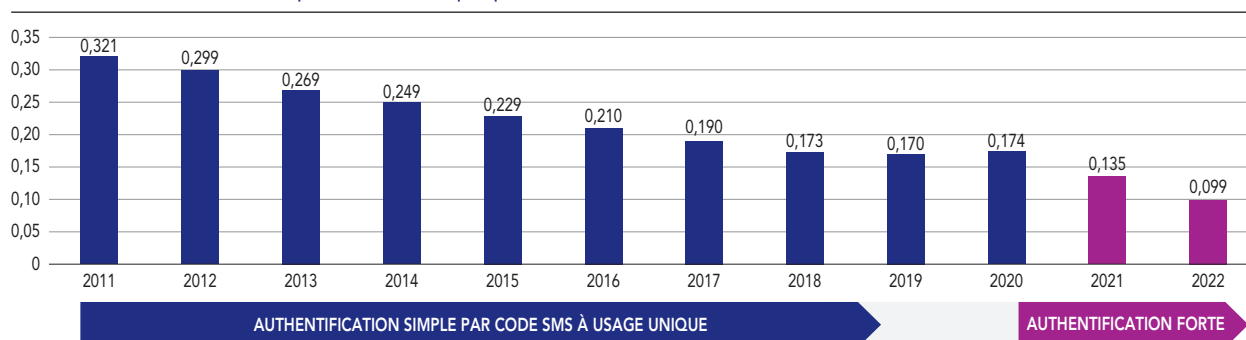
Dans le cas du recours à un facteur biométrique, la clé de validation de l'opération de paiement générée après lecture de l'empreinte devra être également à usage unique.

S'il est encore trop tôt pour tirer un bilan définitif de la mise en place de l'authentification forte, l'Observatoire note d'ores et déjà qu'elle a contribué à faire baisser substantiellement le taux de fraude sur les paiements Internet, après deux ans de stagnation qui soulignaient les limites atteintes en matière de sécurité par l'utilisation de l'authentification simple (SMS-OTP – *one time password*, code SMS à usage unique) déployée durant les années 2010. Les premières données disponibles concernant 2022 montrent que le taux de fraude devrait continuer à baisser de façon significative.

¹ Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015

concernant les services de paiement dans le marché intérieur.

Évolution du taux de fraude sur les paiements domestiques par carte sur Internet (en %)



Source : Observatoire de la sécurité des moyens de paiement.

Sur l'ensemble des paiements par carte sur Internet (y compris les paiements réalisés auprès de sites étrangers par les porteurs français), le taux de fraude en montant sur les paiements en ligne est ainsi passé de 0,249 % en 2020 à 0,196 % en 2021, soit son plus bas niveau historique, alors que sur la même année, le montant des opérations de paiement par carte a crû de 21 % pour atteindre 177,1 milliards d'euros.

2.1.2 Le développement de nouvelles techniques de fraude fondées sur la manipulation pour contourner l'authentification forte

Si la mise en place de l'authentification forte permet d'assurer un haut niveau de sécurité technologique sur l'ensemble de la chaîne des paiements, elle rend d'autant plus nécessaire de renforcer la vigilance des utilisateurs, qui sont de plus en plus ciblés par des fraudeurs. À défaut de pouvoir émettre eux-mêmes des paiements frauduleux, les fraudeurs essaient en effet de manipuler leurs victimes par téléphone ou par messagerie instantanée pour les amener à valider à leur place des opérations frauduleuses, en se faisant généralement passer pour leur banque (par exemple, en prétextant des tests de sécurité, la lutte contre la fraude ou en annonçant une opération atypique sur le compte de la victime nécessitant un contrôle par authentification). Ils parviennent à convaincre leur victime de communiquer des informations leur permettant d'utiliser à distance leurs moyens de paiement. Ils récoltent d'abord des informations sur leur victime grâce aux attaques de type hameçonnage par SMS ou message électronique, aux vols de données à des tiers, mais aussi grâce aux réseaux sociaux et à différentes sources publiques, puis contactent directement la victime. Les fraudeurs ont également recours au « *spoofing* », c'est-à-dire qu'ils parviennent à usurper le numéro de téléphone d'une agence bancaire afin de rassurer leur victime.

Si l'Observatoire constate que la proportion de paiements frauduleux avec authentification forte est restée contenue en 2021, soit 9 % du nombre total des paiements frauduleux par carte sur Internet, leur proportion dans le montant total des opérations frauduleuses est bien plus significative (30 % du montant total de 103 millions d'euros).

Selon les associations de consommateurs, ce nouveau type de fraude entraînerait une augmentation du montant du préjudice financier supporté par les consommateurs, en dépit de la baisse globale de la fraude. En effet, avec la mise en œuvre de l'authentification forte, le risque de refus de remboursement des opérations frauduleuses par la banque à son client est susceptible d'avoir augmenté de manière significative.

À ce titre, les associations de consommateurs ont alerté la Banque de France et l'Observatoire de la sécurité des moyens de paiement sur les difficultés rencontrées par leurs adhérents pour bénéficier du droit à remboursement en cas de fraude prévu par les textes, en particulier dans les cas où l'opération contestée a fait l'objet d'une authentification forte.

2.1.3 Les travaux conduits par l'Observatoire sur le traitement des contestations pour motif de fraude

L'Observatoire a mis en place un groupe de travail chargé d'émettre des recommandations sur le traitement des demandes de remboursement d'opérations frauduleuses en vue d'assurer la bonne application des dispositions de la DSP 2 en matière de protection des consommateurs victimes de fraude.

Le groupe de travail s'est réuni à cinq reprises entre octobre 2022 et février 2023. Les participants à ce groupe de travail représentent les associations de consommateurs,

les prestataires de services de paiement, leurs fédérations professionnelles, les médiateurs et les autorités (police, gendarmerie, Autorité de contrôle prudentiel et de résolution – ACPR, Banque de France).

Le secrétariat du groupe de travail a défini les éléments en entrée ainsi que les livrables attendus en sortie :

Périmètre de la mission du groupe de travail

Éléments en entrée	Livrables attendus en sortie
Réglementation et jurisprudence applicables au traitement des contestations	Rappel des règles applicables en matière de traitement des demandes de remboursement pour motif de fraude
Identification des développements récents en matière de typologie des cas de fraude	Grille d'analyse des demandes de remboursement (identifier les cas pour lesquels un remboursement immédiat devrait être systématique)
Expérience des médiateurs bancaires et des associations de consommateurs sur des demandes non satisfaites de remboursement pour motif de fraude	Recommandations sur le traitement des demandes de remboursement pour motif de fraude
Synthèse des contrôles sur place conduits par l'ACPR concernant le traitement des demandes de remboursement des clients pour motif de fraude	Revue des motifs identifiés dans le cadre des déclarations à la Banque de France au titre de l'article L.133-18 du Code monétaire et financier (à engager à l'issue de la publication des recommandations présentées dans ce document)

Source : Observatoire de la sécurité des moyens de paiement.

2.2 Réglementation applicable aux contestations d'opérations de paiement

2.2.1 Le caractère « autorisé » de la transaction comme facteur déterminant

Selon le Code monétaire et financier (CMF), le remboursement d'une opération contestée est conditionné par le fait qu'elle ait été autorisée ou non par le payeur². L'autorisation de paiement par le payeur signifie que celui-ci a explicitement donné son consentement à son exécution dans les conditions prévues par sa convention de compte, notamment par l'utilisation du moyen d'authentification forte mis à sa disposition.

Le schéma *infra* illustre l'articulation des textes relatifs aux opérations contestées dans le Code monétaire et financier.

- Si l'opération est reconnue comme « autorisée » et qu'elle n'a pas été affectée par une erreur d'exécution de la part du prestataire de services de paiement

du payeur, la réglementation relative aux moyens de paiement ne prévoit pas de droit à remboursement. C'est le cas notamment pour les demandes de remboursement pour cause de litige commercial entre le payeur et le bénéficiaire (par exemple : non-livraison ou malfaçon d'un produit, souscription d'un produit d'épargne, de crédit ou d'un service financier auprès d'un intermédiaire malveillant, etc.). **À défaut de droit à remboursement prévu par la réglementation, la qualification de l'opération comme « autorisée » n'empêche pas une réclamation à l'encontre du bénéficiaire, voire une action civile ou pénale.**

- Si l'opération est reconnue comme « non autorisée », le payeur dispose, en règle générale, d'un droit à remboursement immédiat prévu par le Code monétaire et financier. Les modalités diffèrent toutefois en fonction de différents paramètres, tels que la nature de l'instrument de paiement, le fait qu'il soit doté de données de sécurité personnalisées ou l'usage d'un dispositif d'authentification forte lors de la transaction. **Ce remboursement peut cependant être refusé en cas de comportement frauduleux de l'utilisateur lui-même ou, pour les seules opérations authentifiées de manière forte dans les conditions prévues par la loi³, en cas de négligence grave de l'utilisateur démontrée par le prestataire de services de paiement.**

L'appréciation du caractère autorisé ou non d'une opération est donc un critère déterminant pour le remboursement des clients qui contestent une opération de paiement pour motif de fraude. Cette question est particulièrement sensible dans le cas d'opérations ayant fait l'objet d'une authentification forte, où il convient de déterminer dans quelle mesure le succès de l'authentification forte peut être ou non assimilé à un consentement du porteur de l'instrument de paiement.

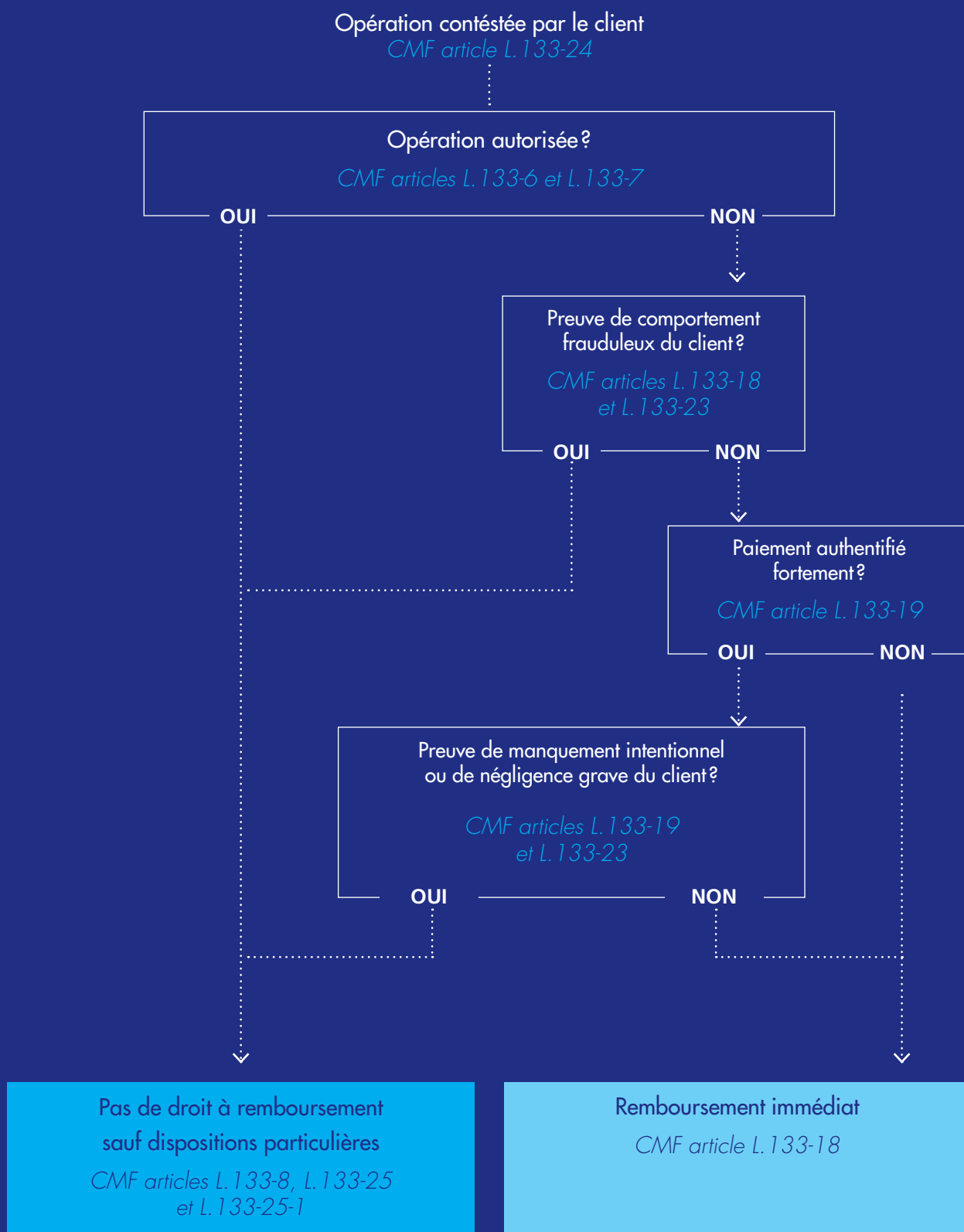
L'objectif des recommandations présentées ci-après est de réduire la « zone grise » sur l'appréciation du caractère « non autorisé » d'une opération contestée, par l'examen de différents cas de contestation, du plus simple au plus complexe. Il s'agit de déterminer sous quelles conditions l'opération peut être présumée non autorisée et donner lieu à remboursement immédiat, à moins que le prestataire de services de paiement n'apporte la preuve de la fraude ou de la négligence grave de l'utilisateur.

² Hors cas particulier du régime de remboursement applicable à certaines opérations autorisées, dont les prélèvements intervenus depuis moins

de huit semaines (articles L.133-25 et L.133-25-1 du CMF).

³ Article L.133-4 alinéa f du CMF.

TEXTES LÉGISLATIFS DU CODE MONÉTAIRE ET FINANCIER (CMF) LIÉS AUX OPÉRATIONS DE PAIEMENT CONTESTÉES PAR LE CLIENT



Source : Observatoire de la sécurité des moyens de paiement.

2.2.2 Apports de la jurisprudence sur l'appréciation de la négligence grave de l'utilisateur de services de paiement

Les textes ne précisent pas explicitement quels sont les éléments qui caractérisent une négligence grave de l'utilisateur, qui est le principal motif invoqué par les prestataires de services de paiement pour refuser le remboursement d'un paiement non autorisé. En outre, il n'existe pas encore de jurisprudence de la Cour de cassation portant sur une contestation d'opération effectuée postérieurement à l'entrée en vigueur de la DSP 2, ni de textes pris pour sa transposition et son application. La jurisprudence actuelle (relative à des contestations d'opérations effectuées antérieurement à l'entrée en vigueur de la DSP 2) repose sur le concept d'utilisateur « normalement attentif ». Dans ce contexte, il convient, pour les prestataires de services de paiement qui souhaitent recourir à ce motif d'exclusion du droit à remboursement, d'évaluer le cas au regard de la jurisprudence. Même si celle-ci sera vraisemblablement amenée à s'enrichir dans les prochaines années, certaines décisions sont néanmoins d'ores et déjà éclairantes.

2.3 Recommandations générales applicables au traitement des contestations d'opérations de paiement

2.3.1 Délai pour la conduite des investigations

Lorsque des investigations doivent être conduites par le prestataire de services de paiement (par exemple, investigations liées à une opération de paiement authentifiée de manière forte, *cf. paragraphe 4.3 infra*), il apparaît nécessaire que la durée de ces investigations soit limitée dans le temps. En effet, il s'agit, d'une part d'éviter la disparition ou l'oubli des éléments d'information utiles au PSP, et d'autre part de permettre au client de disposer, à une échéance suffisamment proche et connue, d'une réponse claire et définitive à sa contestation.

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 trente jours, sauf situation exceptionnelle.

2.3.2 Modalités et délai de reprise des fonds

Il existe différents cas de figure dans lesquels une décision initiale de remboursement du client par le prestataire de services de paiement est susceptible d'être remise en cause *a posteriori*. Ainsi, le prestataire peut procéder à une reprise des fonds, par exemple, en cas d'investigations complémentaires le conduisant à revenir sur sa décision initiale ou si l'utilisateur vient à être remboursé par un autre canal (par la contrepartie de l'opération, via un mécanisme d'assurance, etc.). Il apparaît nécessaire que l'utilisateur soit informé, le cas échéant, de cette possibilité au moment de son remboursement initial.

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 issu des 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.

2.3.3 Information délivrée au client en cas de refus de remboursement ou de reprise des fonds

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.

2.4 Recommandations applicables au traitement de cas spécifiques

Les cas présentés dans cette partie excluent volontairement les demandes de remboursement ne relevant pas du périmètre de la fraude aux moyens de paiement, telles que les litiges commerciaux et les escroqueries (par exemple, faux produits d'épargne, investissements dans des cryptoactifs crapuleux, arnaques au crédit, etc.), lorsque les opérations concernées ont été autorisées.

De même, les recommandations sont centrées sur l'application du droit à remboursement prévu par la réglementation relative aux moyens de paiement. Elles excluent les autres mécanismes pouvant exister par ailleurs, tels que les assurances de moyens de paiement, ou encore les gestes commerciaux consentis par les prestataires de services de paiement.

2.4.1 Opérations de paiement effectuées sans authentification forte

Toutes les opérations ne sont pas soumises à l'obligation d'authentification forte. La réglementation issue de la deuxième directive européenne sur les services de paiement (DSP 2) prévoit un ensemble de cas d'exclusion ou d'exemption à son application :

- Les **paiements en dehors de l'Union européenne (transactions dites *one leg*)** ;
- Les **ordres de paiement émis par le bénéficiaire du paiement**, tels que les prélèvements ou les paiements par carte de type *Merchant Initiated Transactions (MIT)*, c'est-à-dire émis par le commerçant sans connexion active de l'utilisateur : notamment les paiements fractionnés ou différés, les abonnements et les paiements à l'usage ;
- Les **paiements éligibles à un motif d'exemption à l'authentification forte prévu par les normes techniques de réglementation (RTS)** arrêtées par l'Autorité bancaire européenne (ABE)⁴ :
 - les paiements sur Internet de faible valeur (article 16), soit moins de trente euros, et dans la limite de cinq opérations consécutives ou d'un montant cumulé de cent euros ;
 - les paiements présentant un faible niveau de risque (article 18), c'est-à-dire correspondant aux habitudes d'achat du porteur (achat depuis son terminal habituel, adresse de livraison connue, nature de l'achat, montant, etc.) et pour un montant n'excédant pas cinq cents euros ;
 - les paiements récurrents (article 14), c'est-à-dire d'un montant et d'une périodicité fixes en faveur du même bénéficiaire, à compter de la deuxième transaction ;
 - les paiements vers un bénéficiaire de confiance (article 13), c'est-à-dire vers un bénéficiaire désigné comme étant de confiance par le payeur, cette désignation ayant elle-même fait l'objet d'une authentification forte lors de l'ajout du bénéficiaire (cette authentification forte n'a ni pour objet ni pour effet d'authentifier de manière forte les opérations de paiement ultérieurement effectuées en faveur de ce bénéficiaire) ;

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 délai¹ 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 SEPA²), 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 (prélèvements ou paiements 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.

Références : articles L. 133-19, L. 133-18, L. 133-25 et L. 133-25-1 du CMF et recueil de règles relatives au prélèvement SEPA (SEPA Direct Debit Core Scheme Rulebook V1.1 section 4.3.4).

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 réclamation, 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.

- les paiements initiés électroniquement par des processus ou protocoles de paiement sécurisés réservés à un usage entre professionnels (article 17).
- **Les paiements émis dans le cadre des mécanismes de continuité des infrastructures d'authentification**, en cas d'incident ne permettant pas de mettre en œuvre l'authentification forte du payeur, ainsi que les paiements par carte bancaire effectués durant la phase transitoire (du 14 septembre 2019 au 15 juin 2021) de déploiement de l'authentification forte.

Dans tous les cas listés ci-dessus, l'opération ne peut pas être considérée comme authentifiée de manière forte au sens de la réglementation, même si dans la plupart des cas l'absence d'authentification forte est autorisée ou tolérée.

Le prestataire de services de paiement doit être en mesure de justifier qu'une opération a été authentifiée, et doit à ce titre conserver les éléments techniques (piste d'audit) relatifs à cette authentification. Il en est de même pour la piste d'audit de l'authentification forte effectuée pour l'enrôlement d'un facteur d'authentification.

2.4.2 Paiement au moyen d'une application mobile se substituant à l'instrument de paiement

Pour réaliser des paiements par une solution mobile disposant de son propre mode d'authentification (ce qui est le cas notamment des solutions mobiles « X-Pay » proposées par les fabricants de terminaux et les éditeurs de systèmes d'exploitation), l'utilisateur doit préalablement enrôler son

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 délai¹ au remboursement du montant de cette opération.

Références : article L. 133-18 du CMF et ABE Q&A 2021_6141.

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 réclamation. Il doit également inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs, etc.).

instrument de paiement sur l'application de paiement de son terminal mobile. Cet enrôlement, considéré comme une opération sensible au sens de la réglementation, nécessite une authentification forte de la part de l'utilisateur (ABE, recueil réglementaire unique : *Single Rulebook Question and Answer – Q&A – 2021_6141*). La responsabilité de la mise en œuvre de l'authentification forte repose sur le prestataire de services de paiement, à qui il appartient de justifier du respect de cette obligation.

2.4.3 Paiement ayant fait l'objet d'une authentification forte

Comme mentionné précédemment, l'essentiel de la « zone grise » concerne les opérations contestées ayant donné lieu à une authentification forte. Le processus d'investigation des prestataires de services de paiement doit s'attacher à examiner les éléments et paramètres susceptibles d'altérer l'authentification forte de l'utilisateur.

Les **éléments d'analyse à prendre en compte** sont notamment :

- **L'existence possible d'une prise de possession du moyen d'authentification forte par une tierce partie**, en particulier en cas d'occurrence d'un ou plusieurs facteurs ci-après :
 - le transfert du moyen d'authentification forte en amont de la fraude (par exemple, enrôlement d'un nouveau mobile);
 - l'émission d'une nouvelle carte SIM par l'opérateur téléphonique dans le cas d'une solution d'authentification forte de type « SMS renforcé »;
 - la saisie des identifiants par une tierce partie ou sur un terminal n'étant pas identifié comme appartenant à l'utilisateur (cas des solutions d'authentification forte nécessitant une saisie des données d'authentification sur la page de paiement).

⁴ Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques

de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

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 (tel 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, 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 délai¹ au remboursement de la transaction ;

- soit le prestataire de services de paiement dispose de bonnes raisons de soupçonner une fraude de l'utilisateur² 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'utilisateur³, ou que ce dernier a été gravement négligent⁴ 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.

Références : articles L. 133-18, L. 133-19 et L. 133-23 du CMF.

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 réclamation. Il doit également inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs, etc.).

2 Au sens de l'article L. 133-18.

3 Au sens de l'article L. 133-6.

4 Au sens des articles L. 133-19 et L. 133-23.

- **Les paramètres de l'opération, visant à identifier dans quelle mesure l'utilisateur en est ou non à l'origine :** cette analyse est nécessaire afin de distinguer d'une part les cas de contestation qui pourraient relever d'un litige commercial plutôt que d'une fraude aux moyens de paiement (dans le cas d'un litige commercial, l'opération a été initiée par l'utilisateur), et d'autre part les cas où l'opération a manifestement été initiée par une personne distincte de l'utilisateur (l'utilisateur pouvant cependant être sollicité par le fraudeur au moment de l'authentification).
- **Les éléments relatifs au contexte de l'opération,** notamment **la qualité et l'exhaustivité des informations fournies par le prestataire de services de paiement** au moment de l'authentification de l'opération ou par des mécanismes d'alerte en temps réel, ainsi que **les éléments rapportés par l'utilisateur** (cf. recommandation n° 8).

2.5 Recommandations à l'attention des consommateurs et de leurs représentants

2.5.1 Bonnes pratiques pour la sécurité des moyens de paiement

Face à l'ingéniosité des fraudeurs qui cherchent des moyens de contournement face à des dispositifs de sécurité de plus en plus sophistiqués, les consommateurs ont, par leur comportement vigilant et responsable, un rôle clé pour préserver la sécurité de leurs propres moyens de paiement.

En particulier, en ce qui concerne leurs usages sur Internet, il leur revient de veiller à la sécurité des données associées à leurs moyens de paiement. Les utilisateurs doivent, en particulier, éviter leur divulgation à des tiers, car cette action est propice aux attaques frauduleuses. En effet, ces données sont tout aussi sensibles que le code confidentiel de leur carte de paiement. Le non-respect de ces bonnes pratiques peut constituer une négligence de l'utilisateur qui peut être retenue contre lui.

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, personnel de services 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.).

Référence : article L. 133-16 du CMF.

2.5.2 Transparence dans la déclaration des cas de fraude

La lutte contre la fraude, quel que soit le type d'opération, implique que toutes les parties prenantes, y compris les utilisateurs des moyens de paiement victimes des fraudeurs, coopèrent et fassent preuve de la plus grande transparence dans la description des faits relatifs à la fraude. La transmission d'une information exhaustive est nécessaire à bien des égards :

- l'instruction du dossier,
- l'identification des auteurs,
- la mise en œuvre de poursuites pénales à leur encontre,
- le renforcement des mécanismes de filtrage antifraude des professionnels des paiements,
- 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.

Le traitement des contestations d'opérations frauduleuses auprès des PSP comprend habituellement plusieurs niveaux de recours :

- la contestation initiale doit être adressée auprès du chargé de clientèle de l'établissement teneur de compte, qui est le point de contact privilégié de l'utilisateur, ou, selon la procédure de contestation spécialement prévue par l'établissement, sur l'espace de banque en ligne par exemple;

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 des démarches en ligne sur les plateformes Perceval ou Thésée¹ ou du dépôt de plainte au commissariat de police ou dans une unité de gendarmerie), les consommateurs et leurs représentants veillent à fournir l'ensemble des éléments dont ils disposent concernant la fraude dont ils ont été victimes.

Les utilisateurs veillent notamment à fournir tous les éléments connus sur :

- la nature et le contexte de l'opération : par exemple, leur niveau de connaissance du bénéficiaire, les procédés techniques ou manipulateurs 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 signalement ou le dépôt de plainte auprès des forces de l'ordre, etc.

¹ Perceval est le téléservice pour signaler aux forces de l'ordre les fraudes à la carte bancaire en ligne. Thésée permet de porter plainte en ligne contre des arnaques ou des escroqueries sur Internet, notamment dans le cas des fraudes aux virements.

- en cas de réponse insatisfaisante, l'utilisateur peut se tourner vers le service réclamation de son prestataire de paiement ⁵ ;
- enfin, il peut saisir le médiateur désigné par son prestataire de services de paiement.

Par ailleurs, le client peut engager une action en justice, s'il l'estime utile, à tout moment après le rejet de sa contestation initiale.

2.6 Recommandations visant à prévenir la fraude

2.6.1 Consultation des comptes du client à l'aide de la banque en ligne ou de l'application mobile

L'un des scénarios de fraude actuellement observé consiste, pour le fraudeur, à récupérer par hameçonnage l'identifiant et le mot de passe de la banque en ligne, ainsi que les informations personnelles du client (nom et prénom, numéro de téléphone, etc.).

Muni de ces informations, le fraudeur se connecte à l'espace de banque en ligne du client pour réunir des informations sur les produits détenus par le client et la situation des comptes (solde, dernières opérations effectuées, etc.). Ainsi, le fraudeur peut contacter le client en usurpant l'identité du prestataire de services de paiement, cette usurpation étant rendue crédible par la détention d'informations bancaires précises le concernant et qu'un tiers n'est pas censé connaître. Mis en confiance, le client victime de la fraude sera incité à accéder à la demande du fraudeur de valider des opérations (ajout de bénéficiaire, ordres de virement, etc.) par authentification forte.

Ce scénario de fraude peut être évité par la mise en place de l'authentification forte à chaque consultation de la

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 ou un point d'accès à Internet qui n'a pas été précédemment utilisé par le client.

banque en ligne, sauf si la consultation se fait à partir d'un terminal régulièrement utilisé par l'utilisateur et que la dernière connexion avec authentification forte date de moins de 180 jours.

2.6.2 Information délivrée au client lors de l'ajout d'un bénéficiaire de virement

La réglementation actuelle en matière de sécurité des paiements ne prévoit pas de contrôle systématique sur le nom du bénéficiaire d'un virement : un ordre de virement peut être exécuté dès lors que l'IBAN ⁶ bénéficiaire est valide, que le compte bénéficiaire existe et n'a pas été clos, indépendamment de la concordance entre le nom du bénéficiaire fourni par le payeur et le nom du titulaire réel du compte.

Cette situation est exploitée par certains fraudeurs, notamment dans le cadre du scénario dit de « substitution d'IBAN » : le fraudeur transmet l'IBAN d'un compte dont il est titulaire (ou dont le titulaire est complice de la fraude) en l'associant à l'intitulé d'un bénéficiaire de confiance (par exemple, le Trésor public ou un notaire).

Or, lors de l'ajout d'un bénéficiaire, l'émetteur du virement est invité à saisir le nom du bénéficiaire. Une étape de « validation de l'IBAN », nécessitant un délai pouvant atteindre plusieurs jours, est même annoncée sur l'espace de banque en ligne et l'application mobile de certains établissements. L'émetteur du virement peut ainsi présumer, à tort, de l'existence d'un contrôle de concordance, et que

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 IBAN et nom du bénéficiaire a été mis en œuvre. À défaut, il doit être précisé à l'utilisateur que le champ « nom du bénéficiaire » est exclusivement destiné à faciliter le suivi des opérations par le client qui émet des virements, et que son contenu ne fait l'objet d'aucun contrôle de concordance avec l'identité du titulaire de l'IBAN du bénéficiaire.

Par ailleurs, les prestataires de services de paiement établis en France sont encouragés à explorer par anticipation la possibilité d'implémenter au plus tôt un service de confirmation du bénéficiaire comme envisagé par la Commission européenne dans sa proposition de révision du règlement SEPA.

le virement ne sera pas exécuté ou pourra être annulé par le payeur dans le cas où le véritable titulaire du compte bénéficiaire ne correspond pas au nom saisi lors de l'ajout de l'IBAN de ce compte.

Cette situation devrait toutefois évoluer au cours des prochaines années. En effet, dans sa proposition de révision du règlement SEPA⁷, la Commission européenne prévoit notamment de renforcer la confiance dans les paiements instantanés avec l'obligation pour les prestataires de vérifier la concordance entre l'IBAN et le nom du bénéficiaire fournis par le payeur afin d'alerter celui-ci d'une éventuelle erreur ou fraude avant que le paiement ne soit effectué.

2.6.3 Information et options présentées à l'utilisateur du service de paiement au moment de l'authentification forte

Dans le cas de fraude par manipulation, le fraudeur s'appuie sur l'emprise qu'il exerce sur sa victime pour l'amener à passer outre l'ensemble des messages et alertes adressés par le prestataire de services de paiement. Cette manipulation est facilitée lorsque ces messages et alertes sont insuffisamment précis et exhaustifs sur la nature et les caractéristiques de l'opération en attente de validation. Le renforcement du caractère explicite et de l'exhaustivité de l'information présentée, mais aussi du choix donné à l'utilisateur durant son parcours d'authentification, constituent des mesures efficaces de prévention de la fraude par manipulation.

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. Elle doit notamment mentionner i) le montant, ii) le bénéficiaire, iii) le caractère unique ou récurrent de l'opération, iv) la périodicité dans le cas d'une opération récurrente ainsi que v) 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.

2.6.4 Simplicité d'accès aux procédures de blocage des instruments de paiement

Dans le cas où l'utilisateur détecte une activité anormale sur ses comptes ou instruments de paiement, ou identifie une faille dans la protection de ses données, il doit pouvoir mettre en opposition les instruments de paiement concernés auprès de son prestataire de services de paiement. Cette procédure doit être simple d'accès afin d'assurer la meilleure réactivité possible, à l'instar du centre de mise en opposition qui existe aujourd'hui pour les cartes de paiement.

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.

Références : articles L. 133-15 et L. 133-17 du CMF.

2.6.5 Rôle des fournisseurs de services et technologies de l'information dans la lutte contre la fraude

Les opérateurs de téléphonie et les fournisseurs de services numériques sont des parties prenantes centrales dans la sécurité des opérations de paiement effectuées à distance, pour lesquelles ils assurent la mise en relation entre les différentes parties et l'échange de données. Ils ont ainsi une responsabilité dans la lutte contre les techniques utilisées par les fraudeurs pour collecter des données de paiement à l'insu de l'utilisateur. Les techniques sont variées : par des messages électroniques (hameçonnage) ou SMS (*smishing*), usurpant l'identité d'un expéditeur légitime, la mise en ligne de faux sites miroirs, ou encore l'affichage, lors d'un appel entrant malveillant, du numéro de téléphone d'un interlocuteur légitime (*spoofing*).

5 Si l'utilisateur engage une réclamation sur la décision finale du prestataire de services de paiement à la suite de sa contestation, la recommandation 2022-R-01 du 9 mai 2022 de l'ACPR sur le traitement des réclamations serait alors pleinement applicable. Celle-ci complète les présentes recommandations. Cf. <https://acpr.banque-france.fr/>

6 IBAN – international bank account number.

7 Proposition du 26 octobre 2022 – 2022/0341 (COD) – visant à rendre les paiements instantanés en euros accessibles à tous les particuliers et à toutes les entreprises qui possèdent un compte bancaire dans l'Union européenne ou dans un pays de l'Espace économique européen (EEE).

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 contenu, éditeurs de sites de référencement, moteurs de recherche, fournisseurs de services de messagerie, etc.) veillent à protéger les utilisateurs contre les risques d'usurpation d'identité et d'atteinte à l'intégrité et la confidentialité de leurs données. Ils œuvrent à empêcher l'utilisation de techniques frauduleuses telles que l'hameçonnage, le *spoofing* ou le *SIM-swapping*.

2.7 Conditions d'application des recommandations

Les treize recommandations de l'Observatoire constituent des pratiques de référence pour les acteurs du marché des paiements. Elles précisent les attentes des autorités françaises au regard de la réglementation européenne. Elles n'ont pas vocation à se substituer à la réglementation applicable, ni à la jurisprudence en la matière.

Les prestataires de services de paiement s'engagent à prendre en considération les recommandations n° 1 à 6 dans leurs pratiques en matière de traitement des contestations d'opérations de paiement non autorisées. L'ensemble des acteurs, quant à eux, s'engagent à jouer un rôle proactif dans la sécurité des paiements en veillant à appliquer les recommandations n° 7 à 13, pour celles qui les concernent, dans la gestion de leurs activités au quotidien.

Dans un contexte où les mécanismes de fraude évoluent rapidement, l'Observatoire s'engage à procéder à un bilan de ces recommandations et, le cas échéant, à leur révision sous un délai maximal de 18 mois à compter de leur adoption.

LES SOLUTIONS D'ACCEPTATION DE PAIEMENT SUR SMARTPHONE OU TABLETTE

3.1 Introduction

Dans son rapport annuel 2016, l'Observatoire avait réalisé une étude¹ 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*). Ce dernier est un boîtier qui permet la lecture de la puce en se connectant à un *smartphone* (ou une tablette), soit en filaire, soit en utilisant la technologie sans fil Bluetooth.

Le *smartphone* ou la tablette se révélait être le maillon faible dans la sécurité de la solution de paiement en mobilité. En effet, en 2016, les technologies embarquées dans le *smartphone* ne proposaient pas de mécanismes de sécurité permettant de garantir la confidentialité. De plus, l'intégrité des données des transactions de paiement par carte et les cadres de sécurité étaient absents. Dans ce contexte, les acteurs de marché se sont plutôt orientés vers les terminaux m-POS. Cette solution permettait alors de répondre aux exigences de sécurité, en maintenant un dispositif de lecture physique de la carte à puce dans un boîtier dédié distinct du *smartphone* ou de la tablette. Le développement des terminaux m-POS est toutefois resté marginal et représente en 2022 moins de 1 % du parc de terminaux déployés en France.

Depuis 2016, le Conseil des normes de sécurité de l'industrie des cartes de paiement (*Payment card industry Security standards council* – PCI SSC) a publié deux nouvelles normes :

- SPoC (*Software-based PIN entry on COTS*), relative à la sécurisation des saisies de code PIN à partir d'un appareil commercial prêt à l'emploi (*commercial off-the-shelf* – COTS) tel que le *smartphone* ou la tablette ;
- CPoC (*Contactless Payments on COTS*), relative à la sécurisation des seuls paiements en mode sans contact sur un COTS.

Une troisième norme, MPoC (*Mobile Payments on COTS*), publiée en novembre 2022, devrait permettre un développement plus important des solutions d'acceptation de paiement par carte sur *smartphone* ou tablette.

En parallèle de ce travail de normalisation, les réseaux de paiement par carte ont mis en place leurs propres processus de certification pour permettre aux acquéreurs de conduire des expérimentations à petite échelle auprès de quelques commerçants. L'Observatoire note à cette occasion que ces solutions d'acceptation sur *smartphone* ou tablette sont à la fois proposées par des acteurs historiques de la monétique, parfois par le biais d'acquisitions de jeunes pousses spécialisées, et des acteurs technologiques issus du secteur du mobile.

Les évolutions rapides du marché invitent l'Observatoire à étudier de nouveau la sécurité des solutions de paiement en mobilité et plus précisément 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 les perçoit en effet comme des alternatives aux terminaux de paiement électroniques (TPE) traditionnels pour l'acceptation des paiements par carte, mais aussi comme des solutions foncièrement différentes puisqu'elles sont entièrement basées sur du logiciel.

¹ Cf. <https://www.banque-france.fr/>

Selon ses promoteurs, les solutions SoftPOS seraient notamment intéressantes pour les professionnels et commerçants qui ont besoin de solutions de paiement basiques et accessibles, comme les très petites entreprises ainsi que les entrepreneurs mobiles (services de livraison, vendeurs sur les marchés, commerces éphémères ou ambulants, facteurs, etc.). Ces solutions pourraient intéresser également des commerces plus sédentaires, aujourd'hui déjà équipés de TPE traditionnels, pour des raisons de coûts ou d'innovation. Dans tous les cas, le déploiement des solutions SoftPOS constituerait un changement de paradigme pour les paiements par carte de proximité, puisque le code PIN ne serait plus contrôlé en local à travers la lecture de la puce, mais transmis et contrôlé par les serveurs de l'établissement bancaire émetteur. Le déploiement des solutions de SoftPOS présuppose donc une généralisation de la fonctionnalité dite « *PIN Online* »² et reste incompatible dans les environnements déconnectés (« zone blanche », souterrains, etc.).

Les solutions SoftPOS sont donc autant des alternatives que des concurrents aux TPE traditionnels, qui ont pourtant démontré depuis de nombreuses années leur robustesse et leur sécurité, avec un niveau de fraude très bas sur les paiements par carte de proximité et un très faible nombre de cas de compromission. **Il appartient donc à l'Observatoire d'évaluer si les solutions SoftPOS peuvent garantir un haut niveau de sécurité sur les paiements par carte de proximité et, le cas échéant, identifier les conditions pour y parvenir.**

Outre le défi de sécurité lié à l'usage d'un *smartphone* grand public comme terminal de paiement, l'Observatoire note que les solutions SoftPOS font face à deux autres défis :

- d'une part, un défi d'acculturation pour établir la confiance des consommateurs et des commerçants sur ces nouvelles solutions, tant les utilisateurs ont l'habitude de saisir leur code PIN sur des terminaux dédiés à l'acceptation ;
- d'autre part, un défi d'accessibilité pour que ces solutions puissent être utilisées par les personnes en situation de handicap, conformément aux engagements pris par la Place française dans la cadre de la charte du Comité national des moyens de paiement et à la directive européenne en matière d'accessibilité³ qui entrera en application le 28 juin 2025 pour les nouveaux produits et services.

3.2 Panorama des solutions actuelles

Toutes les solutions de paiement en mobilité présentées dans ce chapitre impliquant des terminaux de paiement traditionnels possèdent en principe le même niveau de

sécurité. La sécurité des mécanismes de saisie du code PIN, de chiffrement des données et des composants électroniques est en effet certifiée par des laboratoires de certification agréés par EMVCo, consortium en charge de la gestion et du développement des spécifications EMV⁴. Toutefois, leurs caractéristiques techniques et fonctionnelles varient pour répondre aux besoins de mobilité de chaque commerçant.

3.2.1 Terminal de paiement portable



Le terminal de paiement portable est généralement connecté par un système sans fil, Bluetooth, Wi-Fi ou infrarouge, à une base fixe qui se trouve à l'emplacement du point de vente.

Ces terminaux de paiement portables sont conçus pour être utilisés dans les points de vente d'un magasin ou les restaurants. Ils ne fonctionnent que lorsqu'ils sont proches de la station (rayon de dix à trente mètres) qui dispose d'une connexion vers les serveurs d'acceptation.

3.2.2 Terminal de paiement autonome et mobile



Le terminal de paiement autonome et mobile fonctionne sans fil, sur batterie et n'a pas besoin de se connecter à une base. Ils fonctionnent en utilisant la connectivité mobile GPRS,

4G ou 5G pour communiquer avec le serveur d'acceptation. Il faut une carte SIM monétique pour utiliser l'appareil. Certaines cartes SIM sont capables de détecter le meilleur opérateur disponible en fonction de la localisation et ce, même à l'étranger. Il existe également des modèles compatibles avec le Bluetooth ou le Wi-Fi.

3.2.3 Terminal de paiement (TPE) Android



C'est un terminal de paiement dont le système d'exploitation utilisé est Android. Un TPE Android est avant tout un terminal de paiement classique, avec un lecteur de carte et un module d'acceptation des paiements sans contact. Mais

contrairement aux terminaux de paiement traditionnels, les TPE Android permettent d'accéder à d'autres applications

développées sous Android et ainsi enrichir les actions possibles avec le TPE (logiciel de caisse, logiciel de relation client, paiement par QR code, gestion d'un programme de fidélité, etc.). Dans la plupart des cas, les applications tierces sont disponibles dans le cadre de magasins d'applications privés (*stores*), qui sont fournis par les industriels de l'acceptation monétique. Du côté de la connectivité, ils fonctionnent souvent grâce à une connexion sans fil 4G ou Wi-Fi, permettant une utilisation même en cas de perte de réseau. Ils sont aussi plus puissants puisqu'ils disposent en général de plus de mémoire vive. Les TPE Android sont soumis aux mêmes réglementations et normes de sécurité que les TPE traditionnels.

3.2.4 Terminal de paiement mobile m-POS



La solution de paiement mobile fondée sur la technologie m-POS repose sur deux éléments distincts et connectés. Le premier élément est un lecteur de cartes à puce, et parfois de cartes à piste magnétique, certifié EMV, fonctionnant sur batterie. Celui-ci se connecte soit par l'intermédiaire d'un câble, soit par Bluetooth, à l'appareil mobile (deuxième élément), généralement un *smartphone*, qui héberge l'application de paiement.

3.2.5 Terminal de paiement SoftPOS



La solution de paiement mobile fondée sur la technologie SoftPOS ne nécessite aucun matériel autre qu'un appareil mobile, *smartphone* ou tablette, doté d'un composant NFC. Les spécialistes de l'informatique parlent d'appareil COTS (*commercial off-the-shelf*), c'est-à-dire un appareil mobile standard fabriqué en série disponible dans le commerce⁵. Toutes les transactions sont effectuées directement à partir de l'appareil mobile du commerçant par le biais d'une application dotée de toutes les certifications de sécurité EMV nécessaires. Jusqu'en 2022, en l'absence de la spécification MPoC et de programme de certification associé, les solutions pilotes SoftPOS en cours permettant les paiements avec saisie du code PIN étaient certifiées par des programmes spécifiques mis en place par les réseaux de paiement par carte (CB, Visa, Mastercard, etc.).

3.3 Les risques

Jusqu'à présent, les terminaux de paiement électroniques sur les points de vente se limitaient à des équipements matériels, entièrement dédiés à l'acceptation et au traitement des transactions. Conçus et fabriqués pour garantir la sécurité des informations, ceux-ci sont tributaires de la sécurité matérielle fournie par leurs fabricants. Ces terminaux sont également dépendants en matière de maintenance, effectuée par son titulaire, souvent par le biais de sociétés spécialisées dans la gestion de parc de terminaux. Au fil du temps, les terminaux de paiement ont évolué vers des systèmes d'exploitation Android, et l'ensemble des points de vulnérabilité (surface d'attaque), jusqu'alors essentiellement matériel, s'est étendu aux logiciels et aux équipements mobiles. La technologie SoftPOS parachève cette évolution, puisqu'elle marque la transition entre des solutions matérielles sécurisées et des applications mobiles, purement logicielles, installées sur des équipements grand public.

Les solutions SoftPOS, s'exécutant sur divers modèles de *smartphones*, aux composants matériels et logiciels sous-jacents différents, leur sécurité diffère fondamentalement de celle des TPE traditionnels. En effet, un terminal de paiement traditionnel est réputé « digne de confiance » grâce aux certifications obtenues lors de sa mise sur le marché, aux contrôles et aux maintenances réalisés tout au long de son cycle de vie. À l'inverse, le *smartphone* est un appareil grand public non dédié, qui reste très souvent la cible des cybercriminels et qui est par conséquent perçu, à tort ou à raison, comme « peu fiable ».

2 Le *PIN Online* est une fonctionnalité qui consiste à déporter la vérification du code PIN vers les serveurs de l'établissement émetteur. Cela permet par exemple des usages où le consommateur n'insère plus la carte dans le terminal, mais appose sa carte comme pour un paiement sans contact et tape son code PIN sur le terminal. La vérification du code PIN ne se fait plus par lecture de la puce mais par les serveurs sécurisés de l'établissement bancaire émetteur de la carte.

3 Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services. Cette directive a été transposée pour sa partie législative par la loi n° 2023-171

du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture.

4 EMV (Europay Mastercard Visa) se présente comme une technologie de paiement et un standard mondial de sécurité dont dispose la puce d'une carte bancaire. Il s'agit d'un ensemble de normes qui garantissent la compatibilité des terminaux de paiement et des cartes à puce.

5 Il est toutefois possible que des applications SoftPOS soient déployées sur des appareils mobiles non COTS, c'est-à-dire des appareils développés et fabriqués pour les besoins des professionnels.

Pour assurer leur sécurité et limiter la fraude, les solutions SoftPOS doivent résister à l'ensemble des attaques possibles sur un *smartphone* (cf. encadré 2), notamment aux *malwares*, aux organisations criminelles, aux pirates distants et acteurs malveillants qui chercheraient à accéder et compromettre l'application SoftPOS. Si celle-ci n'est pas correctement protégée, les solutions qu'elle propose peuvent être détournées et exploitées de manière abusive (faux paiements, transactions non autorisées côté commerçants, collecte des données de cartes bancaires, blocage des comptes des commerçants, etc.).

En pratique, la fragmentation des technologies matérielles dans les *smartphones* a conduit la plupart des fournisseurs de solutions SoftPOS à embarquer dans leurs applications les mécanismes de sécurité à même de couvrir un nombre étendu de marques et de modèles de *smartphones*.

3.4 Les standards de sécurité

Depuis 2016, les professionnels du secteur des paiements ont travaillé à l'élaboration ou la mise à jour de normes de sécurité pour assurer la sécurité technique des solutions d'acceptation des paiements par carte sur *smartphone* ou tablette. L'Observatoire accueille avec intérêt ces vecteurs de standardisation et de contrôle et appelle l'ensemble des acteurs de l'acceptation de paiement (commerçants, gestionnaires de parc de terminaux et acquéreurs) à contrôler rigoureusement le niveau de certification des solutions avant de les déployer, distribuer ou accepter.

3.4.1 EMV Level 2

EMV définit les standards qui permettent d'accepter, de manière sécurisée, les paiements par carte à puce. Ils sont implémentés dans l'ensemble du parc des terminaux de paiement et des cartes bancaires en circulation en France. Plus précisément, les spécifications EMV décrivent le « protocole » ou les éléments nécessaires pour que la carte à puce communique avec un lecteur de carte à puce dans un terminal d'acceptation et échange des informations pour exécuter un paiement. Pour les paiements par contact, la puce doit entrer en contact physique avec le lecteur de puce pour que la transaction de paiement ait lieu. En sans contact, la puce doit se trouver à une distance suffisante du lecteur (4 cm maximum) pour que l'information circule entre la puce et le terminal de paiement.

Tous les produits acceptant des paiements par carte à puce doivent obtenir les certifications EMV nécessaires avant d'être mis sur le marché. Un terminal de paiement

doit obtenir les certifications EMV Level 1 (niveau 1), qui attestent la conformité du lecteur de carte à puce par rapport au protocole de communication (interfaces mécaniques, électriques et de niveau transport), et EMV Level 2 (niveau 2), qui attestent la conformité du logiciel d'acceptation (appelé le *kernel*, noyau) par rapport aux spécifications de la puce EMV et aux spécifications des fonctions qui réalisent les paiements EMV.

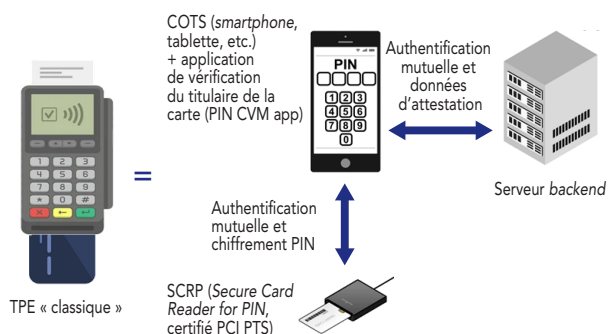
Les tests de certification relatifs aux lecteurs de cartes bancaires (EMV Level 1) sont incompatibles avec le paiement par *smartphone* et ne sont donc pas réalisés. En revanche, l'ensemble des autres tests de certification à destination des TPE (EMV Level 2) est appliqué aux solutions SoftPOS.

Les tests de certification EMV Level 2, quant à eux, n'attestent que la conformité des fonctions de traitement EMV implémentées dans les logiciels d'acceptation, que celles-ci soient embarquées dans un terminal dédié ou un *smartphone*. Il est absolument nécessaire de les compléter avec les certifications PCI présentées ci-après qui valideront les mécanismes de protection des données de paiement de bout en bout depuis le logiciel d'acceptation jusqu'au serveur *backend*.

3.4.2 PCI Software-Based PIN entry on COTS (PCI SPoC) – 2018

PCI SPoC est une norme de sécurité qui définit les exigences permettant de sécuriser l'authentification des transactions à l'aide d'une vérification logicielle du code PIN sur les appareils commerciaux prêts à l'emploi (COTS), par exemple un *smartphone* ou une tablette. Toutefois, la saisie du code PIN nécessite obligatoirement l'usage d'un élément matériel supplémentaire, conforme à la norme *PCI PIN Transaction Security* (PCI PTS), approuvé par PCI pour l'authentification du code PIN (PCI PTS POI[®]) et connecté à l'appareil mobile, en filaire ou par Bluetooth.

Anatomie d'une solution PCI SPoC (Software-based PIN Entry on COTS)



Source : Observatoire de la sécurité des moyens de paiement.

PCI SPoC définit un certain nombre de composants et de processus pour authentifier les transactions à l'aide d'un code PIN saisi sur *smartphone* ou tablette. Au minimum, le système se compose d'un lecteur de carte EMV⁷ (appelé *Secure Card Reader for PIN – SCR*), d'un système dorsal de traitement et de surveillance des paiements (serveur *backend*), et d'une application PIN CVM (*PIN Cardholder Verification Method*) qui accepte le PIN du titulaire de la carte.

Lors d'un paiement avec une solution certifiée PCI SPoC, le consommateur insère sa carte dans le lecteur de carte sécurisé pour code PIN (SCR) qui lit les informations de compte, puis il saisit son code PIN sur l'écran du *smartphone* ou de la tablette du commerçant pour authentifier la transaction. Les informations du code PIN sur l'appareil mobile sont capturées par une application mobile PIN CVM conforme à la norme PCI qui échange ces informations avec le SCR par le biais d'une communication sécurisée. Enfin, le SCR établit une communication sécurisée avec l'appareil mobile et le système de surveillance *backend* pour attester et traiter la transaction.

Le principal avantage de PCI SPoC est l'isolement des informations du code PIN des autres données de compte, ce qui empêche les attaques par corrélation⁸. Ainsi, PCI SPoC garantit l'intégrité de l'application de saisie du code PIN. En complément, PCI SPoC nécessite un service de surveillance actif pour appliquer des contrôles de sécurité supplémentaires pour :

- l'attestation (garantissant que les mécanismes de sécurité sont intacts et opérationnels),
- la détection (notification de la présence d'anomalies),
- et la riposte (déclenchement des commandes pour alerter et agir).

3.4.3 PCI Contactless Payments on COTS (PCI CPoC) – 2019

PCI CPoC fournit un ensemble de principes et d'exigences pour construire une solution d'acceptation de paiement sans contact mobile. La carte est lue à l'aide de l'interface NFC intégrée à un appareil commercial prêt à l'emploi (COTS), par exemple un *smartphone* ou une tablette. Dans ce schéma type, contrairement au SPoC, il n'existe pas de lecteur de carte PIN (SCR). Par conséquent, la norme n'autorise pas les transactions nécessitant la saisie de code PIN. Le cas d'usage est uniquement limité aux paiements sans contact et sans saisie de code PIN, ce qui couvre à la fois les paiements par carte sans contact en dessous des plafonds réglementaires (maximum de cinquante euros par transaction) et les paiements par carte sans contact

Anatomie d'une solution PCI CPoC (Contactless Payments on COTS)



TPE « classique »
en mode sans contact uniquement

Source : Observatoire de la sécurité des moyens de paiement.

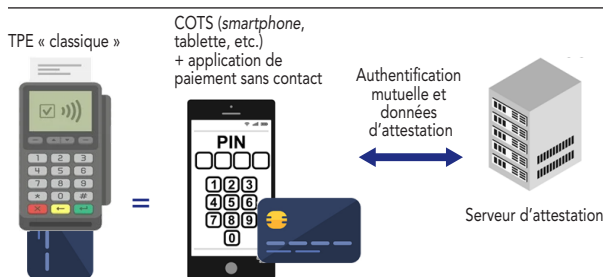
au moyen d'un portefeuille mobile (l'authentification du porteur se faisant alors directement sur son téléphone).

Les principaux éléments d'une solution conforme à PCI CPoC comprennent i) un appareil COTS avec une interface NFC intégrée dans l'appareil COTS pour lire la carte de paiement, ii) une application logicielle d'acceptation de paiement certifiée qui s'exécute sur le dispositif COTS du commerçant et iii) des systèmes dorsaux indépendants du dispositif COTS (serveur *backend*) prenant en charge la surveillance, les contrôles d'intégrité et le traitement des paiements.

3.4.4 PCI Mobile Payments on COTS (PCI MPoC) – 2022

L'intérêt grandissant des commerçants pour les solutions SPoC et CPoC et le développement des solutions conformes à ces normes se heurtent à l'obligation de saisir le code PIN lorsque le montant de la transaction dépasse cinquante

Anatomie d'une solution PCI MPoC (Mobile Payments on COTS)



Source : Observatoire de la sécurité des moyens de paiement.

6 Point of Interaction – POI.

7 Europay Mastercard Visa, abrégé par le sigle EMV, est le standard international de sécurité des cartes de paiement (cartes à puce) depuis 1995.

8 Une attaque par corrélation est une méthode de cryptanalyse utilisée contre le chiffement par flot (aussi appelé chiffement en continu),

qui est l'une des deux grandes catégories de chiffement modernes en cryptographie symétrique. Le chiffement par lot utilisant des générateurs pseudo-aléatoires, il est possible d'exploiter l'existence d'une éventuelle corrélation entre la sortie du générateur pseudo-aléatoire et celle d'un des registres utilisés pour déchiffrer les données.

euros ou que l'utilisation du sans contact en opérations successives dépasse les plafonds fixés par la banque du porteur en conformité avec la réglementation européenne.

Pour y répondre, le PCI SSC a publié en novembre 2022 une nouvelle norme, le PCI MPoC (*Mobile Payments on COTS*).

La norme PCI MPoC adopte un nouveau paradigme, l'architecture modulaire, pour offrir une plus grande flexibilité aux fournisseurs d'applications SoftPOS. Ce processus doit permettre de couvrir davantage de cas d'usage et d'intégrer différents types d'appareil et de composant tout en reprenant les principes qui ont structuré les normes PCI SPoC et PCI CPoC.

Tandis que les normes PCI SPoC et PCI CPoC définissent un ensemble d'exigences qu'une solution doit satisfaire, PCI MPoC définit en premier lieu des objectifs à atteindre pour les décliner ensuite sous forme d'exigences. Cette démarche transforme l'approche de sécurité qui passe d'une simple mise en conformité à une véritable assurance sécurité, qui responsabilise le fournisseur sur les résultats davantage que sur les moyens.

3.4.5 La certification des solutions SoftPOS

La confiance dans une solution d'acceptation repose sur un haut niveau de sécurité garanti par le contrôle réalisé par un laboratoire de certification sur la base d'un cadre d'exigences de sécurité.

Dans un contexte où les parcours de certification MPoC ne sont pas encore disponibles, la certification des solutions SoftPOS repose sur les cadres d'exigences de sécurité proposés par les réseaux de paiement principaux tels que Visa, Mastercard et le Groupement des cartes bancaires (abrégié CB). Ces programmes de certification sont spécifiques à chacun des réseaux de paiement. Néanmoins, certains réseaux comme Visa et Mastercard se sont accordés sur un format standardisé du rapport de conformité produit par les laboratoires de test. De son côté, CB a collaboré avec un laboratoire d'évaluation reconnu pour concevoir un cadre, permettant à la fois d'obtenir un bon niveau d'assurance de sécurité et de ne faire qu'une seule évaluation compatible avec les exigences des différents schémas de paiement (chaque schéma disposant de ses exigences propres et validant son propre rapport).

Ces cadres d'exigences de sécurité permettent d'obtenir l'assurance d'un niveau minimum de sécurité pour la mise en œuvre de programmes pilotes et de prédeployements, en vue d'un agrément futur de ces solutions. Ils seront mis à jour pour s'aligner avec le cadre d'exigences PCI MPoC et seront utilisés pour l'évaluation des futures solutions SoftPOS.

3.5 La sécurité technique des solutions SoftPOS

La sécurisation des solutions SoftPOS est étroitement liée aux mécanismes de sécurité disponibles dans le système d'exploitation déployé sur chaque équipement mobile ainsi qu'aux choix des fournisseurs quant à l'usage ou non des composants matériels de sécurité additionnels inclus dans le *smartphone* ou la tablette. Jusqu'au début de l'année 2022, tous les fournisseurs de solutions SoftPOS ont privilégié le système d'exploitation Android en raison de l'accès autorisé au composant NFC intégré dans l'équipement mobile. Ce composant est indispensable au fonctionnement de la technologie SoftPOS. Depuis, Apple, fournisseur unique du système d'exploitation iOS, invite les fournisseurs à rendre leurs solutions SoftPOS compatibles avec iOS en intégrant leur kit de développement logiciel propriétaire appelé « SoftPOS SDK » (*SoftPOS Software Development Kit*, kit de développement logiciel).

3.5.1 Sécurité à la conception

S'affranchir de l'environnement physique et logique des terminaux de paiement électronique certifiés EMV et PCI représente un grand défi dans la conception des applications SoftPOS.

Il existe deux types d'environnement sur lesquels seront déployées les applications de paiement SoftPOS :

- Un modèle d'appareil mobile grand public dont le système d'exploitation est administré et dont les applications installées, y compris l'application SoftPOS, proviennent d'un magasin d'applications privé. Dans ce contexte, les mises à jour du système d'exploitation et des applications sont contrôlées et appliquées selon les règles définies par une équipe en charge de la gestion de ces appareils. C'est généralement le cas des grands commerçants, où la gestion des terminaux est confiée à une équipe dédiée ou externalisée auprès d'une société spécialisée dans l'équipement monétique.
- Un modèle d'appareil mobile grand public d'un commerçant ou professionnel de plus petite taille (petites et moyennes entreprises, indépendants, itinérants, etc.). Des applications mobiles en provenance de magasins d'applications publics y sont déployées, l'application de paiement SoftPOS n'est qu'une application parmi d'autres, et les mises à jour de sécurité ne sont pas appliquées systématiquement. Le *smartphone* peut alors également servir à des fins privées, si le professionnel ne se sert que d'un appareil pour sa vie personnelle et professionnelle.

Pour couvrir ces deux environnements, les fournisseurs de solutions SoftPOS doivent intégrer la sécurité dès la conception de leurs produits, directement dans le code source de leurs applications mobiles, afin de réduire la surface d'attaque, de ne pas laisser de failles ou d'accès interdits.

3.5.2 Environnement d'exécution de confiance – *Trusted Execution Environment (TEE)*

Le TEE est un espace sécurisé par des dispositifs matériels et logiciels qui est inclus dans le microprocesseur du téléphone. Il ne fournit que des services relatifs à la sécurité et dispose de son propre environnement d'exécution indépendant du système d'exploitation. Plusieurs implémentations de TEE existent sur le marché, mais elles obéissent toutes à ce même concept. Les applications communes sont quant à elles exécutées dans le système d'exploitation du *smartphone*, par exemple Android.

Le rôle d'un TEE est plus précisément de protéger les données (clés cryptographiques, mots de passe, et données bancaires telles des identifiants de carte, de compte de paiement, etc.) et les applications des attaques internes et externes au téléphone, comme les *malwares*, en garantissant leur séparation du reste de l'environnement du téléphone, ainsi qu'un accès sous contrôle. De par ses caractéristiques, le TEE est donc particulièrement adapté aux usages bancaires et notamment aux applications sensibles de paiement par mobile. Le TEE peut notamment assurer la sécurité du PIN si le clavier virtuel est exécuté dans le TEE.

3.5.3 Cloud kernels

Le *kernel* EMV est au cœur des paiements par carte en point de vente avec ou sans contact. C'est un composant logiciel qui communique avec la carte de paiement par l'intermédiaire du lecteur de carte physique ou l'interface NFC afin de réaliser l'authentification de la carte de paiement, la vérification du porteur et les opérations de gestion du risque.

Traditionnellement, dans le cadre des solutions SoftPOS, le *kernel* EMV est embarqué dans le composant appelé élément de sécurité (*Secure Element – SE*) du *smartphone*. Le lien étroit entre le *kernel* et l'élément de sécurité complexifie les opérations de maintenance telles que la mise à jour du *kernel* ou de ses paramètres.

C'est pourquoi il existe *kernels* EMV déployés dans des serveurs à distance ou *cloud* (*cloud kernel*).

Cette technologie nécessite une connexion à Internet sans laquelle envoyer les données des transactions vers le *cloud kernel* pour traitement n'est plus possible. Toutefois, elle permet de contourner le lien entre le *kernel* et l'élément de sécurité en simplifiant par la même occasion les opérations de maintenance. Cela permet aussi de couvrir plusieurs équipements mobiles avec leurs différents systèmes d'exploitation, dès lors qu'ils dépendent tous d'un seul service de *cloud kernel*. En matière de garantie du niveau de sécurité, les *cloud kernels* peuvent obtenir une certification EMV *Level 2* par le programme de certification mis en place par EMVCo. Les tests de certification pour les *cloud kernels* sont identiques aux *kernels Level 2* embarqués. Enfin, certains fournisseurs proposent de déployer les *cloud kernels* dans des environnements certifiés PCI-DSS⁹ dans lesquels il est possible d'enregistrer toutes les données EMV et les commandes ADPU¹⁰ dans une base de données utilisée pour la surveillance à des fins de lutte contre la fraude.

3.6 Les recommandations de l'Observatoire

À l'attention des fournisseurs de solutions d'acceptation sur *smartphone* ou tablette (développeurs, acquéreurs ou sociétés spécialisées dans l'acceptation monétique)

- Obtenir les certifications techniques nécessaires avant l'expérimentation ou le lancement commercial d'une solution d'acceptation SoftPOS.
- Choisir très attentivement 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 est à l'heure actuelle inaccessible. En effet, il est un moyen de paiement plus sûr que d'autres plus exposés à la fraude, comme le chèque.
- Mettre en place un programme d'actions et de contrôles destiné à assurer la sécurité dans le temps de ces équipements (contrôle des applications tierces installées, mises à jour forcées du système d'exploitation, etc.).

.../...

⁹ La norme de sécurité de l'industrie des cartes de paiement PCI DSS (*Payment Card Industry Data Security Standard*) représente le standard de référence de sécurité des données. L'objectif de cette norme est de protéger les données sensibles des porteurs de cartes de paiement. Elle comporte des objectifs de contrôle pour garantir la bonne protection des données du titulaire.

¹⁰ L'Unité de données de protocole d'application APDU (*Application Protocol Data Unit*) est un format normalisé par l'ISO 7816-4 qui permet de structurer les commandes échangées entre les périphériques NFC. Il est utilisé pour envoyer des commandes et en recevoir les réponses.

- Accompagner et former activement les commerçants utilisateurs d'applications SoftPOS aux enjeux de sécurité associés à ces équipements.
- 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.

À l'attention des commerçants utilisateurs d'une application SoftPOS

- 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 : garder les équipements sous contrôle visuel, les mettre en sécurité quand le magasin est fermé et les contrôler régulièrement et leur apposer des signes distinctifs.
- Appliquer les principes de sécurité applicables à tout *smartphone* : mettre à jour régulièrement le système d'exploitation contre les vulnérabilités, vérifier la fiabilité des applications tierces installées en n'autorisant que les applications provenant de magasins d'applications fiables (*stores*), etc.
- 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.

À l'attention des consommateurs amenés à payer sur des applications SoftPOS

- 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.
- 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).

Cela étant, le déploiement d'application SoftPOS à large échelle constituerait un changement de paradigme majeur dans la sécurité des paiements par carte de proximité :

- en augmentant la diffusion et la circulation des données sensibles de paiement par carte, qui seraient traitées par un nombre croissant d'équipements, de serveurs et d'acteurs, ce qui augmente la surface potentielle d'attaque ;
- en reportant de plus en plus la sécurité des paiements par carte sur des équipements matériels ou logiciels qui ne sont pas dans le champ de contrôle direct des professionnels des paiements ;
- en responsabilisant encore plus fortement le commerçant sur la sécurité de son équipement d'acceptation.

L'Observatoire perçoit ainsi parallèlement aux risques de sécurité techniques, qui peuvent être identifiés et traités au moment du développement de ces solutions, d'autres risques de sécurité, davantage liés à des facteurs humains, dans le déploiement et la maintenance dans le temps de ces nouvelles solutions d'acceptation.

Aussi attrayante que soit la technologie SoftPOS, son adoption doit donc être le fruit d'une profonde réflexion sur les potentiels bénéfices et risques encourus. Ainsi, l'expérience utilisateur ou le coût de maintenance peuvent constituer de réels avantages. Toutefois, ils sont à mettre en regard des risques de sécurité liés à la variabilité des composants matériels, des systèmes d'exploitation et des applications installées sur les équipements mobiles grand public sur lesquels seront également déployés ces logiciels de paiement.

Dans la majorité des situations, les terminaux de paiement dédiés, qui se sont aussi adaptés à des situations de mobilité (terminaux autonomes, terminaux m-POS), restent des solutions connues des consommateurs et qui ont démontré dans le temps leur robustesse et leur sécurité. Tout en reconnaissant que les solutions d'acceptation de paiement par mobile peuvent être compatibles avec de hauts niveaux de sécurité, l'Observatoire appelle donc les acteurs de marché à être particulièrement rigoureux et sélectifs dans le développement des solutions SoftPOS. Cela suppose de privilégier, au moins dans les premiers temps, son déploiement dans des environnements de confiance particulièrement contrôlés par la chaîne d'acceptation ou pour des situations où le paiement par carte est aujourd'hui inaccessible. Ce type de paiement pourrait, grâce à ces nouvelles solutions d'acceptation, se substituer à d'autres moyens de paiement plus exposés à la fraude comme le chèque.

3.7 Conclusion

L'Observatoire note que le contexte de marché a fortement évolué depuis la dernière étude de 2016 sur les solutions d'acceptation de paiement sur mobile. La sécurité technique de ces solutions est désormais rendue possible par l'élaboration de standards et de programmes de certification, ainsi que par la présence de composants matériels et logiciels de sécurité dans les téléphones. L'Observatoire considère ainsi que les solutions SoftPOS pourraient être en mesure d'atteindre un niveau de sécurité technique équivalent aux paiements par carte avec lecture de la puce par un terminal dédié.

Les potentiels vecteurs d'attaque d'une solution SoftPOS

Attaque par *malwares*

Ce risque se matérialise si les mises à jour de sécurité recommandées pour le système d'exploitation de l'appareil mobile du commerçant ne sont pas régulièrement installées ou si une application mobile tierce non sécurisée est installée sur le même appareil que l'application SoftPOS. Les *malwares* pourraient alors exploiter les vulnérabilités du téléphone pour accéder et compromettre l'application SoftPOS.

La contre-mesure déployée par les solutions SoftPOS est un mécanisme d'attestation qui contrôle fréquemment le niveau de sécurité générale du *smartphone* (version du système d'exploitation, détection de logiciels connus pour être porteurs de *malwares*, etc.). En complément, l'Observatoire invite les commerçants utilisateurs de solutions SoftPOS à être particulièrement diligents dans l'application des mises à jour de sécurité proposées sur leurs *smartphones* et les applications installées. De plus, l'Observatoire invite à considérer le *smartphone* sur lequel est installée l'application de paiement comme un appareil aussi sensible qu'un terminal de paiement, sur lequel il est souhaitable de limiter l'installation d'applications tierces et de n'autoriser que celles provenant de magasins d'applications fiables (*stores*).

Si la gestion du parc de terminaux est centralisée auprès d'une équipe ou d'un prestataire dédié, l'Observatoire recommande de prévoir des mises à jour forcées des *smartphones* et de contrôler les applications tierces pouvant être installées.

Attaque de type « homme du milieu » (*man-in-the-middle attack*)

Une attaque *man-in-the-middle* (MitM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que leur canal de communication a été compromis. Les principales catégories d'attaques MitM sont l'écoute des communications Wi-Fi, le détournement de session, l'usurpation d'adresse IP et l'usurpation de DNS (*domain name system*, système de nom de domaine).

La contre-mesure utilisée par la très grande majorité des communications réseaux à l'heure actuelle est

le chiffrement des communications. Les données capturées sont ainsi inexploitable sous réserve que l'algorithme de chiffrement choisi soit suffisamment robuste et non obsolète.

L'Observatoire invite tous les acteurs intervenant dans le développement, la distribution et le contrôle d'applications SoftPOS à maintenir une veille active sur les failles des protocoles de communication et des équipements réseaux et à effectuer dès que possible les maintenances correctives.

Les fausses applications SoftPOS

Ces faux logiciels pourraient être utilisés pour capturer les données de la carte. La fraude ne consiste alors pas à détourner ou falsifier une opération de paiement légitime, mais à capturer certaines données pour initier des transactions dans d'autres environnements (paiements sur Internet ou à distance, émission d'une carte contrefaite, etc.). Il peut s'agir des données de la carte (numéro, code de confirmation, date d'expiration), mais aussi du code PIN. C'est l'équivalent dans l'environnement logiciel des terminaux piratés avec des dispositifs matériels de *skimming* ou de *shimming*. Contrairement aux terminaux traditionnels, en l'absence d'élément matériel visible, le consommateur pourra, *a priori*, difficilement identifier les fausses applications SoftPOS.

Dans ce schéma de fraude, le commerçant peut participer activement à la fraude s'il présente cette fausse application en toute connaissance de cause au consommateur, ou passivement si la fausse application SoftPOS s'est substituée à son application légitime à son insu. Un exemple de participation active serait un commerçant, ou un collaborateur de ce dernier, qui déciderait de présenter un *smartphone* sur lequel est installée une fausse application SoftPOS pour capturer les données de la carte, prétendre que cela fonctionne mal lorsque la transaction est en échec et revenir avec un autre *smartphone* sur lequel est installée la véritable application SoftPOS. Un exemple de participation passive serait la substitution par le fraudeur, à l'insu du commerçant, du *smartphone* par un appareil équivalent sur lequel est installée la fausse application SoftPOS. Celle-ci prétendra alors que la transaction a réussi.

L'Observatoire invite les acteurs de marché à intégrer des éléments distinctifs et reconnaissables par le consommateur dans l'application de paiement SoftPOS dans le but d'éveiller sa vigilance dès les premiers instants de l'acte d'achat. En cas de doute, l'Observatoire recommande au consommateur de demander un autre terminal ou de choisir un autre moyen de paiement.

Le détournement

L'application SoftPOS est fonctionnelle, mais elle est configurée avec un autre acquéreur et permet ainsi de détourner les fonds. Cette fraude se fait à l'insu du commerçant et du consommateur. Le premier ne reçoit pas les fonds, tandis que le consommateur règle le montant de la transaction légitime et ne se rend donc pas compte de la supercherie. Ce type de fraude repose sur les mêmes mécanismes de substitution, qui existent pour les terminaux traditionnels.

La contre-mesure pour ce type d'attaque peut difficilement être d'ordre technologique. L'Observatoire appelle les commerçants à appliquer à leurs *smartphones* servant de terminal d'acceptation les mêmes règles de sécurité et de vigilance que celles applicables aux terminaux traditionnels : garder les terminaux sous contrôle et dans le champ de vision du commerçant, les mettre en sécurité quand le magasin est fermé, les contrôler régulièrement, leur apposer des signes distinctifs et toutes autres mesures de prudence jugées pertinentes.

ACTIONS CONDUITES PAR L'OBSERVATOIRE EN 2022

Ce chapitre revient sur les actions et les recommandations de l'Observatoire en matière d'authentification forte des paiements par carte (4.1), des paiements par chèque (4.2) et de veille technologique (4.3).

4.1 L'authentification forte des paiements par carte

Le déploiement de l'authentification forte des paiements sur Internet, introduite par la deuxième directive européenne sur les services de paiement (DSP 2), est terminé en France depuis 2021, comme l'avait souligné l'Observatoire dans son rapport annuel de l'année dernière. Au-delà du suivi des effets positifs apportés par l'authentification forte en matière de réduction de la fraude (*cf. chapitre 1*), l'Observatoire est resté mobilisé en 2022 pour veiller à l'amélioration durable de la sécurité des paiements sur Internet. À cette fin, il a apporté des clarifications sur l'application de la réglementation en matière de gestion des exemptions et a travaillé avec les secteurs des télécommunications, notamment les opérateurs téléphoniques, pour identifier des pistes de sécurisation supplémentaires aux moyens d'authentification.

4.1.1 Aperçu de l'équipement des porteurs en solutions d'authentification forte

L'équipement en authentification forte des porteurs de carte fut essentiellement réalisé entre 2019 et 2021. À fin 2022, l'Observatoire note que les solutions d'authentification forte n'évoluent qu'à la marge :

- **L'application mobile sécurisée** reste la principale solution d'authentification forte en France : 73 % des porteurs de carte en sont équipés (contre 68 % en 2021), mais ce type de solution est utilisée dans 81 %

des paiements authentifiés. Pour rappel, il s'agit d'une solution qui permet au porteur de s'authentifier, avec un code confidentiel ou un facteur biométrique, par l'intermédiaire de l'application bancaire installée sur son téléphone mobile.

- **L'OTP renforcé** qui combine un code à usage unique (*one time password* – OTP), reçu par SMS ou par message vocal (serveur vocal interactif – SVI), avec un mot de passe statique connu par le porteur. La proportion de porteurs équipés de ce dispositif s'est réduite de cinq points pour atteindre 23 % à fin 2022.
- **L'appareil physique** : mis à disposition du porteur par son prestataire de services de paiement, il peut s'agir d'un générateur de codes doté d'un clavier de saisie, d'une clé USB ou d'un lecteur de QR code. Ce dispositif s'adresse en particulier aux clients qui effectuent leurs achats en ligne systématiquement depuis l'ordinateur de leur domicile. Seulement 3 % des porteurs en étaient équipés à fin 2022, dans une proportion stable par rapport à 2021.

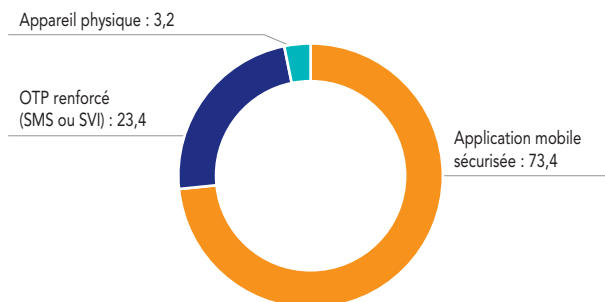
Si tous ces dispositifs répondent aux exigences réglementaires pour être reconnus comme des solutions d'authentification forte, l'application mobile sécurisée comme l'appareil physique sont jugés les plus sûrs. En effet, ces solutions reposent sur un dispositif physique qui ne peut pas être récupéré par un fraudeur agissant à distance. L'application mobile sécurisée est aussi perçue comme la solution la plus ergonomique et simple d'utilisation pour les clients. Ces deux raisons cumulées expliquent que l'application mobile sécurisée gagne du terrain dans l'équipement des porteurs, au détriment de l'OTP renforcé.

L'Observatoire rappelle toutefois que les utilisateurs doivent disposer de la liberté de choix de leur solution d'authentification. Les prestataires de services de

paiement sont donc invités à offrir au moins une méthode alternative et gratuite à l'application mobile sécurisée.

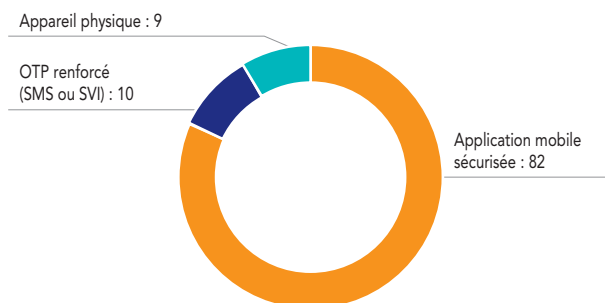
Cette vue d'ensemble ne couvre pas les solutions d'authentification forte déléguées à un tiers, comme les portefeuilles mobiles ou portefeuilles électroniques. Dans de telles situations, comme le rappelle l'Autorité bancaire européenne (ABE)¹, si l'authentification forte est techniquement mise en œuvre par le fournisseur tiers, l'émetteur reste responsable de la conformité réglementaire de la solution. La prestation de services entre l'émetteur et le fournisseur de la solution doit être conforme aux orientations de l'Autorité bancaire européenne relatives à l'externalisation du 25 février 2019 (EBA/GL/2019/02). De plus, l'enregistrement de la carte dans le portefeuille mobile doit faire l'objet d'une authentification forte préalable et systématique sous la responsabilité directe de l'émetteur (*Question and Answer – Q&A – n° 5622 de l'ABE*).

G1 Répartition de l'équipement des porteurs (en %)



Note : OTP – *one time password*, code à usage unique; SVI – serveur vocal interactif.
Source : Observatoire de la sécurité des moyens de paiement.

G2 Répartition de l'usage des solutions d'authentification forte parmi les paiements fortement authentifiés (en %)

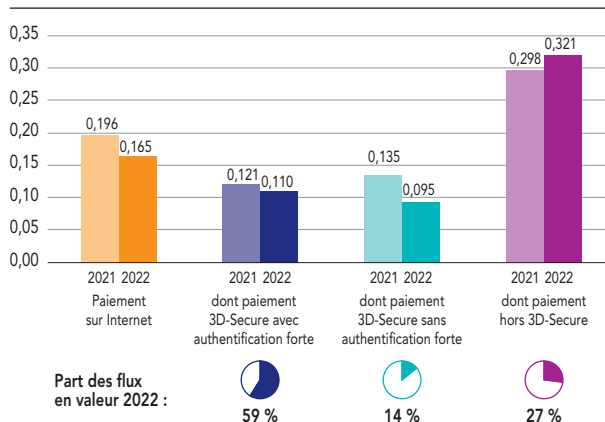


Note : OTP – *one time password*, code à usage unique; SVI – serveur vocal interactif.
Source : Observatoire de la sécurité des moyens de paiement.

4.1.2 Suivi de la fraude sur les paiements par carte

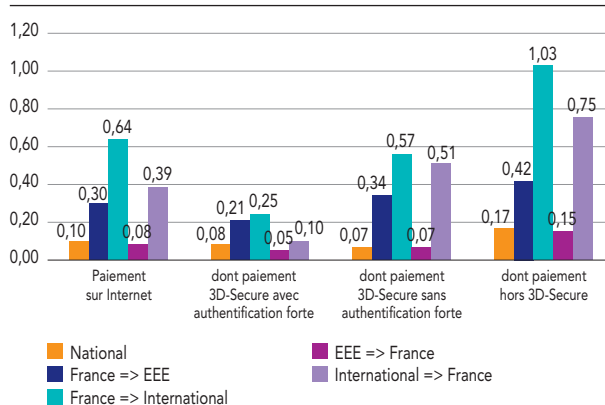
Le dispositif d'exemption à l'authentification forte prévu par la DSP 2 pour les transactions par carte sur Internet², car considérées plus sûres (faibles montants, faibles risques, etc.), se révèle globalement efficace. En effet, le taux de fraude des paiements 3D-Secure qui sont exemptés d'authentification forte (0,095 %) est très proche de celui des paiements 3D-Secure avec authentification forte (0,110 %). En revanche, les paiements hors 3D-Secure, qui représentent encore 27 % des transactions par carte sur Internet en valeur, restent proportionnellement trois fois plus fraudés, avec un taux de fraude à 0,321 %, en hausse par rapport à 2021.

G3 Taux de fraude des transactions sur Internet des cartes émises en France (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G4 Taux de fraude des paiements par carte sur Internet par canal d'authentification et zone géographique en 2022 (en %)



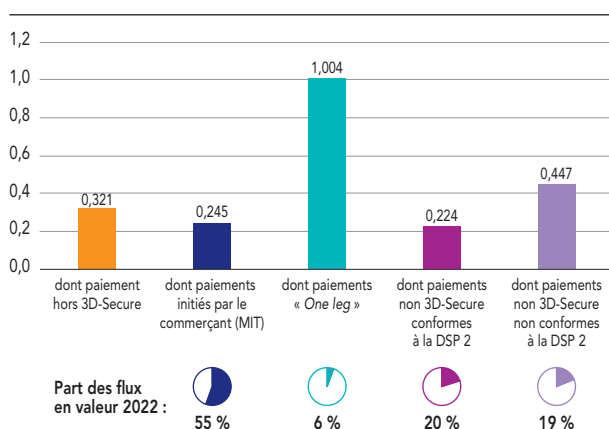
Note : EEE – Espace économique européen.

Source : Observatoire de la sécurité des moyens de paiement.

Ces observations générales méritent d'être détaillées par zone géographique :

- Au niveau national, les transactions s'appuyant sur le protocole 3D-Secure sont proportionnellement deux fois moins fraudées que celles ne l'utilisant pas. Parmi les transactions 3D-Secure, le taux de fraude est particulièrement bas pour les transactions 3D-Secure sans authentification forte (0,07 %), indiquant un très bon usage des exemptions au niveau domestique.
- Au niveau de l'Espace économique européen (EEE), ce bon usage des exemptions est également observé pour les paiements avec des cartes émises dans l'EEE et acceptées par des marchands français (0,07 % pour les paiements exemptés dans 3D-Secure, contre 0,05 % pour les paiements fortement authentifiés). En revanche, les paiements des porteurs français auprès de commerçants européens affichent des taux de fraude sensiblement supérieurs. En particulier, les paiements 3D-Secure qui sont exemptés d'authentification forte restent plus risqués que ceux avec authentification forte (0,34 %, contre 0,21 %). Ces chiffres révèlent un usage moins avisé des exemptions ou une infrastructure 3D-Secure moins efficace contre la fraude au niveau européen.
- Au niveau international, les règles d'authentification forte de la DSP 2 ne s'appliquent que sur une base volontaire et sous réserve de capacité de la contrepartie à les supporter. Les paiements sur Internet acceptés par les marchands français restent donc plus sûrs que les paiements des porteurs français auprès de marchands établis en dehors de l'EEE (0,39 %, contre 0,64 %).

G5 Taux de fraude des paiements par carte sur Internet hors 3D-Secure (en %)



Note : MIT – *Merchant Initiated Transactions*, transactions émises par le commerçant sans connexion active de l'utilisateur ; paiements *one-leg* : opérations non soumises à l'obligation d'authentification forte, car effectuées avec un commerçant ou un porteur de carte situé hors Espace économique européen ; DSP 2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

En 2022, les paiements hors 3D-Secure (3DS) représentent 27 % des montants échangés, mais supportent 53 % des montants de fraude affectant les paiements par carte sur Internet. En raison de leur profil de risque plus sensible, l'Observatoire a collecté pour la première fois en 2022 des données plus détaillées sur les paiements hors 3D-Secure. L'Observatoire en retire les principaux enseignements suivants :

- **Les paiements initiés par les marchands** (MIT – *Merchant Initiated Transactions*), qui représentent une part majoritaire des flux de paiement hors 3DS (55 %), affichent un taux de fraude près de deux fois supérieur aux paiements qui sont initiés par le porteur (CIT – *Customer Initiated Transactions*). L'Observatoire rappelle qu'au titre de la réglementation européenne ces transactions MIT doivent être chaînées à une preuve de l'authentification forte initiale du porteur. Celle-ci doit être sollicitée au moment où le porteur consent à ces opérations ultérieures (par exemple : souscription à un abonnement, achat avec expédition différée, paiement associé à une réservation, etc.).
- **Les paiements non conformes à la DSP 2**, c'est-à-dire autorisés sans authentification forte alors qu'il n'y a aucun motif d'exemption qui puisse le justifier, représentent une part non négligeable de ces opérations (19 % en montants). L'Observatoire sera donc très attentif en 2023 à l'extinction de cette catégorie, compte tenu de leur taux de fraude très élevé (0,447 %).
- **Les paiements non 3DS, mais conformes à la DSP 2**, car présentant en autorisation un motif d'exemption accepté par l'émetteur, affichent un taux de fraude deux fois supérieur aux paiements 3DS exemptés d'authentification forte (respectivement 0,224 %, contre 0,095 %). L'Observatoire cherchera à comprendre cet écart de performance pour des transactions qui présentent *a priori* la même expérience pour le consommateur.
- Enfin, **les paiements dits « one leg »** réalisés auprès de marchands établis en dehors de l'Espace économique européen, qui ne sont donc pas soumis aux règles de la DSP2, ont un taux de fraude très élevé (1,004 %). Toutefois, ces opérations restent peu nombreuses parmi les flux hors 3D-Secure.

1 Autorité bancaire européenne, communiqué de presse, 31 janvier 2023 : « EBA clarifies the application of strong customer authentication requirements to digital wallets ».

2 Les transactions par carte sur Internet couvrent tout paiement

électronique réalisé sur Internet (site commerçant ou en passant par une application mobile). Les paiements initiés par courrier postal ou électronique (courriel), par fax ou par appel téléphonique en sont donc exclus, car classés dans la catégorie distincte « Paiements à distance hors Internet ».

4.1.3 Rappel des principes applicables en matière d'exemption à l'authentification forte

La seconde directive européenne sur les services de paiement (DSP 2)³ fixe comme règle générale le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique. Toutefois, certains cas particuliers font figure d'exceptions définies sous forme d'exemptions dans les normes techniques réglementaires relatives à l'authentification forte et aux interfaces d'accès aux comptes (ci-après évoquées par le sigle RTS pour *regulatory technical standards*)⁴.

Les exemptions s'appuient sur des conditions d'application strictement définies, excepté l'exemption visée à l'article 18 des RTS, portant sur les transactions à faible niveau de risque (communément désignée sous l'acronyme TRA, pour *transaction risk analysis*). En effet, pour cette exemption, l'éligibilité de la transaction repose presque entièrement sur l'appréciation des prestataires de services de paiement (PSP), ce qui est donc susceptible d'induire des distorsions dans son application.

Afin d'apporter davantage de lisibilité à l'ensemble des parties prenantes (prestataires de services de paiement, mais aussi prestataires techniques, systèmes de paiement par carte, commerçants et consommateurs), l'Observatoire s'est attaché à formaliser les principes applicables pour la mise en œuvre des exemptions. Un éclairage particulier est apporté sur l'exemption TRA, notamment au regard des textes réglementaires et des précisions formulées par l'Autorité bancaire européenne dans ses avis⁵ et ses réponses d'interprétation réglementaire (processus de Q&A)⁶.

Principes généraux applicables à toutes les exemptions à l'authentification forte

Caractère non obligatoire et disponibilité de l'exemption

Bien que les exemptions ne présentent pas de caractère obligatoire, les prestataires de services de paiement (PSP) sont invités à les mettre en œuvre dès lors qu'ils sont en capacité technique de le faire et que les conditions d'application définies dans les RTS sont respectées.

Responsabilité du prestataire de services de paiement du payeur en matière de sécurité

Le PSP du payeur, chargé par la DSP 2 de veiller à la sécurité des paiements initiés par ses utilisateurs, conserve en toutes circonstances la faculté de requérir une authentification forte de son utilisateur dès lors que son appréciation du niveau de risque de l'opération le justifie, quand bien même l'opération remplit les critères d'éligibilité à une exemption (Q&A n° 4034 et 4480 de l'ABE).

Égalité de traitement entre prestataires de services de paiement À niveau de risque jugé équivalent, le PSP du payeur veille à répondre de façon équitable aux demandes d'exemption indépendamment de l'identité du PSP du bénéficiaire. En particulier, il veille à permettre aux autres PSP acquéreurs d'accéder aux mêmes exemptions que celles qu'il accorde aux opérations pour lesquelles il est lui-même le PSP du bénéficiaire.

Principes spécifiques applicables à l'exemption TRA

Respect du taux de fraude de référence par le PSP requérant l'exemption

Les RTS prévoient qu'un PSP ne peut recourir à l'exemption TRA que si les deux conditions suivantes sont remplies :

- il a déployé un mécanisme de contrôle des opérations en temps réel, intégrant les facteurs d'analyse spécifiés dans la réglementation dans une note de risque attribuée à chaque opération individuelle (article 18 des RTS, Q&A 4127),
- et si son taux de fraude pour le type d'opération concernée est suffisamment maîtrisé. Les taux de fraude de référence pour accéder à l'exemption TRA sont définis en annexe des RTS (cf. tableau ci-dessous).

T1 Taux de fraude de référence fixés par les RTS

Taux de fraude du PSP		Montant unitaire maximal des transactions éligibles à la TRA
Paiement par carte sur Internet	Virement par Internet	
≤ 0,01 %	≤ 0,005 %	500 €
≤ 0,06 %	≤ 0,010 %	250 €
≤ 0,13 %	≤ 0,015 %	100 €
> 0,13 %	> 0,015 %	Non éligible

Note : RTS – *regulatory technical standards*, normes techniques de réglementation ;

TRA – *transaction risk analysis*, transaction à faible niveau de risque ;

PSP – prestataire de services de paiement.

Source : Règlement délégué (UE) 2018/289 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 réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

Ces taux de fraude sont calculés :

- au niveau du PSP comme entité légale agréée (Q&A n° 4439 de l'ABE),
- pour chaque trimestre calendaire (articles 19 et 20 des RTS, Q&A n° 4045 de l'ABE),
- conformément aux orientations méthodologiques de l'ABE sur la fraude (EBA/GL/2018/05), aujourd'hui reprises dans la collecte semestrielle de la Banque de France « Recensement de la fraude aux moyens de paiement scripturaux »,
- et intègrent l'ensemble des paiements électroniques à distance liés à une carte, avec une approche globale et non par fourchette (Q&A n° 4043 et n° 4702 de l'ABE).

Par conséquent, le taux de fraude doit être calculé globalement en valeur sur le périmètre d'application de la DSP 2. Il s'agit des paiements émis électroniquement à l'initiative du payeur et pour lesquels les PSP du payeur et du bénéficiaire qui sont tous deux localisés au sein de l'Espace économique européen, tous canaux d'initiation, systèmes de paiement par carte et pays de l'EEE confondus. Ce calcul exclut donc les transactions i) émises non électroniquement (ordres papier, fax, etc.) ou ii) émises par le bénéficiaire (transactions MIT, etc.), ainsi que iii) celles dont la contrepartie se situe hors EEE (transactions dites *one-leg out*).

Comme point de référence, d'après les statistiques de l'Observatoire collectées auprès des systèmes de paiement par carte, le taux de fraude moyen pour des paiements par carte sur Internet issus du périmètre défini ci-dessus était en 2022 de :

- 0,12 % pour les cartes émises en France,
- 0,09 % pour les cartes acceptées en France.

Ces moyennes indiquent manifestement que tous les PSP émetteurs ou acquéreurs ne sont aujourd'hui pas éligibles à l'exemption TRA. Selon les PSP, la probabilité d'être en mesure d'utiliser cette exemption est aléatoire pour les transactions supérieures comprises entre 100 et 250 euros, eu égard au taux de fraude maximum de 0,06 % autorisé par la réglementation, et très faible pour les transactions supérieures à 250 et 500 euros, eu égard aux taux de fraude maximum de 0,01 % autorisé par la réglementation.

Taux de fraude à prendre en compte dans le cas des paiements par carte sur Internet

Dans le cas des transactions par carte sur Internet, l'exemption TRA peut être requise soit par le PSP émetteur (on parle de TRA émetteur), soit par le PSP acquéreur (TRA acquéreur). Seul le taux de fraude de référence du PSP demandant le recours à l'exemption TRA doit être pris en considération (Q&A n° 4034 de l'ABE) :

- en cas de demande de TRA acquéreur, le PSP émetteur a la possibilité de valider l'exemption même si son propre taux de fraude ne lui permet pas de solliciter une TRA émetteur pour la même transaction ;
- dans le cas où le taux de fraude du PSP acquéreur ne lui permet pas de requérir l'application d'une exemption TRA, il conserve la faculté de fournir au PSP émetteur des éléments d'appréciation d'un faible niveau de risque en vue d'inviter celui-ci à considérer de façon éclairée la possibilité de recourir à une exemption TRA émetteur ;
- le contrôle du positionnement du taux de fraude par rapport aux taux de référence relève de la seule responsabilité du PSP qui requiert l'exemption.

Responsabilité en cas de fraude

En cas de fraude sur une transaction ayant bénéficié de l'exemption TRA, la réglementation dispose que la responsabilité financière est supportée par le PSP à l'origine de la demande de TRA⁷. Ainsi, en cas de fraude sur une transaction associée :

- à une TRA (émetteur ou acquéreur), le PSP émetteur doit rembourser immédiatement et intégralement les opérations non autorisées au titulaire du moyen de paiement ;
- en complément, dans le cas d'une TRA acquéreur, le PSP acquéreur est tenu de rembourser à son tour et dans tous les cas le préjudice financier au PSP émetteur.

Calcul des taux de fraude pour les paiements par carte

L'Observatoire invite les PSP fournissant des services d'émission et d'acquisition à calculer des taux de fraude dissociés pour ces deux activités, et à considérer uniquement le taux de fraude relatif à leur rôle respectif dans une transaction donnée, c'est-à-dire :

- un taux de fraude en tant que PSP émetteur pour accorder une exemption TRA émetteur,
- un taux de fraude en tant que PSP acquéreur pour demander une exemption TRA acquéreur.

Suspension du droit d'usage de l'exemption TRA et notification à la Banque de France

Conformément à l'article 20 des RTS, les PSP doivent informer immédiatement la Banque de France si :

- leur taux de fraude, calculé pour les besoins de la TRA, dépasse l'un des taux de référence fixés par la réglementation, limitant ainsi leur capacité d'usage de l'exemption TRA ;
- leur taux de fraude est au contraire redevenu conforme à l'un des taux de référence, libérant de nouveau leur capacité d'usage de l'exemption TRA.

3 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

4 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 réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

5 Notamment l'avis suivant de l'ABE de juin 2018 : « EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) ».

6 L'accès aux Q&A de l'ABE se fait par l'intermédiaire de son *Single Rulebook* : www.eba.europa.eu/single-rule-book-qa

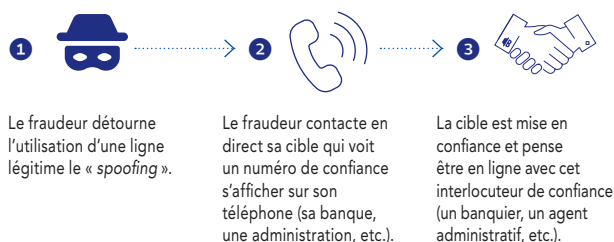
7 Références : articles 73 et 74 de la DSP 2, complété par Q&A 4042 de l'ABE.

Conformément au courrier du 19 décembre 2019 de la Banque de France, diffusé à l'ensemble des PSP par l'intermédiaire du Comité français d'organisation et de normalisation bancaires – CFONB (Communication n°20200002 du 8 janvier 2020), ces deux notifications sont à déclarer par les PSP, sous format libre, par courriel (2323-notifications-UT@banque-france.fr).

4.1.4 Travaux avec les opérateurs de téléphonie

Avec la dématérialisation des démarches bancaires, de plus en plus d'échanges entre le client et sa banque se font à distance. Malgré les mesures de sécurité mises en place par les banques afin de réduire la fraude sur les paiements en ligne, les fraudeurs exploitent plusieurs vulnérabilités du secteur téléphonique pour établir de nouveaux scénarios de fraude. Face à ce constat, l'Observatoire a sollicité en 2022 le secteur des télécommunications afin d'identifier des contre-mesures efficaces.

L'usurpation de numéro de ligne téléphonique (*spoofing*)



Source : Observatoire de la sécurité des moyens de paiement.

La loi dite « Naegelen »⁸, votée en 2020, vise à rendre impossibles de telles pratiques à compter de son entrée en application en juillet 2023. Les acteurs des télécommunications sont en train de déployer une nouvelle infrastructure afin d'assurer un meilleur niveau de confiance dans les numéros présentés lors des appels.

L'usurpation des identifiants des banques ou d'autres acteurs sensibles dans les numéros SMS (*smishing*)

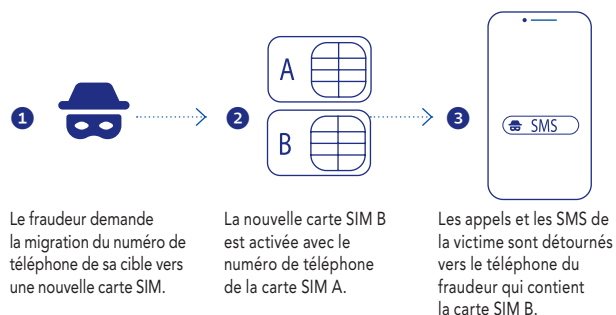


Source : Observatoire de la sécurité des moyens de paiement.

L'Association française du Multimédia Mobile (AF2M), regroupant les principaux opérateurs téléphoniques, a lancé

en octobre 2022 un plan d'action piloté pour protéger le recours à ces identifiants, couplé à la promotion du numéro court 33700 pour inviter les consommateurs à déclarer les SMS frauduleux reçus.

Les remises frauduleuses des cartes SIM (*SIM swapping*)



Source : Observatoire de la sécurité des moyens de paiement.

Un des dispositifs d'authentification le plus utilisé par les prestataires de services de paiement s'appuie sur l'utilisation de la ligne de téléphonie mobile du client afin d'envoyer à ce dernier par SMS un code à usage unique. Celui-ci est en effet reconnu comme un facteur de possession de la ligne téléphonique et sert autant à authentifier des transactions qu'à sécuriser des opérations sensibles (accès à la banque en ligne, ajout d'un bénéficiaire de confiance, ajout d'une carte dans un portefeuille mobile, etc.).

L'Observatoire constate malheureusement la persistance de pratiques frauduleuses, telles que le *SIM swapping*, utilisées afin de détourner les appels et SMS du porteur légitime de la carte vers un fraudeur. Ce phénomène a pris une nouvelle ampleur ces dernières années avec le développement des cartes SIM numériques (ou eSIM) qui permettent d'installer plusieurs lignes sur un même téléphone, ou de disposer d'une même ligne téléphonique sur plusieurs terminaux (par exemple sur un téléphone mobile multifonctions et une montre connectée en même temps).

Une mesure corrective consiste en la mise à disposition d'une interface de programmation d'application (*application programming interface* – API) interopérateurs. Celle-ci permet de se renseigner sur une carte SIM à laquelle est associé un numéro de téléphone donné. Ce dispositif appelé « *SIM Verify* » est en cours de test par quelques établissements pour enrichir le moteur de risque des solutions d'authentification forte recourant à des codes SMS, étant noté que la consultation de l'API est facturée.

Une autre mesure corrective préconisée par l'Observatoire est la plus forte sécurisation des procédures de délivrance de cartes SIM par les opérateurs téléphoniques. Ces procédures

devraient faire systématiquement appel à une authentification multifacteurs. Ainsi, comme le recommandait l'Observatoire dans son rapport annuel 2021⁹, les opérateurs téléphoniques peuvent recourir à des moyens d'identification électroniques de niveau substantiel ou élevé, ou à des solutions d'identité numérique apportant un niveau de sécurité équivalent pour sécuriser les changements de carte SIM et les demandes de eSIM.

4.1.5 Perspectives pour 2023

La réussite de la migration, dans le cadre de la directive DSP 2, avec la baisse significative du niveau de fraude sur les paiements par carte sur Internet, est une illustration d'une coopération réussie entre les acteurs de la Place. L'Observatoire tient à ce dialogue continu et cette collaboration en impliquant tous les acteurs requis dans le combat contre la fraude, les acteurs financiers comme les commerçants. Il continuera de renforcer ce dialogue et de veiller au suivi de la bonne application des règles de la DSP 2 et à l'harmonisation des pratiques au niveau du marché français et au niveau européen. En 2023, le groupe de travail « Authentification forte » de l'Observatoire continuera de travailler sur les trois axes suivants :

- l'intensification du dialogue et de la coopération avec le secteur des télécommunications, y compris avec l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), afin de concourir utilement à une meilleure sécurité des opérations et procédures téléphoniques ;
- la contribution active aux travaux réglementaires européens pour garantir l'harmonisation des règles et des pratiques en matière d'authentification forte des paiements, notamment dans la perspective de la révision de la DSP 2, avec une attention sur les règles applicables pour la mise en œuvre des exemptions à l'authentification forte et pour les cartes tokenisées ;
- la surveillance des taux de fraude des paiements sur Internet en réalisant des analyses comparatives avec les autres pays européens, grâce à la publication des premiers indicateurs de fraude aux moyens de paiement par les autorités européennes.

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

Dans un contexte de baisse rapide des paiements par chèque et de risques toujours élevés de fraude, l'Observatoire a conduit une étude spécifique sur la sécurité des paiements par

chèque. Les enseignements de cette étude ont été publiés en juillet 2021 dans son rapport annuel relatif à l'exercice 2020¹⁰. L'Observatoire a alors émis dix recommandations qui s'adressent à l'ensemble des acteurs de la filière, c'est-à-dire principalement les établissements bancaires, les sociétés spécialisées dans le traitement du chèque, les autorités publiques et les utilisateurs de ce moyen de paiement.

Deux ans après l'émission de ces recommandations, l'Observatoire note des progrès intéressants dans leur mise en œuvre. Compte tenu des niveaux toujours élevés de fraude, les efforts doivent être durablement poursuivis. Des progrès notables sont notamment attendus dans i) la sécurisation de l'envoi des chèquiers par voie postale et ii) la simplification des procédures de mise en opposition des formules de chèque volées.

En tenant compte des contrôles déjà effectués et de la politique de risques de chaque établissement, la Banque de France s'assure de la bonne mise en œuvre de ces recommandations par les établissements bancaires. Cette action entre dans le cadre de ses fonctions de surveillance¹¹, y compris au travers de missions de contrôle sur place. En parallèle, l'Observatoire a établi un groupe de travail « Chèque » qui réunit les experts du chèque, les représentants des utilisateurs et les pouvoirs publics. Ce groupe échange des informations sur les dernières tendances de fraude et structure la coopération entre les acteurs dans la lutte contre la fraude.

Des actions de sensibilisation ont également été effectuées en 2022 par divers acteurs :

- le site Assurance Banque Épargne-Info Service (ABE-IS), mis en place par l'Autorité de contrôle prudentiel et de résolution (ACPR), l'Autorité des marchés financiers (AMF) et la Banque de France, a fait une série de *podcasts* dont un épisode traitant des mesures permettant de se protéger contre la fraude au chèque¹² ;

8 Loi n° 2020-901 du 24 juillet 2020 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux.

9 Cf. Chapitre 3, « L'identité numérique et la sécurité des paiements. »

10 Cf. le chapitre 4, « Étude sur la fraude au chèque : enseignements et recommandations ».

11 Article L. 141-4 du Code monétaire et financier, paragraphe 4 : « La Banque de France s'assure de la sécurité des moyens de paiement tels que définis à l'article L. 311-3, autres que la

monnaie fiduciaire, et de la pertinence des normes applicables en la matière. Si elle estime qu'un de ces moyens de paiement présente des garanties insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier. Si ces recommandations n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au Journal officiel ».

12 Cf. *Amaques financières, et si on en parlait ! La minute info | Banque de France (abe-infoservice.fr)*

T2 Vue synthétique de la mise en œuvre des dix recommandations de l'Observatoire sur la fraude au chèque

Recommandation	Niveau de réalisation
Recommandation n° 1 : Révision de la collecte statistique de la Banque de France pour améliorer la connaissance des phénomènes de fraude au chèque	Réalisée
Recommandation n° 2 : Améliorer les contrôles de la banque du remettant contre les remises frauduleuses	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 3 : Soutenir le développement des contrôles du côté de l'établissement tiré	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 4 : Protéger les chèques du vol dans leur acheminement et chez le client	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 5 : Simplifier les procédures de mise en opposition pour perte ou vol	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 6 : Offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du Fichier national des chèques irréguliers (FNCI)	Nouvelle offre de mandataire spécifique mise en place par le service Vérifiance-FNCI-Banque de France, en cours de déploiement
Recommandation n° 7 : Renforcer la surveillance de la Banque de France sur la résistance physique des formules contre la falsification et la contrefaçon	Réalisée
Recommandation n° 8 : Assurer l'efficacité du service Vérifiance-FNCI-Banque de France de lutte contre la contrefaçon de chèques	Réalisée
Recommandation n° 9 : Structurer durablement la coopération entre les acteurs dans la lutte contre la fraude et soutenir l'action des forces de l'ordre	Réalisée
Recommandation n° 10 : Soutenir par un plan de communication la vigilance des utilisateurs dans l'usage du chèque	Réalisée

Source : Observatoire de la sécurité des moyens de paiement.

- la Banque de France a également mis en ligne, dans le cadre de sa mission d'éducation financière, une série de contenus traitant des chèques et des mesures de prévention contre la fraude, notamment un épisode de *La Minute Cash* traitant des arnaques aux chèques ¹³ ;
- la *task-force* nationale de lutte contre les arnaques, animée par la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et associant l'ensemble des administrations et autorités intéressées dans la lutte contre les fraudes, a mis à jour en juillet 2022 son guide de prévention contre les arnaques, dont la fiche n° 3 traite spécialement des escroqueries au chèque bancaire ¹⁴ ;
- la Fédération bancaire française (FBF) a mis à jour en octobre 2022 sur son site Internet *Les clés de la banque*, un guide consacré au chèque, qui fournit huit réflexes de sécurité ¹⁵ .

4.2.1 La finalisation de la révision du référentiel de sécurité du chèque (RSC) de la Banque de France

Au titre de sa mission de surveillance ¹⁶ sur la sécurité des moyens de paiement, la Banque de France s'assure de la sécurité des normes applicables au chèque. En complément des dispositions législatives et réglementaires rassemblées dans le Code monétaire et financier, le fonctionnement du système français de paiement par chèque est déterminé par le règlement de 2001 relatif à la compensation des chèques, ainsi que par des textes professionnels publiés par le Comité français d'organisation et de normalisation bancaire (CFONB), dont la Banque de France fait partie. En complément, la Banque de France fait valoir ses exigences de sécurité au travers du référentiel de sécurité du chèque (RSC). Depuis son origine en 2005, le RSC couvre les différents

aspects de la sécurité du chèque (la fiabilité des opérations, la continuité d'activité et la lutte contre la fraude). Pour vérifier son respect, la Banque de France demande aux établissements bancaires de lui remettre un questionnaire annuel d'autoévaluation. Compte tenu des nouvelles recommandations de l'Observatoire formulées en 2021, et pour couvrir encore plus explicitement les risques de fraude, la Banque de France a de nouveau révisé le RSC en avril 2022. Cette révision traduit ainsi de manière opérationnelle les recommandations de l'Observatoire dans les établissements bancaires. La nouvelle version du RSC et son questionnaire associé ont été publiés sur le site de la Banque de France en avril 2022 pour une première application sur l'exercice 2022. En outre, le RSC est désormais enrichi de deux nouvelles procédures, applicables depuis janvier 2023, qui visent à renforcer la sécurité du chèque :

- D'une part, les incidents graves affectant le système de paiement sur le chèque doivent désormais être notifiés à la Banque de France par le biais d'une interface sécurisée. Cette procédure instaure pour le chèque une procédure équivalente à celle des incidents opérationnels et de sécurité majeurs que déclarent les établissements sur les autres services de paiement en application de la deuxième directive européenne sur les services de paiement (DSP 2) ¹⁷.
- D'autre part, les établissements tirés de chèque doivent transmettre à la Banque de France des spécimens de chèques mis en circulation, accompagnés d'un formulaire consacré à leurs signes de sécurité. Cette procédure permet à la Banque de France de renforcer sa surveillance des formules et d'apprécier les éléments de sécurité propres à chaque établissement bancaire, qui sont destinés à lutter contre la contrefaçon et la falsification des chèques.

4.2.2 Amélioration des contrôles par les banques sur les opérations par chèque (recommandations n° 2 et 3)

Pour lutter contre le développement de la fraude par cavalerie, par laquelle des personnes sont mobilisées pour encaisser des chèques frauduleux pour le compte d'autrui ¹⁸, concourant ainsi à la réalisation d'une fraude, les établissements bancaires ont construit des outils de détection de remises frauduleuses ou atypiques. En cas de soupçon de fraude, ces outils permettent aux établissements remettants de chèques d'actionner des mécanismes de temporisation ou de blocage de la mise à disposition des fonds sur le compte du client. Dans l'attente d'un éventuel rejet du chèque pour fraude de la part de la banque du tireur, la banque retarde ainsi le crédit du chèque de quelques jours ou renforce les contrôles sur les opérations ultérieures.

Depuis 2021, l'Observatoire mesure les effets de ces mesures par le biais de nouveaux indicateurs remontés par les établissements bancaires. **En 2022, ces indicateurs montrent une amélioration de leur performance avec 161 millions d'euros de fraude déjouée sur 557 millions d'euros de chèques frauduleux remis à l'encaissement, ce qui a ainsi permis de déjouer 29 % de la fraude au chèque en 2022, contre 26 % en 2021.**

Pour soutenir le développement de ces outils, l'Observatoire appelle les pouvoirs publics à autoriser les banques en tant que présentateurs de chèques à consulter le Fichier national des chèques irréguliers (FNCI) tenu par la Banque de France. Il est aujourd'hui ouvert aux seuls bénéficiaires de chèques, à condition que la consultation ne soit pas obligatoire et qu'elle n'engage pas leur responsabilité. Cela pourrait permettre aux banques en tant que banquiers remettants de connaître les chèques mis en opposition au moment de la remise ou lors des traitements.

En parallèle, les banques tirées commencent à développer des outils et des processus de contrôle des chèques reçus en paiement permettant de déclencher des alertes sur les chèques soupçonnés d'être frauduleux et de questionner leurs clients émetteurs de ces chèques. La Banque de France analyse la qualité et la pertinence de ces premiers développements lors de ses actions de surveillance des établissements bancaires.

Enfin, pour renforcer sa surveillance des établissements bancaires, la Banque de France a révisé sa collecte statistique « Recensement de la fraude aux moyens de paiement

13 Cf. *S3E5 La Minute Cash | L'arnaque au chèque* - YouTube

14 Cf. *Guide-TF-actualise-1907.pdf* (economie.gouv.fr)

15 Le guide est accessible sous le lien Internet suivant : www.lescledelabanque.com/particulier/le-cheque-8-reflexes-securite

16 Article L. 141-4 du Code monétaire et financier, paragraphe 4 : « La Banque de France s'assure de la sécurité des moyens de paiement tels que définis à l'article L. 311-3, autres que la monnaie fiduciaire, et de la pertinence des normes applicables en la matière. Si elle estime qu'un de ces moyens de paiement présente des garanties insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier. Si ces recommandations

n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au Journal officiel ».

17 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, article 96.

18 Il s'agit de remises frauduleuses de chèques par le biais de personnes intermédiaires, parfois appelées « mules ». Qu'elles soient volontaires ou trompées, ces personnes intermédiaires acceptent d'encaisser les chèques frauduleux sur leur compte avant de restituer à l'escroc tout ou partie des fonds. Après que les chèques ont été rejetés pour fraude, les crédits des opérations d'encaissement sont annulés.

scripturaux » en complétant ses indicateurs de recensement des fraudes sur le chèque. Depuis 2022, les établissements tirés de chèque, c'est-à-dire les établissements bancaires qui tiennent le compte des débiteurs qui ont émis un chèque, doivent également déclarer les fraudes au chèque. Ces statistiques viennent compléter celles qui sont recueillies auprès des établissements remettants, c'est-à-dire les établissements bancaires qui tiennent le compte des créanciers qui ont remis des chèques à l'encaissement. Pour ses besoins de surveillance, la Banque de France analyse ces nouvelles données pour identifier les établissements bancaires les plus exposés à la fraude au chèque en tant que tirés.

4.2.3 Protection du chèque du vol lors de l'acheminement chez le client (recommandation n° 4)

Pour lutter plus efficacement contre le vol de chèques pendant la phase d'acheminement chez le client, l'Observatoire a appelé les établissements bancaires à sécuriser par tout moyen l'acheminement des chèques par voie postale et à adopter en ce domaine un dispositif de vigilance permanente assurant une réaction rapide. Les utilisateurs sont également invités à préférer le retrait sécurisé du chèque en agence. Or, après la crise liée à la Covid-19 et les périodes de confinement afférentes, il est apparu que les utilisateurs privilégiaient de plus en plus la réception du chèque à domicile. À ce stade, l'Observatoire estime qu'environ deux tiers des chèques sont acheminés par voie postale sous différentes formes d'envoi (lettre simple, lettre suivie, lettre recommandée avec accusé de réception). **Dans ce contexte, l'Observatoire souligne que les clients doivent garder à tout moment la possibilité de retirer leur chèque en agence, au moins pour les clients d'un établissement bancaire disposant d'un réseau d'agences. Cette possibilité doit être explicitement offerte aux clients, et ceci à titre gratuit**¹⁹.

Les établissements bancaires ont engagé différentes initiatives pour sécuriser encore davantage les envois de chèques, comme l'envoi systématique d'un SMS à l'attention de leurs clients afin, d'une part, de les prévenir de l'arrivée prochaine de leur chèque et d'autre part, d'appeler à leur vigilance en leur demandant de se manifester s'ils ne l'ont pas reçu dans un délai déterminé. Si ces initiatives vont dans le bon sens, elles ne répondent pas toujours à la recommandation de l'Observatoire, qui privilégie les actions permettant une mise en opposition très réactive des chèques volés. Dans ce contexte, le groupe de travail sur la fraude au chèque de l'Observatoire prévoit de réaliser des travaux plus approfondis sur les pratiques des banques en matière d'envoi des chèques, par exemple pour éviter les envois automatiques de chèques pour lesquels le destinataire

n'aurait pas été alerté au préalable. Ces travaux couvriront le suivi des déclarations au FNCI par les banques des chèques volés ou perdus pendant leur acheminement chez le client.

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

Que le chèque ait fait l'objet d'une perte ou d'un vol au cours de l'acheminement postal ou bien chez le client (cambriolage, vol à la tire, etc.), l'Observatoire a rappelé la nécessité d'agir sans tarder pour s'assurer de son inscription au FNCI.

Les procédures d'opposition sont encadrées par des dispositions législatives qui se sont traduites, au sein des établissements bancaires, par des formalités contraignantes. Les modalités d'opposition, très disparates d'un établissement à l'autre, supposent toujours une première action de déclaration d'opposition, qui passe par différents moyens (agence, centre d'appel, téléphone, déclaration sur l'espace Web de banque en ligne, application bancaire mobile, messagerie sécurisée, etc.). Celle-ci est généralement suivie, à quelques exceptions près, par une confirmation écrite de l'opposition sous la forme d'une lettre recommandée avec accusé de réception. De même, il est apparu que certaines pratiques tarifaires peuvent être de nature à décourager le client de procéder à une opposition.

À ce stade, des projets de simplification sont bien prévus dans certains groupes bancaires, mais des améliorations substantielles sont encore attendues dans l'amélioration des procédures de mise en opposition. L'objectif est de les rendre simples, claires et accessibles aux différentes typologies de clientèle. Conformément à l'article L. 131-35²⁰ du Code monétaire et financier, « *le tireur doit immédiatement confirmer son opposition par écrit, quel que soit le support de cet écrit* ». L'Observatoire souligne que la confirmation écrite de l'opposition ne suppose pas nécessairement un courrier, mais peut se faire par voie électronique, notamment dans les espaces de banque en ligne, ce qui permet de raccourcir les délais de mise en opposition et de conserver la trace de la confirmation. De même, pour les chèques qui n'auraient jamais été reçus par les clients, l'Observatoire rappelle que les établissements bancaires doivent alors prendre en charge la mise en opposition, qui ne doit pas être refacturée au client (cf. recommandation n° 5).

4.2.5 Consultation du Fichier national des chèques irréguliers (FNCI) au bénéfice du plus grand nombre (recommandation n° 6)

Pour lutter contre la fraude, l'Observatoire a exprimé la nécessité de promouvoir plus largement la consultation du

Fichier national des chèques irréguliers (FNCI). En effet, en consultant le FNCI, le créancier peut identifier un chèque frauduleux avant de l'accepter comme moyen de règlement. Au-delà des chèques rattachés à des comptes en interdit bancaire ou judiciaire ou clos, le FNCI recense tous les chèques mis en opposition signalés par le porteur pour perte, vol ou utilisation frauduleuse (articles L. 131-35 et L. 131-84 du Code monétaire et financier) et tous les faux chèques, correspondant à des cas de contrefaçon, signalés par les établissements bancaires (arrêté du 24 juillet 1992 relatif au traitement automatisé des informations sur la régularité des chèques mis en œuvre par la Banque de France).

Or, la contribution préventive du FNCI dans la lutte contre la fraude reste très marginale. En effet, les consultations du FNCI ont permis de déjouer 7,7 % des cas de fraude au chèque en 2022, contre 5,7 % en 2021. Elle était toutefois de 17,2 % en 2018²¹.

Pour améliorer l'efficacité de ce fichier, l'Observatoire réitère les recommandations suivantes :

- 1) D'une part, que tout chèque volé fasse l'objet d'une mise en opposition et que celle-ci intervienne le plus rapidement possible après le vol. Cette action est fondamentale et doit faire l'objet de plan de remédiations de la part de chacun des acteurs. L'Observatoire constate en effet que le volume de mises en opposition de chèques perdus/volés déclarés au FNCI est en baisse : il passe à 2,4 millions en 2022, contre 2,6 millions en 2021.
- 2) D'autre part, que les personnes acceptant le chèque comme moyen de paiement consultent plus largement le fichier. Même si le nombre de consultations reste toujours très faible en comparaison à l'usage du chèque, l'Observatoire note que le nombre de consultations du FNCI représente depuis 2020 près de 4 % du volume de chèques émis (3,9 % en 2022, contre 3,8 % en 2021)²².

Le FNCI peut être directement consulté au moyen du service Vérifiance-FNCI-Banque de France, service officiel de consultation de la Banque de France. Aux côtés des modalités traditionnelles de consultation par voie informatique ou téléphone, une offre dite « agile » a été déployée par ce service spécialement à l'attention des petits accepteurs de chèques, comme les professionnels, les petits commerçants et les artisans, avec notamment la possibilité de disposer du service par l'intermédiaire d'une application mobile. D'autres sociétés spécialisées dans la prévention des chèques impayés intègrent aussi la consultation du FNCI dans leur offre auprès des accepteurs de chèque.

Néanmoins, pour ouvrir effectivement la consultation du FNCI au plus grand nombre et notamment aux particuliers et aux associations, la Banque de France a mis en place avec le prestataire en charge du service Vérifiance une nouvelle modalité de consultation du FNCI, appelée « mandataire spécifique ». Cette dernière pourrait notamment être proposée aux établissements bancaires, qui souhaiteraient permettre à leurs clients de consulter le FNCI avant d'accepter définitivement un chèque comme moyen de règlement. Par exemple, un particulier pourrait vérifier sur son espace de banque en ligne ou son application bancaire que le chèque qui lui est présenté n'est pas inscrit au FNCI. Une société spécialisée a obtenu ce statut de mandataire spécifique et commercialise sa nouvelle offre auprès des établissements bancaires. L'Observatoire soutient toute démarche ou initiative, qui permet d'offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du FNCI.

4.2.6 Perspectives pour 2023

La pérennisation du groupe de travail « Chèque » de l'OSMP a véritablement permis de renforcer la coopération des acteurs de la filière. Cela a notamment permis l'identification de points de contact du côté des forces de l'ordre pour que les professionnels de la filière (établissements bancaires, acteurs spécialisés dans le traitement du chèque, etc.) puissent remonter des signalements en matière de fraude au chèque.

En 2023, l'action de ce groupe de travail portera notamment sur :

- la réalisation de travaux plus approfondis sur les pratiques des banques en matière de sécurisation de l'envoi des chèquiers par voie postale, par exemple pour éviter que les chèquiers soient envoyés sans alerte préalable au client ;

19 La gratuité de la délivrance des formules de chèque est inscrite dans la loi à l'article L. 131-71 du Code monétaire et financier. Si le chéquier est envoyé par voie postale, les frais postaux peuvent toutefois être refacturés au client.

20 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 ».

21 Cet indicateur est calculé en divisant le nombre de consultations du service Vérifiance-FNCI-Banque de France ayant donné une réponse « rouge » pour des motifs d'opposition ou de faux chèques par le nombre total de tentatives d'utilisation de chèques frauduleux.

22 Cet indicateur est obtenu en divisant le nombre de consultations au service Vérifiance-FNCI-Banque de France par le nombre total de chèques échangés sur une année.

- l'accompagnement de la simplification des procédures de mise en opposition pour perte ou vol, dans leurs dimensions pratiques et tarifaires, afin de garantir l'efficacité de la contribution préventive du FNCI dans la lutte contre la fraude.

4.3 Rappel des principales recommandations de l'Observatoire sur les sujets de veille technologique

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.

4.3.1 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. Avec la publication en 2021 du référentiel d'exigences destiné aux prestataires de vérification d'identité à distance (PVID) et le processus de révision en cours de la réglementation européenne eIDAS sur l'identification électronique et les services de confiance²³, l'Observatoire invite les acteurs du paiement à lutter contre les usurpations d'identité en recourant aux services d'identité numérique conformes aux exigences PVID ou eIDAS.

4.3.2 Recommandations relatives à la sécurité des paiements en temps réel

Les recommandations relatives à la sécurité des paiements en temps réels 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

T3 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
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 : l'Observatoire de la sécurité des moyens de paiement.

T4 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)
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.

paiement, l'Observatoire reste particulièrement attentif à la sécurité des paiements en temps réel. En 2022, le virement instantané représentait 3,8 % du nombre total de virements et 0,3 % 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 84 % par rapport à 2021. L'augmentation devrait se poursuivre dans les prochaines années, soutenue par les stratégies nationales et européennes pour les moyens de paiement et par les initiatives législatives des pouvoirs publics européens. En matière de sécurité, l'Observatoire note que la fraude sur les paiements en temps réel augmente moins vite que les flux, si bien que le taux de fraude sur les virements instantanés est resté relativement stable depuis 2020, aux alentours de 0,044 %. Avec 52 millions d'euros de fraude sur le virement instantané en 2022, soit près de 17 % du total de la fraude recensée sur les virements, l'Observatoire renouvelle son appel vers les 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.

4.3.3 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

23 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*).

T5 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
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 leur 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

Source : Observatoire de la sécurité des moyens de paiement.

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.

4.3.4 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 trois dernières années, porté par la crise sanitaire et la possibilité de payer sans contact dans la limite de cinquante euros. Le nombre de paiements de ce type a ainsi été multiplié par un peu plus de 17,5 entre 2019 et 2022, pour représenter, en 2022, 6 % du nombre de paiements par carte de proximité et 9 % des paiements sans contact, contre respectivement 0,5 % et 1 % avant la crise sanitaire.

Dans le même temps, le taux de fraude des paiements sans contact par mobile, qui avait fortement progressé en 2020 pour s'établir à 0,102 %, s'est contracté en 2022 pour atteindre 0,064 %. 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, comme prévu par la DSP 2 au titre des opérations sensibles, est impérative.

T6 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 <i>smartphones</i>
Donner aux utilisateurs un niveau suffisant de visibilité sur les mesures de sécurité intégrées dans leurs applications tout en insistant sur le besoin de déployer des contre-mesures effectives pour lutter contre l'usage non autorisé de ces applications.	Prestataires de services de paiement
Évaluer régulièrement le niveau de sécurité des solutions de paiement par téléphone mobile.	Prestataires de services de paiement
Mettre à jour régulièrement le système d'exploitation de son téléphone mobile.	Utilisateurs
Choisir de manière non triviale et changer régulièrement les codes confidentiels, mots de passe et toute autre donnée personnelle utilisée pour les procédés d'authentification sur son <i>smartphone</i> , 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.

ANNEXES

A1	Conseils de prudence pour l'utilisation des moyens de paiement	67
A2	Missions et organisation de l'Observatoire	80
A3	Liste nominative des membres de l'Observatoire	82
A4	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux	85
A5	Dossier statistique sur l'usage et la fraude aux moyens de paiement	95

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



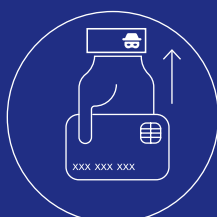
▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

- 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.

CONSEILS APPLICABLES AUX PAIEMENTS PAR CARTE



PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

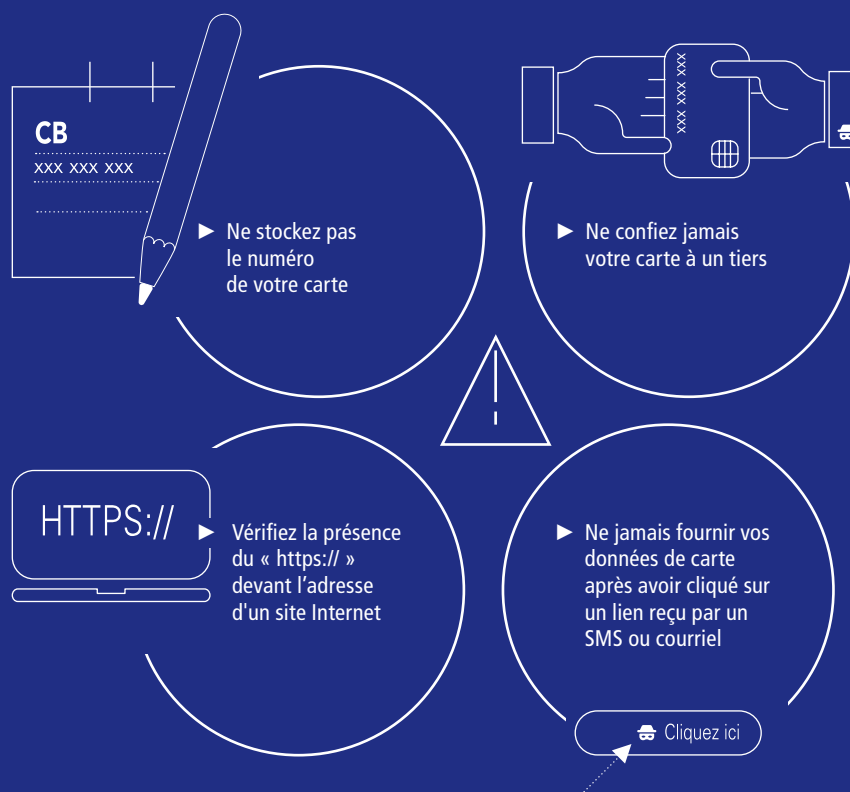
Campagnes
de *phishing* et *smishing*

Vol de carte

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

Manipulation psychosociale

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 votre code confidentiel : ne validez que les opérations de paiement dont vous êtes 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.

CONSEILS APPLICABLES AUX VIREMENTS



PRINCIPAUX CAS DE FRAUDE RENCONTRÉS



Ingénierie sociale

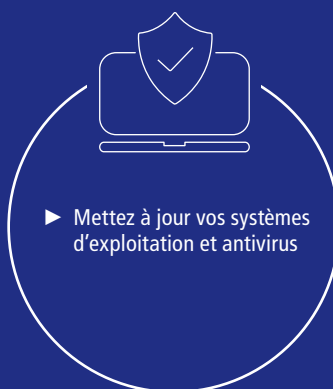


Attaques informatiques



Campagnes
de *phishing* et *smishing*

CONSEILS À DESTINATION DES UTILISATEURS



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 pour effectuer des faux tests dans le but de récupérer des identifiants de connexion, provoquer des virements frauduleux ou encore procéder à l'installation de logiciels malveillants.

▼ LES ATTAQUES INFORMATIQUES

- **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.).

CONSEILS APPLICABLES AUX PRÉLÈVEMENTS



PRINCIPAUX CAS DE FRAUDE RENCONTRÉS



Entente frauduleuse
entre le créancier
et le débiteur



Émission illégitime
d'ordres de prélèvement



Usurpation d'IBAN

CONSEILS À DESTINATION DES UTILISATEURS



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 mandats de prélèvement correspondants. 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.

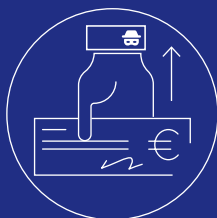
▷ CONSEILS À DESTINATION DE TOUS LES DÉBITEURS

- 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 débité 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.

CONSEILS APPLICABLES AUX CHÈQUES

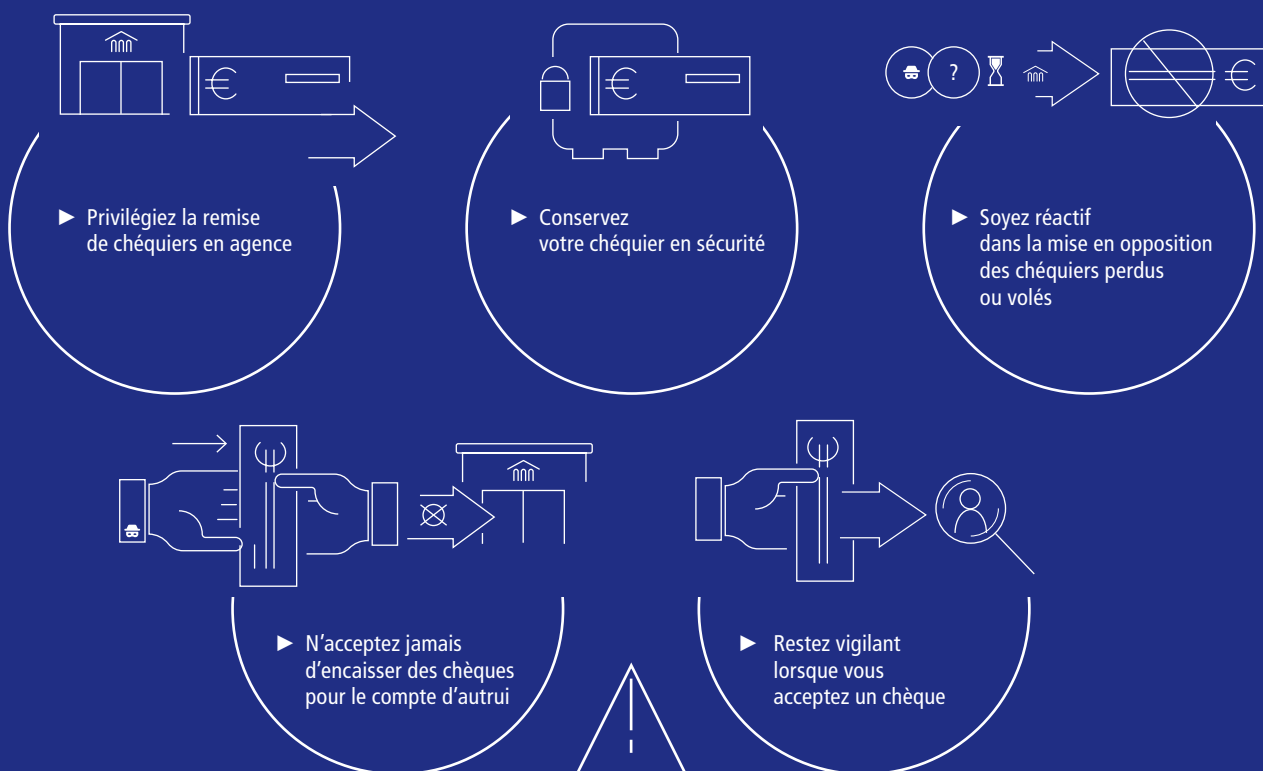


PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Vol de chèque(s)
ou chéquierContrefaçon
d'un chèqueFalsification
d'un chèque

Fraude à la « mule »

CONSEILS À DESTINATION DES UTILISATEURS



PRINCIPAUX CAS DE FRAUDE AU CHÈQUE RENCONTRÉS

▼ ORIGINE DES CHÈQUES FRAUDULEUX

- Vol de chèquiers 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

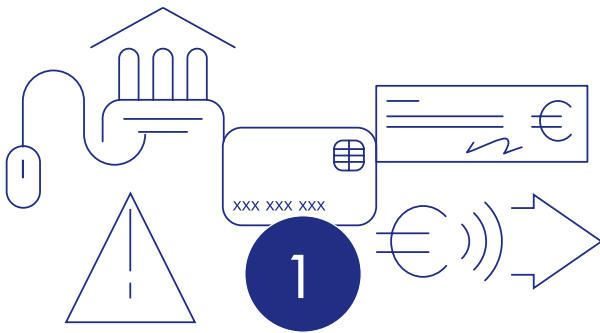
- Privilégiez dans la mesure du possible la remise de chèquiers en agence et en cas d'envoi par voie postale, soyez très attentifs à sa réception et faites opposition aussitôt que le délai est anormalement long.
- Conservez votre chéquier en sécurité et remplissez votre chèque avec soin, à l'encre noire, 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 chèquiers perdus ou volés, ou des chèques non reçus par leur bénéficiaire.

▷ CONSEILS À DESTINATION DES COMMERÇANTS

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

DEUXIÈME PARTIE – RÉAGIR EN CAS DE FRAUDE





FAIRE OPPOSITION

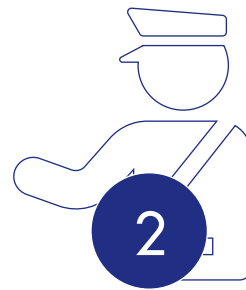
- **Faites immédiatement opposition** dès que vous constatez la perte, le vol, le détournement ou toute utilisation non autorisée de votre moyen de paiement ou des données qui y sont liées. Cette opposition permet de bloquer le moyen de paiement, évitant ainsi par la suite toute opération frauduleuse.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

▼ En pratique

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



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



SIGNALER LA FRAUDE AUPRÈS DES FORCES DE L'ORDRE

- **Il est recommandé de systématiquement signaler les cas de fraude aux moyens de paiement aux forces de l'ordre**, en privilégiant les démarches sur les plateformes Perceval pour les fraudes à la carte bancaire sur Internet et Thésée¹ 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.**

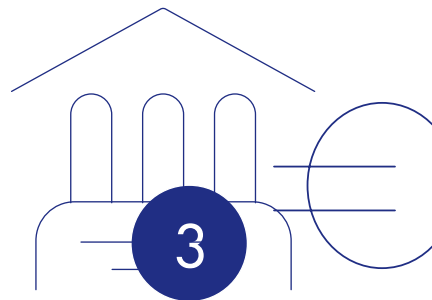
Toutefois, l'utilisateur peut aussi porter plainte auprès d'un commissariat de police ou d'une unité de gendarmerie en cas de vol de votre moyen de paiement et en cas d'utilisation frauduleuse de celui-ci ou des données qui lui sont liées. Afin de gagner du temps lors de votre rendez-vous, une pré-plainte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



▼ 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.**

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.

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 remboursement² 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 contraignantes³.

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 à ces mêmes services, 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.

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.

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 ;
- quatorze représentants des émetteurs de moyens de paiement et des opérateurs de systèmes de paiement ;
- cinq représentants du collège consommateurs du Conseil national de la consommation ;
- huit représentants des organisations professionnelles de 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 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 François Villeroy de Galhau, 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 20 juin 2023.

PRÉSIDENT

François VILLEROY DE GALHAU

Gouverneur de la Banque de France

REPRÉSENTANTS DES ASSEMBLÉES

Éric BOCQUET

Sénateur

Michaël TAVERNE

Député

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

- La secrétaire générale ou son représentant :
Nathalie AUFAUVRE
Grégoire VUARLOT

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 :
Vivien MURA

Sur proposition du ministre de l'Économie, de l'Industrie et du Numérique :

- Le haut fonctionnaire de défense et de sécurité ou son représentant :
Samuel HEUZÉ

- Le directeur général du Trésor ou son représentant :
Bastien LAFON

- 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

- Le directeur général de la Concurrence, de la Consommation et de la Répression des fraudes ou son représentant :
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
Léa OBADIA

Sur proposition du ministre de l'Intérieur :

- Le sous-directeur de la lutte contre la criminalité financière à la Direction centrale de la police judiciaire (DCPJ) ou son représentant :
Thomas DE RICOLFIS
Anne-Sophie COULBOIS

- Le directeur général de la Gendarmerie nationale ou son représentant :
Étienne LESTRELIN

Sur proposition de la Commission nationale de l'informatique et des libertés :

- Le chef du service des Affaires économiques ou son représentant :
Nacéra BEKHAT
Aymeric PONTVIANNE

REPRÉSENTANTS DES ÉMETTEURS DE MOYENS DE PAIEMENT ET DES OPÉRATEURS DE SYSTÈMES DE PAIEMENT

Thomas GOUSSEAU

Membre du conseil d'administration
Association française des établissements de paiement et de monnaie électronique (Afepe)

Amelia NEWSOM-DAVIS

Directrice *Pay Services* d'Orange
Association française du Multimédia Mobile (AF2M)

Corinne DENAEYER

Chargée d'études
Association française des sociétés financières (ASF)

Sébastien MARINOT

Directeur – Stratégie et Relations de place *Cash Management*
BNP Paribas (BNPP)

Mireille MERCIER

Directrice des projets de Place et moyens de paiement
Office de coordination bancaire et financière (OCBF)

Caroline GAYE

Directrice générale
American Express France (Amex)

Violette BOUVERET

Vice-présidente *Cyber & Intelligence*
MasterCard France

Philippe LAULANIE

Administrateur
Groupement des cartes bancaires (GCB)

Jean-Paul ALBERT

Directeur de la monétique
Société Générale

Évelyne BOTTOLIER-CURTET

Card scheme relationships manager
Groupe BPCE

Romain BOISSON

Directeur régional
Visa Europe France

Jérôme RAGUÉNÈS

Directeur du département Numérique,
Paievements et Résilience opérationnelle
Fédération bancaire française (FBF)

Jean-Marie VALLÉE

Directeur général
STET

Marie-Anne LIVI

Directrice – Stratégie et relations de place
Crédit Agricole

REPRÉSENTANTS DES ENTREPRISES

Bernard COHEN-HADAD

Président de la Commission financement des entreprises
Confédération des petites et moyennes entreprises (CPME)

Émilie TISON

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

Isabelle CHARLIER

Présidente de la Commission monétique et moyens de paiement
Association française des trésoriers d'entreprise (AFTE)

**REPRÉSENTANTS DU COLLÈGE « CONSOMMATEURS »
DU CONSEIL NATIONAL DE LA CONSOMMATION**

Mélissa HOWARD

Juriste

Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN

Juriste

Union nationale des associations familiales (Unaf)

Xavier KRUGER

Chargé de mission banque-assurance

UFC – Que choisir

Hervé MONDANGE

Juriste

Association Force ouvrière consommateurs (Afoc)

Bernard FILLIAT

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

**REPRÉSENTANTS DES ORGANISATIONS PROFESSIONNELLES
DE COMMERÇANTS**

Bertrand PINEAU

Délégué général

Mercatel

Isabelle CLAIRAC

Directrice générale de Market Pay

Fédération du commerce et de la distribution (FCD)

Philippe JOGUET

Correspondant sur les questions financières

Conseil du commerce de France (CdCF)

Marc LOLIVIER

Délégué général

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

Magalie CARRÉ

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

PERSONNALITÉS QUALIFIÉES EN RAISON DE LEURS COMPÉTENCES

Églantine DELMAS

Directeur général des opérations France

Worldline

David NACCACHE

Professeur

École normale supérieure (ENS)

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 désormais 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.). L'Observatoire de la sécurité des cartes de paiement avait par exemple estimé dans son rapport annuel 2015² que l'impact des mesures de cette nature réduisait de 5 % l'estimation brute de la fraude pour les paiements par carte.

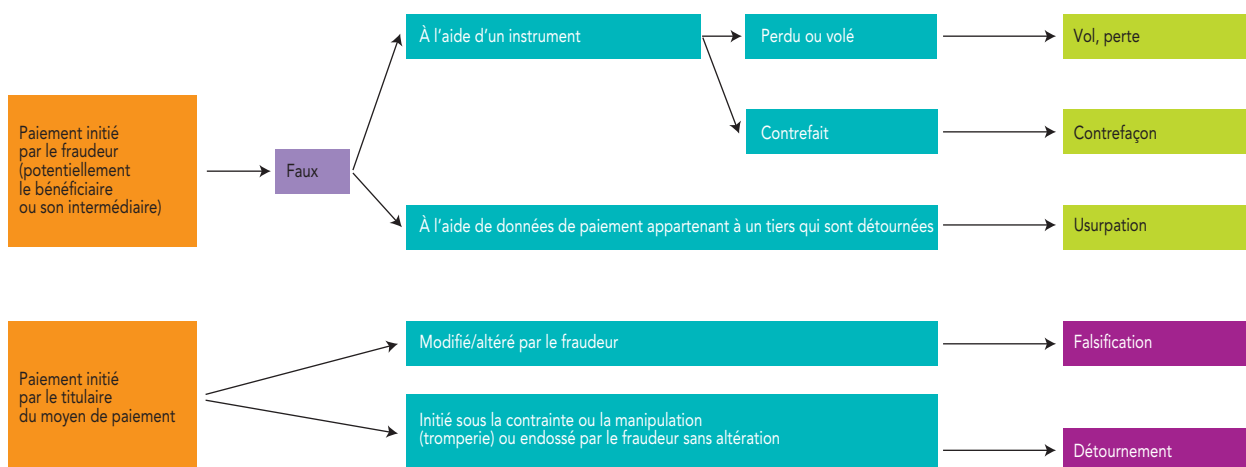
Origine des données de fraude

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 »).

² Cf. *Rapport annuel de l'Observatoire de la sécurité des cartes de paiement 2015* (page 12).

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 ;
- **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 (interbancaire³ ou privatif⁴) 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 :

- des membres du Groupement des cartes bancaires CB, de MasterCard, de Visa Europe et de UnionPay par l'intermédiaire de ceux-ci ;
- 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.

³ 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.

⁴ 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.
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), la manipulation du payeur ayant pour effet d'obtenir un paiement par carte (détournement), 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
Paie ment de proximité et sur automate	Paie ment réalisé au point de vente ou sur automate, y compris le paie ment en mode sans contact.
Paie ment à distance (hors Internet)	Paie ment réalisé par courrier, postal ou électronique (courriel), ou par fax/téléphone, souvent qualifié de paie ment MOTO par les systèmes de paie ment par carte pour « <i>Mail Order, Telephone Order</i> ».
Paie ment sur Internet	Paie ment 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 3D-Secure avec authentification forte	Paiement réalisé sur Internet au travers de l'infrastructure 3D-Secure avec une authentification forte du porteur.
Paiement 3D-Secure sans authentification forte	Paiement réalisé sur Internet au travers de l'infrastructure 3D-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 – <i>one time password</i> – seul) sont également comprises dans cette catégorie.
Paiement non authentifié	Tout paiement réalisé en dehors de l'infrastructure 3D-Secure, recouvrant : • paiement non assujéti 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 : <i>Merchant Initiated Transaction</i> – MIT) et le paiement dit « <i>One leg</i> » (l'émetteur ou l'acquéreur du paiement est situé hors de l'Union européenne); • paiement assujéti 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 assujéti 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 paiement⁵ 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.

5 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 (<i>phishing</i> , <i>malware</i> , 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 (<i>Electronic Banking Internet Communication Standard</i> , 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 (<i>international bank account number</i>) 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 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.



Des tableaux complémentaires, ainsi que l'ensemble des tableaux contenus dans cette annexe, sont disponibles pour téléchargement à l'adresse suivante :
<https://www.banque-france.fr/dossier-statistique-2022-annexe-5-du-rapport-annuel>

PANORAMA DES MOYENS DE PAIEMENT

T1 Cartographie des moyens de paiement scripturaux en 2022

(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
	2022	Variation 2022/2021	Part	2022	Variation 2022/2021	Part	
Paiement carte ^{a)}	18 258	13,2	59,6	746	13,0	1,8	41
<i>dont sans contact</i>	9 103	23,5	29,7	148	18,3	0,3	16
<i>dont paiement par mobile</i>	845	136,5	2,8	18	136,1	0,0	21
Chèque	1 008	- 8,8	3,3	540	- 8,3	1,3	536
Virement	5 158	6,5	16,8	38 895	0,4	91,4	7 541
<i>dont VGM ^{b)}</i>	19	114,1	0,1	15 908	- 19,1	37,4	825 710
<i>dont virement instantané (SCT Inst)</i>	198	84,8	0,6	119	137,7	0,3	601
Prélèvement	4 914	- 2,1	16,0	2 041	7,7	4,8	415
Effet de commerce	75	0,0	0,2	222	4,8	0,5	2 949
Monnaie électronique	75	18,7	0,2	1	- 39,3	0,0	7
Transmission de fonds	3	74,7	0,0	1	- 32,9	0,0	241
Total	29 491	8,3	96,3	42 445	0,9	99,7	1 439
Retrait par carte ^{a)}	1 136	4,5	3,7	133	7,3	0,3	117
Total transactions	30 627	8,1	100,0	42 578	0,9	100,0	1 390

a) Cartes émises en France uniquement.

b) VGM : virement de gros montant émis au travers de systèmes de paiement de montant élevé (Target 2, Euro1), correspondant exclusivement à des paiements professionnels.

Source : Observatoire de la sécurité des moyens de paiement.

T2 Évolution historique des paiements scripturaux

a) En volume
(en millions de transactions)

	2016	2017	2018	2019	2020	2021	2022
Carte	11 134	12 581	13 179	14 485	13 852	16 129	18 258
<i>dont sans contact</i>	635	1 300	2 374	3 779	5 159	7 369	9 103
<i>dont par mobile</i>	0	5	11	48	129	357	845
Chèque	2 137	1 927	1 747	1 587	1 175	1 106	1 008
Virement	3 753	3 870	4 038	4 269	4 483	4 843	5 158
<i>dont virement instantané (SCT inst)</i>	nd	nd	0	14	45	107	198
Prélèvement	3 963	4 091	4 211	4 370	4 622	5 020	4 914
Effet de commerce	82	81	81	78	71	75	75
Monnaie électronique	38	55	65	62	36	63	75
Transmission de fonds	20	18	16	16	15	2	3
Total paiements scripturaux	21 107	22 605	23 320	24 851	24 238	27 238	29 491
Retrait par carte	1 491	1 481	1 439	1 392	1 064	1 086	1 136

b) En montant
(en milliards d'euros)

	2016	2017	2018	2019	2020	2021	2022
Carte	499	530	568	600	578	660	746
<i>dont sans contact</i>	7	13	25	43	80	125	148
<i>dont par mobile</i>	0,005	0,1	0,2	1	3	8	18
Chèque	1 077	1 002	891	814	614	589	540
Virement	23 697	24 069	24 296	25 164	32 712	38 723	38 895
<i>dont virement instantané (SCT Inst)</i>	nd	nd	0,086	7	27	50	119
Prélèvement	1 492	1 579	1 645	1 711	1 684	1 895	2 041
Effet de commerce	266	260	252	232	197	212	222
Monnaie électronique	1	1	1	1	1	1	1
Transmission de fonds	0,8	1,6	2	2	2	1	1
Total paiements scripturaux	27 032	27 440	27 653	28 522	35 786	42 081	42 445
Retrait par carte	129	135	137	137	116	124	133

Note : nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T3 Répartition de la fraude sur les moyens de paiement en 2022

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

	Volume			Valeur			Taux de fraude	Montant moyen
	2022	Variation 2022/2021	Part	2022	Variation 2022/2021	Part	2022	
Paiement carte ^{a)}	6 692 988	-1,1	93,4	420 585 823	-0,2	35,3	0,056	63
<i>dont sans contact</i>	796 027	31,7	11,1	23 047 180	41,6	1,9	0,016	29
<i>dont par mobile</i>	162 869	95,6	2,3	10 942 984	95,1	0,9	0,061	67
Chèque (nouvelle approche) ^{b)}	218 122	-6,1	3,0	395 416 196	-15,0	33,2	0,073	1 813
Chèque (ancienne approche)	266 216	-2,5	3,7	556 796 815	-11,0	46,7	0,103	2 092
Virement	76 846	64,5	1,1	313 163 442	9,0	26,3	0,001	4 075
<i>dont virement instantané (SCT inst)</i>	33 193	157,1	0,5	52 768 218	135,5	4,4	0,044	1 590
Prélèvement	49 453	-80,3	0,7	19 853 012	-21,6	1,7	0,001	401
Effet de commerce	1	0,0	0,0	12 079	0,0	0,0	0,000	12 079
Monnaie électronique	1 945	-2,8	0,0	77 349	-43,7	0,0	0,015	40
Transmission de fonds	154	-84,0	0,0	77 162	-68,7	0,0	0,009	501
Total paiements	7 039 509	-3,5	98,3	1 149 185 062	-4,2	96,4	0,003	163
Retrait par carte ^{a)}	123 574	-4,3	1,7	43 148 054	0,5	3,6	0,032	349
Total transactions	7 163 083	-3,6	100,0	1 192 333 116	-4,0	100,0	0,003	166

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.

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)

	2016	2017	2018	2019	2020	2021	2022
Carte	5 300 847	5 364 312	6 068 959	7 071 095	7 421 137	6 764 752	6 692 988
<i>dont sans contact</i>	125 860	248 991	445 919	603 509	537 061	604 278	796 027
<i>dont par mobile</i>	nd	22	2 070	3 494	33 761	83 266	162 869
Chèque (nouvelle approche)	nd	nd	nd	nd	190 001	232 277	218 122
Chèque (ancienne approche)	120 295	114 906	166 421	183 488	220 685	272 970	266 216
Virement	5 585	4 642	7 736	15 934	35 893	46 718	76 846
<i>dont virement instantané (SCT inst)</i>	nd	nd	5	729	7 131	12 913	33 193
Prélèvement	1 176	25 801	309 377	43 519	6 485	251 010	49 453
Effet de commerce	4	3	5	1	62	1	1
Monnaie électronique	nd	nd	nd	nd	nd	2 001	1 945
Transmission de fonds	nd	nd	nd	nd	nd	962	154
Total fraude paiements scripturaux	5 427 907	5 509 664	6 552 498	7 314 037	7 684 262	7 297 721	7 039 509
Retrait par carte	202 158	177 562	158 908	165 505	113 067	129 083	123 574
Total fraude transactions	5 630 065	5 687 226	6 711 406	7 479 542	7 797 329	7 426 804	7 163 083

b) En valeur
(en euros)

	2016	2017	2018	2019	2020	2021	2022
Carte	378 455 912	344 962 084	401 604 986	428 249 931	439 489 315	421 410 285	420 585 823
<i>dont sans contact</i>	1 410 566	2 748 790	5 234 852	8 479 354	11 292 261	16 274 668	23 047 180
<i>dont par mobile</i>	nd	1 227	73 682	216 236	2 792 574	5 610 270	10 942 984
Chèque (nouvelle approche)	nd	nd	nd	nd	401 611 189	465 021 167	395 416 196
Chèque (ancienne approche)	276 716 554	296 072 847	450 108 464	539 215 175	538 059 139	625 703 442	556 796 815
Virement	86 284 101	78 286 492	97 327 128	161 642 174	266 969 099	287 264 068	313 163 442
<i>dont virement instantané (SCT inst)</i>	nd	nd	29 800	2 203 240	10 562 419	22 406 942	52 768 218
Prélèvement	39 935 882	8 726 403	58 346 253	10 990 025	1 891 051	25 318 677	19 853 012
Effet de commerce	1 018 149	153 100	226 217	74 686	538 918	12 079	12 079
Monnaie électronique	nd	nd	nd	nd	nd	137 340	77 349
Transmission de fonds	nd	nd	nd	nd	nd	246 362	77 162
Total fraude paiements scripturaux	782 410 598	728 200 926	1 007 613 048	1 140 171 991	1 246 947 522	1 199 409 978	1 149 185 062
Retrait par carte	48 650 966	42 038 924	37 630 659	41 651 788	33 950 879	42 950 169	43 148 054
Total fraude transactions	831 061 564	770 239 850	1 045 243 707	1 181 823 779	1 280 898 401	1 242 360 147	1 192 333 116

Notes : 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.
nd, non disponible.

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)

	2017		2018		2019	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	10 969 923	428 693 263	11 222 954	443 193 792	12 171 755	459 066 750
dont paiements sans contact (y compris paiements par mobile)	1 300 071	13 204 448	2 374 029	25 219 537	3 778 756	42 903 452
dont paiements par mobile	4 600	93 204	11 399	200 876	47 885	850 983
Paiements à distance (hors Internet)	48 775	3 627 542	63 021	4 696 704	77 150	4 838 911
Paiements sur Internet	1 562 378	97 393 059	1 893 443	119 903 848	2 236 049	135 352 563
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd
Retraits	1 481 470	134 932 233	1 439 414	136 638 334	1 391 930	136 507 651
Total	14 062 546	664 646 097	14 618 833	704 432 677	15 876 884	735 765 875

Note : 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)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	11 193 795	424 105 649	12 935 438	475 079 750	14 868 338	537 503 850
dont paiements sans contact (y compris paiements par mobile)	5 159 657	79 664 370	7 368 699	125 082 420	9 102 931	148 006 593
dont paiements par mobile	129 105	2 734 667	357 355	7 596 769	845 223	17 937 091
Paiements à distance (hors Internet)	134 114	7 567 877	76 931	7 995 010	105 781	16 994 865
Paiements sur Internet	2 524 317	146 563 476	3 116 285	177 056 237	3 283 604	191 418 128
dont paiements 3D-Secure avec authentification forte	nd	nd	787 664	85 221 641	1 034 950	112 713 734
dont paiements 3D-Secure sans authentification forte	nd	nd	444 723	19 267 910	781 313	27 091 534
dont paiements hors 3D-Secure	nd	nd	1 883 898	72 566 685	1 467 342	51 612 860
Retraits	1 064 095	115 958 207	1 086 289	123 867 648	1 135 675	132 879 066
Total	14 916 322	694 195 208	17 214 942	783 998 644	19 393 398	878 795 909

Note : nd, non disponible.

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)

	2017			2018			2019		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	969 674	59 046 770	0,014	1 142 861	64 546 992	0,015	1 203 233	64 992 145	0,014
dont paiements sans contact (y compris paiements par mobile)	248 991	2 748 790	0,021	445 919	5 234 852	0,021	603 509	8 479 354	0,020
dont paiements par mobile	22	1 227	0,001	2 070	73 682	0,037	3 494	216 236	0,025
Paielements à distance (hors Internet)	360 691	30 621 482	0,844	406 712	28 562 421	0,608	409 319	31 806 788	0,657
Paielements sur Internet	4 033 947	255 293 832	0,262	4 519 386	308 495 573	0,257	5 458 543	331 450 998	0,245
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd	nd	nd	nd
Retraits	177 562	42 038 924	0,031	158 908	37 630 659	0,028	165 505	41 651 788	0,031
Total	5 541 874	387 001 008	0,058	6 227 867	439 235 645	0,062	7 236 600	469 901 719	0,064

Note : 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)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	972 228	47 994 762	0,011	942 376	52 426 587	0,011	1 055 575	62 861 464	0,012
dont paiements sans contact (y compris paiements par mobile)	537 061	11 292 261	0,014	604 278	16 274 668	0,013	796 027	23 047 180	0,016
dont paiements par mobile	33 761	2 792 574	0,102	83 266	5 610 270	0,074	162 869	10 942 984	0,061
Paielements à distance (hors Internet)	411 344	26 899 103	0,355	124 596	22 193 382	0,278	174 364	42 028 102	0,247
Paielements sur Internet	6 037 565	364 595 450	0,249	5 697 780	346 790 316	0,196	5 463 049	315 696 257	0,165
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	496 017	103 029 680	0,121	624 473	124 258 815	0,110
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	364 223	26 046 078	0,135	625 296	25 695 176	0,095
dont paiements hors 3D-Secure	nd	nd	nd	4837 540	217 714 555	0,300	4 213 280	165 742 266	0,321
Retraits	113 067	33 950 879	0,029	129 083	42 950 169	0,035	123 574	43 148 054	0,032
Total	7 534 204	473 440 194	0,068	6 893 835	464 360 454	0,059	6 816 562	463 733 877	0,053

Note : nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2022

(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	866 905	82,1	46 823 896	74,5	13 297	1,3	1 741 496	2,8	83 287	7,9	4 773 344	7,6
dont paiements sans contact (y compris paiements par mobile)	668 928	84,0	16 525 341	71,7	3 742	0,5	61 150	0,3	52 922	6,6	2 551 297	11,1
dont paiements par mobile	86 789	53,3	6 277 156	57,4	229	0,1	7 819	0,1	31 560	19,4	1 713 843	15,7
Paiements à distance (hors Internet)	1 370	0,8	479 506	1,1	47	0,0	13 687	0,0	427	0,2	132 809	0,3
Paiements sur Internet	76 819	1,4	4 743 859	1,5	3 180	0,1	151 727	0,0	55 226	1,0	3 525 928	1,1
dont paiements 3D-Secure avec authentification forte	6 791	1,1	1 147 008	0,9	294	0,0	64 074	0,1	510	0,1	227 034	0,2
dont paiements 3D-Secure sans authentification forte	3 428	0,5	144 810	0,6	305	0,0	6 999	0,0	204	0,0	14 171	0,1
dont paiements hors 3D-Secure	66 600	1,6	3 452 041	2,1	2 581	0,1	80 654	0,0	54 512	1,3	3 284 723	2,0
Retraits	116 493	94,3	41 067 086	95,2	3 663	3,0	1 448 725	3,4	690	0,6	126 506	0,3
Total	1 061 587	15,6	93 114 347	20,1	20 187	0,3	3 355 635	0,7	139 630	2,0	8 558 587	1,8

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2022 (suite)

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

	Numéro de carte usurpé				Autres				Toutes origines	
	Volume		Valeur		Volume		Valeur		Volume	Valeur
	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part		
Paiements de proximité et sur automate	15 936	1,5	1 904 050	3,0	76 150	7,2	7 618 678	12,1	1 055 575	62 861 464
dont paiements sans contact (y compris paiements par mobile)	9 153	1,1	462 310	2,0	61 282	7,7	3 447 082	15,0	796 027	23 047 180
dont paiements par mobile	4 061	2,5	311 402	2,8	40 230	24,7	2 632 764	24,1	162 869	10 942 984
Paiements à distance (hors Internet)	172 272	98,8	41 353 289	98,4	248	0,1	48 811	0,1	174 364	42 028 102
Paiements sur Internet	5 312 602	97,2	304 871 841	96,6	15 222	0,3	2 402 902	0,8	5 463 049	315 696 257
dont paiements 3D-Secure avec authentification forte	615 959	98,6	122 239 678	98,4	919	0,1	581 021	0,5	624 473	124 258 815
dont paiements 3D-Secure sans authentification forte	621 048	99,3	25 491 728	99,2	311	0,0	37 468	0,1	625 296	25 695 176
dont paiements hors 3D-Secure	4 075 595	96,7	157 140 435	94,8	13 992	0,3	1 784 413	1,1	4 213 280	165 742 266
Retraits	325	0,3	39 063	0,1	2 403	1,9	466 674	1,1	123 574	43 148 054
Total	5 501 135	80,7	348 168 243	75,1	94 023	1,4	10 537 065	2,3	6 816 562	463 733 877

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2022

(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
Paielements de proximité et sur automate	989 454	93,7	53 593 598	85,3	40 620	3,8	4 166 195	6,6
dont paiements sans contact (y compris paiements par mobile)	754 985	94,8	20 231 615	87,8	29 368	3,7	1 818 547	7,9
dont paiements par mobile	152 726	93,8	9 566 583	87,4	5 735	3,5	668 917	6,1
Paielements à distance (hors Internet)	120 708	69,2	24 857 056	59,1	30 063	17,2	10 076 248	24,0
Paielements sur Internet	1 874 565	34,3	145 299 292	46,0	2 287 025	41,9	102 735 078	32,5
dont paiements 3D-Secure avec authentification forte	314 967	50,4	72 922 674	58,7	220 335	35,3	39 127 248	31,5
dont paiements 3D-Secure sans authentification forte	342 714	54,8	17 460 124	68,0	204 976	32,8	5 721 496	22,3
dont paiements hors 3D-Secure	1 216 884	28,9	54 916 494	33,1	1 861 714	44,2	57 886 334	34,9
Retraits	115 643	93,6	41 344 934	95,8	2 887	2,3	863 394	2,0
Total	3 100 370	45,5	265 094 880	57,2	2 360 595	34,6	117 840 915	25,4

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2022 (suite)

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

	Transactions internationales				Total	
	Volume		Valeur		Volume	Valeur
	Nombre	Part	Montant	Part		
Paielements de proximité et sur automate	25 501	2,4	5 101 671	8,1	1 055 575	62 861 464
dont paiements sans contact (y compris paiements par mobile)	11 674	1,5	997 018	4,3	796 027	23 047 180
dont paiements par mobile	4 408	2,7	707 484	6,5	162 869	10 942 984
Paielements à distance (hors Internet)	23 593	13,5	7 094 798	16,9	174 364	42 028 102
Paielements sur Internet	1 301 459	23,8	67 661 887	21,4	5 463 049	315 696 257
dont paiements 3D-Secure avec authentification forte	89 171	14,3	12 208 893	9,8	624 473	124 258 815
dont paiements 3D-Secure sans authentification forte	77 606	12,4	2 513 556	9,8	625 296	25 695 176
dont paiements hors 3D-Secure	1 134 682	26,9	52 939 438	31,9	4 213 280	165 742 266
Retraits	5 044	4,1	939 726	2,2	123 574	43 148 054
Total	1 355 597	19,9	80 798 082	17,4	6 816 562	463 733 877

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)

	2017		2018		2019	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	10 645 648	409 574 879	10 864 788	421 977 639	11 774 183	437 193 670
dont paiements sans contact (y compris paiements par mobile)	1 273 939	12 930 723	2 320 822	24 439 724	3 690 364	41 558 002
dont paiements par mobile	4 444	83 492	10 949	190 953	45 249	794 288
Paiements à distance (hors Internet)	26 290	2 072 306	34 893	2 707 270	34 859	2 773 069
Paiements sur Internet	1 268 072	80 134 150	1 515 988	97 756 554	1 768 890	109 593 147
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd
Retraits	1 428 580	128 325 480	1 385 723	129 786 224	1 339 625	130 198 441
Total	13 368 590	620 106 815	13 801 392	652 227 686	14 917 558	679 758 326

Note : 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)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	10 978 602	413 760 411	12 611 966	460 274 895	14 340 211	514 159 801
dont paiements sans contact (y compris paiements par mobile)	5 081 519	78 386 853	7 202 992	121 694 861	8 781 813	141 160 469
dont paiements par mobile	126 945	2 687 300	348 251	7 390 633	808 622	17 132 553
Paiements à distance (hors Internet)	60 243	5 428 918	56 236	5 540 339	87 602	13 259 829
Paiements sur Internet	2 011 431	122 128 921	2 399 865	142 184 895	2 393 161	146 642 890
dont paiements 3D-Secure avec authentification forte	nd	nd	661 960	72 184 112	809 038	88 956 221
dont paiements 3D-Secure sans authentification forte	nd	nd	389 530	15 797 723	717 916	24 981 800
dont paiements hors 3D-Secure	nd	nd	1 348 375	54 203 060	866 207	32 704 868
Retraits	1 038 647	112 337 533	1 056 936	119 485 544	1 101 989	128 161 781
Total	14 088 924	653 655 783	16 125 003	727 485 673	17 922 963	802 224 301

Note : nd, non disponible.

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)

	2017			2018			2019		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	746 547	35 781 960	0,009	977 654	41 383 109	0,010	1 069 418	44 175 058	0,010
dont paiements sans contact (y compris paiements par mobile)	240 293	2 667 829	0,021	426 713	4 967 274	0,020	582 050	7 912 021	0,019
dont paiements par mobile	0	0	0,000	1 717	50 491	0,026	3 215	197 048	0,025
Paielements à distance (hors Internet)	99 860	7 406 798	0,357	159 916	9 512 197	0,351	64 113	7 498 207	0,270
Paielements sur Internet	2 279 763	148 652 859	0,186	2 180 379	163 824 893	0,168	2 630 697	183 067 879	0,167
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd	nd	nd	nd
Retraits	121 686	34 181 829	0,027	109 924	30 893 412	0,024	122 260	35 935 625	0,028
Total	3 247 856	226 023 446	0,036	3 427 873	245 613 611	0,038	3 886 488	270 676 769	0,040

Note : 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)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	793 350	36 280 495	0,009	825 325	43 515 617	0,009	989 454	53 593 598	0,010
dont paiements sans contact (y compris paiements par mobile)	522 873	10 502 092	0,013	576 537	14 002 613	0,012	754 985	20 231 615	0,014
dont paiements par mobile	29 807	2 447 707	0,091	75 039	4 801 997	0,065	152 726	9 566 583	0,056
Paielements à distance (hors Internet)	74 832	8 964 315	0,165	77 941	10 604 251	0,191	120 708	24 857 056	0,187
Paielements sur Internet	2 847 769	212 962 645	0,174	2 577 337	191 873 234	0,135	1 874 565	145 299 292	0,099
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	267 556	69 544 332	0,096	314 967	72 922 674	0,082
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	159 344	11 208 886	0,071	342 714	17 460 124	0,070
dont paiements hors 3D-Secure	nd	nd	nd	2 150 437	111 120 015	0,205	1 216 884	54 916 494	0,168
Retraits	102 962	32 477 429	0,029	121 642	41 437 842	0,035	115 643	41 344 934	0,032
Total	3 818 913	290 684 884	0,044	3 602 245	287 430 944	0,040	3 100 370	265 094 880	0,033

Note : nd, non disponible.

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 2022

(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	720 160 645	40 673 352 376	371 145	35 781 047	0,515	0,088
Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager, etc.)	121 950 525	5 149 814 732	212 055	14 750 850	1,739	0,286
Voyage, transport	238 518 682	21 923 769 597	190 628	17 283 633	0,799	0,079
Téléphonie et communication	401 318 250	14 910 099 186	325 588	15 324 085	0,811	0,103
Alimentation	32 482 983	2 109 085 070	13 718	1 029 111	0,422	0,049
Équipement de la maison, ameublement, bricolage	65 076 308	10 893 000 558	35 615	13 859 215	0,547	0,127
Assurance	12 266 930	2 497 700 204	3 564	529 667	0,291	0,021
Santé, beauté, hygiène	37 868 213	2 428 226 279	25 961	2 307 096	0,686	0,095
Services aux particuliers et aux professionnels	480 090 010	34 617 354 164	635 812	39 595 894	1,324	0,114
Approvisionnement d'un compte, vente de particulier à particulier	121 276 878	11 359 213 472	102 306	20 160 930	0,844	0,177
Jeux en ligne	113 174 813	3 697 908 887	49 613	3 588 319	0,438	0,097
Divers	136 578 925	9 643 194 626	29 268	5 946 501	0,214	0,062
Total	2 480 763 162	159 902 719 151	1 995 273	170 156 348	0,804	0,106

Source : Observatoire de la sécurité des moyens de paiement.

CARTE : ACCEPTATION

T12 Paiements par carte acceptée en France

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

	2017		2018		2019	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	11 076 238	440 943 480	11 286 513	453 608 003	12 277 149	468 895 511
dont paiements sans contact (y compris paiements par mobile)	1 302 753	13 537 550	2 370 247	25 007 584	3 802 953	42 931 374
dont paiements par mobile	6 120	113 383	11 911	209 710	56 169	1 014 657
Paiements à distance (hors Internet)	41 561	4 979 261	50 543	5 757 108	48 998	5 586 755
Paiements sur Internet	1 357 351	90 511 610	1 652 894	112 607 104	1 906 065	121 920 272
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd
Retraits	1 459 903	134 099 783	1 418 919	136 201 131	1 375 145	136 636 741
Total	13 935 054	670 534 135	14 408 869	708 173 346	15 607 358	733 039 279

Note : 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)

	2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	11 284 433	428 180 387	13 031 098	480 804 099	15 093 611	551 753 133
dont paiements sans contact (y compris paiements par mobile)	5 187 488	79 877 184	7 437 197	125 344 168	9 248 429	149 971 446
dont paiements par mobile	145 527	2 979 437	388 175	8 403 747	897 307	19 846 999
Paiements à distance (hors Internet)	69 950	7 087 913	64 620	7 272 724	107 228	18 523 094
Paiements sur Internet	2 158 226	132 554 575	2 565 276	155 816 405	2 589 260	166 197 062
dont paiements 3D-Secure avec authentification forte	nd	nd	708 194	78 650 830	871 961	99 937 461
dont paiements 3D-Secure sans authentification forte	nd	nd	409 008	18 152 505	748 083	27 403 752
dont paiements hors 3D-Secure	nd	nd	1 448 074	59 013 071	969 216	38 855 848
Retraits	1 062 376	116 986 747	1 083 643	125 105 264	1 134 543	134 637 455
Total	14 574 985	684 809 622	16 744 636	768 998 491	18 924 643	871 110 743

Note : nd, non disponible.

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)

	2017			2018			2019		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	837 148	55 604 789	0,0126	1 064 889	58 485 280	0,0129	1 170 399	64 448 538	0,0137
dont paiements sans contact (y compris paiements par mobile)	243 839	2 734 977	0,0202	438 088	5 174 314	0,0207	602 309	8 534 090	0,0199
dont paiements par mobile	377	30 488	0,0269	1 915	64 599	0,0308	3 890	307 230	0,0303
Paielements à distance (hors Internet)	175 974	36 078 041	0,7246	206 957	27 274 865	0,4738	108 259	23 167 505	0,4147
Paielements sur Internet	2 597 284	204 928 799	0,2264	2 537 264	225 819 184	0,2005	2 989 333	232 763 441	0,1909
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	nd	nd	nd	nd	nd	nd
dont paiements hors 3D-Secure	nd	nd	nd	nd	nd	nd	nd	nd	nd
Retraits	127 560	35 741 778	0,0267	114 727	32 353 075	0,0238	127 005	37 354 814	0,0273
Total	3 737 966	332 353 407	0,0496	3 923 837	343 932 404	0,0486	4 394 996	357 734 298	0,0488

Note : 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)

	2020			2021			2022		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paielements de proximité et sur automate	841 280	42 883 367	0,0100	874 166	49 441 754	0,0103	1 084 701	67 409 965	0,0122
dont paiements sans contact (y compris paiements par mobile)	538 313	12 238 895	0,0153	601 803	15 600 613	0,0124	819 535	24 406 015	0,0163
dont paiements par mobile	35 968	3 640 684	0,1222	84 421	5 793 427	0,0689	170 752	12 007 511	0,0605
Paielements à distance (hors Internet)	105 972	17 644 315	0,2489	96 257	15 211 163	0,2092	144 965	35 446 137	0,1914
Paielements sur Internet	3 176 400	248 966 265	0,1878	2 885 920	227 162 875	0,1458	2 252 283	190 461 573	0,1146
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	306 265	76 891 633	0,0978	346 366	80 959 973	0,0810
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	213 403	20 406 481	0,1124	405 445	26 105 266	0,0953
dont paiements hors 3D-Secure	nd	nd	nd	2 366 252	129 864 761	0,2201	1 500 472	83 396 334	0,2146
Retraits	104 960	33 084 175	0,0283	124 077	42 256 276	0,0338	120 217	42 811 637	0,0318
Total	4 228 612	342 578 122	0,0500	3 980 420	334 072 068	0,0434	3 602 166	336 129 312	0,0386

Note : nd, non disponible.

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

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

CHÈQUE

T14 Chèques échangés

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

	2017	2018	2019	2020	2021	2022
Volume	1 926,8	1 746,9	1 586,5	1 175,5	1 105,8	1 008,0
Montant	1 002,0	891,1	814,5	614,2	588,6	539,8
Montant moyen	520,0	510,1	513,4	522,5	532,3	535,5

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

	2017	2018	2019	2020	2021	2022
Volume	114 906	166 421	183 488	220 685	272 970	266 216
Taux de fraude (‰)	0,060	0,095	0,116	0,188	0,247	0,264
Valeur	296 072 847	450 108 464	539 215 175	538 059 139	625 703 442	556 796 815
Taux de fraude (%)	0,030	0,051	0,066	0,088	0,106	0,103
Montant moyen	2 577	2 705	2 939	2 438	2 292	2 092

b) Nouvelle approche

	2017	2018	2019	2020	2021	2022
Volume	nd	nd	nd	190 001	232 277	218 122
Taux de fraude (‰)				0,162	0,210	0,216
Valeur	nd	nd	nd	401 611 189	465 021 167	395 416 196
Taux de fraude (%)				0,065	0,079	0,073
Montant moyen	nd	nd	nd	2 114	2 002	1 813

Notes : L'ancienne approche tenait 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.

nd, non disponible.

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)

	2017		2018		2019		2020		2021		2022	
	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part
Volume												
Vol, perte	89 988	78,3	138 358	83,1	154 211	84,0	196 754	89,2	244 750	89,7	237 854	89,3
Falsification	15 738	13,7	17 178	10,3	16 459	9,0	13 894	6,3	18 074	6,6	18 885	7,1
Contrefaçon	7 234	6,3	8 092	4,9	9 574	5,2	7 207	3,3	5 119	1,9	5 969	2,2
Détournement, rejeu	1 946	1,7	2 793	1,7	3 244	1,8	2 830	1,3	5 026	1,8	3 508	1,3
Valeur												
Vol, perte	130 815 653	44,2	252 890 727	56,2	296 367 562	55,0	365 813 764	68,0	398 739 224	63,7	375 576 575	67,5
Falsification	127 157 212	42,9	145 737 424	32,4	145 881 745	27,1	102 801 337	19,1	100 395 756	16,0	93 152 894	16,7
Contrefaçon	28 097 173	9,5	36 739 051	8,2	76 511 582	14,2	32 340 420	6,0	33 725 041	5,4	32 648 566	5,9
Détournement, rejeu	10 002 809	3,4	14 741 262	3,3	20 454 286	3,8	37 103 618	6,9	92 823 421	14,8	55 418 781	10,0

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.

VIREMENT

T17 Virements émis par type de virements

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

	2017		2018		2019		2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	3 870	24 069 448	4 038	24 211 142	4 251	25 879 217	4 483	32 713 128	4 843	38 722 734	5 158	38 894 879
dont virements SEPA – SCT	3 801	9 259 478	3 974	10 846 914	4 174	9 602 866	4 384	10 029 108	4 668	12 980 883	4 689	9 655 892
dont virements SEPA instantanés – SCT Inst	nd	nd	0	86	14	7 074	45	26 243	107	50 053	198	118 972
dont virements de gros montants – VGM ^{a)}	10	9 483 487	10	10 130 586	9	12 266 316	9	19 042 030	9	19 661 685	19	15 907 892
dont autres virements	59	5 326 483	53	3 233 556	54	4 002 960	45	3 615 748	59	6 030 114	252	13 212 124
Total – hors VGM	3 860	14 585 961	4 028	14 080 556	4 242	13 612 900	4 474	13 671 098	4 834	19 061 050	5 138	22 986 988

a) Il s'agit des virements de gros montant effectués via Target 2 ou Euro1.

Note : SEPA – Single Euro Payments Area, espace unique de paiement en euros ; nd – non disponible.

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 virements

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

	2017			2018			2019		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	4 642	78 286 492	0,0003	7 736	97 327 128	0,0004	15 934	161 642 174	0,0006
dont virements SEPA – SCT	nd	nd	nd	6 521	78 314 614	0,0007	13 302	127 572 549	0,0013
dont virements SEPA instantanés – SCT Inst	nd	nd	nd	5	29 800	0,0345	729	2 203 240	0,0311
dont virements de gros montants – VGM ^{a)}	nd	nd	nd	14	4 622 598	0,0000	15	15 476 053	0,0001
dont autres virements	nd	nd	nd	1 196	14 360 116	0,0004	1 888	16 390 332	0,0004
Total – hors VGM	nd	nd	nd	7 722	92 704 530	0,0007	15 919	146 166 121	0,0011

a) Il s'agit des virements de gros montant effectués via Target 2 ou Euro1.

Note : SEPA – Single Euro Payments Area, espace unique de paiement en euros.

Source : Observatoire de la sécurité des moyens de paiement.

T18 Transactions frauduleuses par type de virements (suite)

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

	2020			2021			2022		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	35 893	266 969 099	0,0008	46 718	287 264 068	0,0007	76 846	313 163 442	0,0008
dont virements SEPA – SCT	25 254	191 474 396	0,0019	33 199	246 527 533	0,0019	40 874	205 737 587	0,0021
dont virements SEPA instantanés – SCT Inst	7 131	10 562 419	0,0402	12 913	22 406 942	0,0448	33 193	52 768 218	0,0444
dont virements de gros montants – VGM ^{a)}	51	2 439 224	0,0000	5	1 539 120	0,0000	49	19 347 774	0,0000
dont autres virements	3 457	62 493 060	0,0017	601	16 790 473	0,0003	2 730	52 722 863	0,0004
Total – hors VGM	35 842	264 529 875	0,0019	46 713	286 724 913	0,0015	76 797	311 228 668	0,0014

a) Il s'agit des virements de gros montant effectués via Target 2 ou Euro1.

Note : SEPA – Single Euro Payments Area, espace unique de paiement en euros.

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)

	2017	2018	2019	2020	2021	2022
Volume	4 642	7 736	15 934	35 893	46 718	76 846
Taux (‰)	0,0012	0,0019	0,0037	0,0080	0,0096	0,0149
Valeur	78 286 492	97 327 128	161 642 174	266 969 099	287 264 068	313 163 442
Taux (%)	0,0003	0,0004	0,0006	0,0008	0,0007	0,0008
Montant moyen	16 865	12 581	10 144	7 438	6 149	4 075

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)

	2017		2018		2019		2020		2021		2022	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	3 803	42 008 522	5 525	51 069 661	13 769	98 525 485	28 211	87 061 255	35 865	87 370 131	57 443	120 006 990
Part	81,9	53,7	71,4	52,5	86,4	61,0	78,6	32,6	76,8	30,4	74,8	38,3
Falsification	57	1 304 143	151	485 131	125	3 438 923	203	3 377 807	875	5 387 862	179	2 838 371
Part	1,2	1,7	2,0	0,5	1,6	2,1	0,6	1,3	1,9	1,9	0,2	0,9
Détournement	464	32 966 084	1 037	40 250 639	1 534	56 514 755	5 731	157 318 883	8 523	168 094 274	16 991	148 732 203
Part	10,0	42,1	13,4	41,4	19,8	35,0	16,0	58,9	18,2	58,5	22,1	47,5
Autres ^{a)}	318	2 007 743	1 023	5 521 697	506	3 163 011	1 748	19 211 154	1 455	26 411 801	2 233	41 585 878
Part	6,9	2,6	13,2	5,7	3,2	2,0	4,9	7,2	3,1	9,2	2,9	13,3

a) La catégorie « autres » regroupe en 2021 les fraudes sur les virements initiés par voie non électronique (courrier, téléphone, etc.).

Source : Observatoire de la sécurité des moyens de paiement.

PRÉLÈVEMENT

T21 Prélèvements émis par type de mandat

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

	2017		2018		2019		2020		2021		2022	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	4 091	1 578 653	4 211	1 644 553	4 370	1 710 931	4 622	1 684 258	5 020	1 895 098	4 914	2 040 963
Prélèvements par type de mandat												
dont prélèvements consentis par mandat électronique	nd	nd	nd	nd	nd	nd	nd	nd	1 106	430 781	1 357	1 045 754
dont prélèvements consentis par mandat papier	nd	nd	nd	nd	nd	nd	nd	nd	3 914	1 464 317	3 558	995 210
Prélèvements par mode d'initiation												
												Volume Valeur
dont prélèvements initiés dans un fichier/lot	4 029	1 526 056	4 151	1 609 405	4 312	1 672 338	4 560	1 647 504	4 936	1 819 420	4 645	1 929 438
dont prélèvements initiés sur la base d'un paiement unique	63	52 596	60	35 148	58	38 593	61	36 754	84	75 678	269	111 525

Note : 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)

	2017	2018	2019	2020	2021	2022
Volume	25 801	309 377	43 519	6 485	251 010	49 453
Taux de fraude (‰)	0,0063	0,0735	0,0100	0,0014	0,0500	0,0101
Valeur	8 726 403	58 346 253	10 990 025	1 891 051	25 318 677	19 853 012
Taux de fraude (%)	0,0006	0,0035	0,0006	0,0001	0,0013	0,0010
Montant moyen	338	189	253	292	101	401

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)

	2017		2018		2019		2020		2021		2022	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	23 943	6 141 836	309 302	58 329 283	14 601	3 961 260	6 011	1 388 326	250 493	25 201 709	43 788	14 206 533
Part	92,8	70,4	100,0	100,0	33,6	36,0	92,7	73,4	99,8	99,5	88,5	71,6
Détournement	1 832	2 305 112	72	16 703	26 223	6 677 467	62	10 720	517	116 968	5 665	5 646 479
Part	7,1	26,4	0,0	0,0	60,3	60,8	1,0	0,6	0,2	0,5	11,5	28,4

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 jusqu'en 2020.

Source : Observatoire de la sécurité des moyens de paiement.

AUTRES

Monnaie électronique

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

 T25 Usage de la monnaie électronique par typologie de transaction

 T26 Transactions frauduleuses par monnaie électronique

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

 T27 Paiements par LCR et BOR

 T28 Typologie de la fraude aux LCR et BOR

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

Alexandre Stervinou

Directeur des Études et de la Surveillance des paiements

Banque de France

Secrétariat de rédaction

Pierre Bienvenu, Aurélie Barberet, Véronique Bugaj,
Caroline Corcy, Yolaine Fischer, Anne-Marie Fourel,
Trân Huynh, Marc-Antoine Jambu, Julien Lasalle,
Ibtissam Lesca, Isabelle Maranghi, Marine Soubielle

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

Banque de France – SG - DISG

Dépôt légal

Juillet 2023

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).



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

© Observatoire de la sécurité des moyens de paiement – 2023