OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2021

BANQUE DE FRANCE
EUROSYSTÈME

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2021

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 2022

SOMMAIRE

SYNTHÈSE

Après une année 2020 marquée par les mesures sanitaires, 2021 a été l'année de la reprise économique et du rebond sous-jacent des flux de paiement, avec la confirmation de nouvelles habitudes des consommateurs, plus numériques et dématérialisées, qui se sont durablement installées. Dans ce rapport annuel 2021, l'Observatoire de la sécurité des moyens de paiement constate que cette numérisation des usages s'accompagne de nouvelles menaces sur les moyens de paiement, avec une croissance marquée des escroqueries et des modes opératoires reposant sur la manipulation. Dans ce contexte, les actions engagées par l'Observatoire et les professionnels des paiements, conjuguées à la vigilance des utilisateurs, ont permis de préserver en 2021 un haut niveau de sécurité et de confiance dans les moyens de paiement scripturaux.

Le chapitre 1 du rapport présente les évolutions des flux et de la fraude aux moyens de paiement en 2021. *L'assouplissement des mesures sanitaires et la reprise économique associée ont engendré une très forte croissance des transactions scripturales (+ 12,4 % en nombre, + 17,5 % en montant), supérieure à la croissance économique, confirmant ainsi la numérisation rapide et durable des usages de paiement :*

- *La carte bancaire conforte son statut de principal moyen de paiement, avec près de 61 % du nombre total d'opérations scripturales. Avec la pandémie, le sans contact est devenu le mode de paiement favori des Français en magasin, représentant désormais plus de la moitié des transactions par carte en proximité (57 %). Le paiement sans contact par mobile, même s'il reste encore limité à 3 % des opérations en magasin, a également vu ses flux tripler en 2021, laissant présager une forte hausse de cet usage dans les années à venir. Enfin, le paiement par Internet a continué sa progression dynamique (+ 21 % en 2021), toujours porté par la croissance du commerce électronique et des nouveaux modes de consommation (retraits en magasins d'achats effectués à distance comme le* drive *ou le* click & collect*, livraisons à domicile du* quick commerce [1]*, abonnements en ligne, etc.) ;*

- *À côté de la carte bancaire, le virement instantané s'installe également dans le paysage des moyens de paiement scripturaux. Son utilisation a plus que doublé en 2021, représentant désormais plus de 2 % du total des virements. Certes encore en retrait par rapport à d'autres pays européens, son usage en France est résolument appelé à croître dans les prochaines années, en lien avec les stratégies nationale et européenne sur les moyens de paiement ;*

- *En parallèle, malgré la reprise économique, les moyens de paiement traditionnels restent en repli. Le chèque poursuit sa décrue, qui est certes moins forte qu'avant la pandémie, avec un recul de 6 % du nombre de transactions et de 4 % des montants échangés. Avec l'assouplissement des mesures sanitaires, les retraits d'espèces par carte résistent mieux (+ 2,1 % en nombre), leur croissance étant toutefois inférieure à celle du total des transactions.*

Dans ce contexte de très forte hausse des transactions scripturales, en partie liée à un effet de rattrapage après une année 2020 atypique, le suivi statistique de l'Observatoire montre que la fraude observée sur les paiements émis en France progresse en valeur à un rythme deux fois inférieur aux flux pour atteindre 1,2 milliard d'euros (+ 8,5 %), et diminue en nombre pour s'établir à 7,5 millions de

1 Le *quick commerce* correspond aux achats sur Internet – généralement au moyen d'un téléphone mobile – associés à une promesse de livraison très rapide à domicile, de quelques minutes à quelques heures. Le *quick commerce* s'est notamment développé dans le secteur alimentaire.

transactions fraudées (– 3,8 %). Ce résultat encourageant reflète différentes tendances selon les moyens de paiement :

- *Pour la quatrième année consécutive, le chèque reste le moyen de paiement le plus fraudé avec un taux de fraude de 0,079 %. Il concentre 37 % des montants de fraude en 2021, soit 465 millions d'euros. Ces chiffres reflètent une nouvelle approche de la fraude au chèque, plus proche de la réalité des préjudices subis, dans la mesure où l'Observatoire tient désormais compte des tentatives de fraudes qui sont déjouées par les établissements bancaires après la remise du chèque (161 millions d'euros de fraudes déjouées en 2021 à soustraire de 626 millions d'euros d'opérations frauduleuses par chèque) ;*

- *La carte est très proche du chèque en matière de montants fraudés : 37 % du montant global de la fraude en 2021 pour 464 millions d'euros. Dans un contexte de progression de l'usage de ce moyen de paiement, l'année 2021 marque néanmoins un recul sensible de la fraude en montant (– 1,9 %) et en taux de fraude (0,059 %, après 0,068 % en 2020). L'Observatoire recense ainsi 1,3 million de carte fraudées et mises en opposition en 2021, en recul de 10 % par rapport à 2020. Ces résultats confirment l'efficacité du recours à l'authentification forte pour les paiements à distance, prévu par la deuxième directive européenne sur les services de paiement (DSP 2), et qui s'est progressivement déployé en France en 2021 dans le cadre du plan de migration piloté par l'Observatoire. Ainsi, le taux de fraude sur les paiements à distance chute de 0,249 % en 2020 à 0,196 % en 2021 (– 21 %), soit son plus bas niveau historique. Avec des risques d'hameçonnage toujours élevés, les numéros de cartes usurpées restent cependant la principale source de fraude à la carte (78 % de la fraude, contre 18 % pour les cartes perdues ou volées), si bien que les paiements sur Internet supportent encore près des trois quarts de la fraude en montant alors qu'ils représentent moins d'un quart des paiements par carte. Dans le même temps, les paiements sans contact confirment leur très haut niveau de sécurité, leur taux de fraude atteignant un plus bas historique de 0,013 %, quasiment équivalent au taux de 0,010 % mesuré pour les paiements de proximité traditionnels avec saisie du code confidentiel ;*

- *Le virement reste le troisième moyen de paiement le plus fraudé (23 % des montants de fraude avec 287 millions d'euros). Toutefois, dans un contexte de progression des flux et d'utilisation privilégiée du virement pour les paiements de masse (salaires, prestations sociales etc.), le taux de fraude par virement reste particulièrement faible et maîtrisé à 0,0007 % (0,0015 % hors virements de gros montant), en légère baisse par rapport à 2020. La maîtrise des taux de fraude est à la fois observée pour les virements de banque en ligne, principalement utilisés par les particuliers (0,0012 %) et pour les virements par canaux télématiques, utilisés par les entreprises et les administrations publiques (0,0006 %). Par ailleurs, dans un contexte de forte hausse des flux, la sécurité du virement instantané reste préservée avec un taux de fraude en légère hausse à 0,045 %, très proche des paiements par carte en France. L'Observatoire note que les détournements de virements, caractérisant des situations où l'initiateur de l'opération est légitime, mais agit sous la manipulation ou la tromperie du fraudeur, sont confirmés comme la première typologie de fraude (59 % des montants fraudés). Ces cas de fraude touchent aussi bien les entreprises, les administrations publiques que les particuliers, les fraudeurs parvenant ainsi à déjouer les mécanismes d'authentification. L'expansion durable des interactions à distance et les usurpations d'identité ou de coordonnées bancaires sont propices à la manipulation directe des utilisateurs qu'il faut continuer de sensibiliser à ces risques. Compte tenu de ces risques, l'Observatoire participera activement aux réflexions visant à identifier de nouveaux leviers de lutte contre la fraude au virement, au bénéfice des établissements bancaires et des utilisateurs ;*

- *Derrière ces trois moyens de paiement, les montants de fraude affectant le prélèvement, les effets de commerce, la monnaie électronique et la transmission de fonds sont relativement négligeables. L'Observatoire constate toutefois une hausse de la fraude au prélèvement, qui a représenté 25 millions d'euros en 2021, contre moins de 2 millions d'euros en 2020, et dont le taux de fraude (0,0013 %) est particulièrement volatil d'une année sur l'autre au cours des quatre dernières années. L'origine de cette hausse, imputable à un nombre très réduit de créanciers, a été identifiée. Des mesures correctives sont mises en œuvre pour y remédier.*

Le chapitre 2 dresse un bilan positif des actions menées par l'Observatoire en 2021 pour renforcer la sécurité des moyens de paiement :

- *Il s'agit tout d'abord du déploiement des mesures d'authentification forte pour les paiements par carte sur Internet, qui a été piloté par l'Observatoire depuis la publication de son plan de migration pour la Place française à l'automne 2019 (voir rapport annuel 2018). L'Observatoire relève avec satisfaction que la Place française a atteint un très haut niveau de conformité aux exigences posées par la DSP 2, à la fois en matière d'équipement des porteurs et de*

traitement des transactions par les commerçants et la chaîne d'acquisition. L'Observatoire se félicite que ces mesures d'authentification forte aient d'ores et déjà permis de faire baisser sensiblement la fraude pour les paiements sur Internet, tout en accompagnant la croissance du commerce électronique et des nouveaux modes de consommation liés. En 2022, l'Observatoire s'attachera à consolider le fonctionnement de ces nouvelles infrastructures d'authentification, tout en continuant à agir contre les fraudes visant à contourner l'authentification forte par manipulation du payeur ;

- *Un an après la publication de dix nouvelles recommandations sur la sécurité du chèque (voir rapport annuel 2020), l'Observatoire dresse un premier point d'étape encourageant avec la réalisation de plusieurs actions concrètes tant du côté des autorités publiques que du côté des professionnels de la filière, avec par exemple la révision du référentiel de sécurité du chèque de la Banque de France, aboutie en avril 2022. Toutefois, au regard des niveaux toujours élevés de fraude, l'Observatoire appelle les acteurs de la filière à poursuivre et amplifier leurs efforts pour renforcer la sécurité de ce moyen de paiement en décroissance, en ciblant notamment la surveillance des opérations par chèque, la simplification des procédures de mise en opposition et la sécurisation de l'acheminement des chéquiers. En tenant compte des contrôles déjà effectués et de la politique de risques de chaque établissement, la Banque de France s'assurera de la bonne mise en œuvre de ses recommandations par les établissements bancaires dans le cadre de ses actions de surveillance ;*

- *L'Observatoire réitère enfin, tant auprès des industriels des paiements que des utilisateurs, la validité de ses recommandations sur certains usages en forte croissance, que l'Observatoire avait couverts par ses travaux de veille au cours des années précédentes. Il s'agit notamment de poursuivre les efforts et les investissements pour renforcer la sécurité des virements instantanés de façon à assurer un développement rapide et sécurisé de ce moyen de paiement appelé à croître fortement, de sensibiliser les utilisateurs dans la protection de leurs propres données de paiement au regard des risques toujours élevés d'hameçonnage, et de renforcer la sécurité des enrôlements pour les solutions de paiement mobile.*

Le chapitre 3 restitue les travaux de veille de l'Observatoire en matière d'identité numérique des personnes physiques. *L'Observatoire constate en effet que la forte croissance des usages numériques ne s'est pas accompagnée d'une mise à niveau équivalente des processus d'identification. Cela a favorisé la croissance des phénomènes d'usurpation d'identité, souvent associés à des techniques de fraude documentaire, qui fragilisent aussi la sécurité des moyens de paiement en trompant l'une des parties à la transaction. Alors que le gouvernement français développe et teste une identité numérique régalienne, associée à la nouvelle carte nationale d'identité électronique, l'Observatoire appelle d'ores et déjà les acteurs de la chaîne des paiements, mais aussi les utilisateurs, à recourir plus largement aux solutions d'identité numérique et aux services de confiance, comme la signature ou le cachet électroniques, qui offrent des niveaux plus robustes de sécurisation des échanges à distance.*

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, qu'ils soient en décroissance, comme le chèque, ou qu'ils soient appelés à se développer dans les années à venir comme le virement instantané ou le paiement mobile. La sécurité de tous les moyens de paiement est la condition pour offrir à tous les utilisateurs, des particuliers aux entreprises, une authentique liberté de choix dans leurs usages au quotidien.

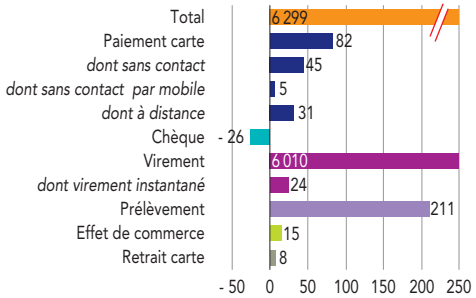
1

ÉTAT DE LA FRAUDE EN 2021

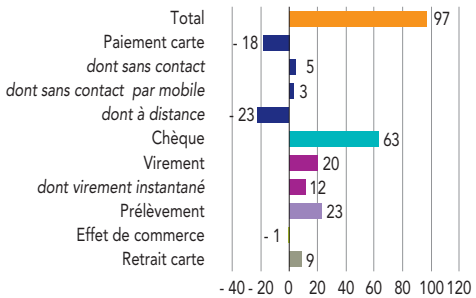
Données clés

G1 Évolution des moyens de paiement entre 2020 et 2021

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



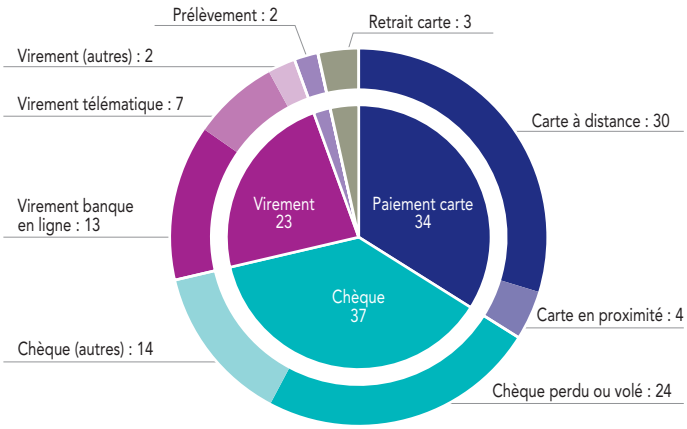
b) Fraude (en millions d'euros)



Note : L'évolution de la fraude entre 2020 et 2021 (graphique b) est présentée ici à méthodologie et périmètre constants, en appliquant notamment sur les deux années la nouvelle approche de mesure de la fraude au chèque.

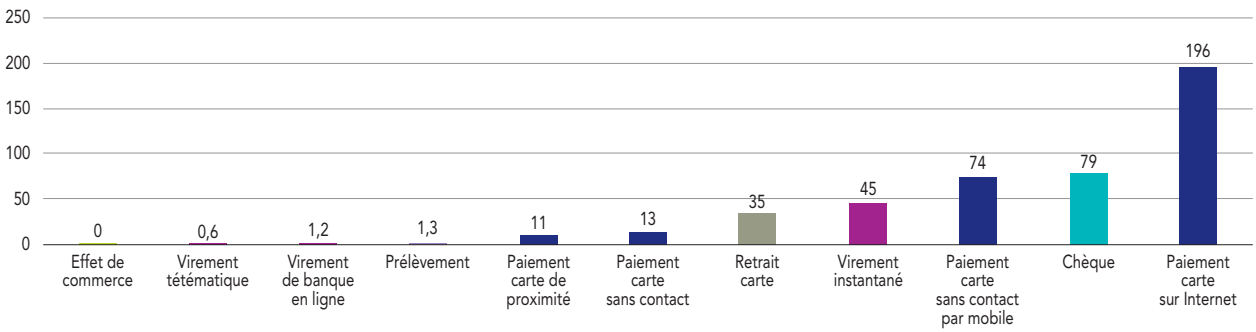
Source : Observatoire de la sécurité des moyens de paiement.

G2 Les principales sources de fraude en montant (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)



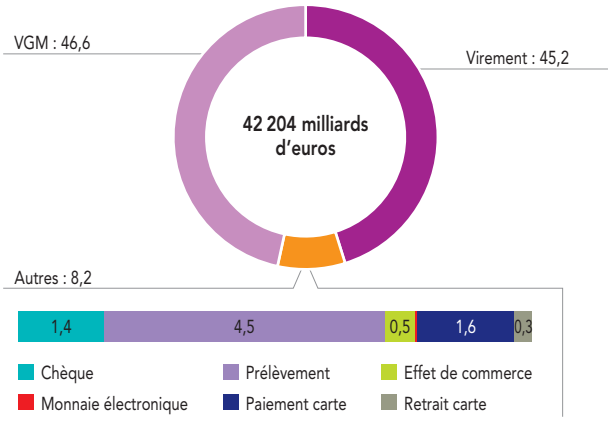
Source : Observatoire de la sécurité des moyens de paiement.

1.1 Vue d'ensemble

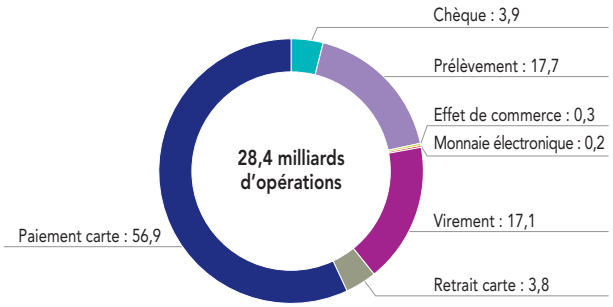
1.1.1 Cartographie des moyens de paiement

G4 Usage des moyens de paiement scripturaux en 2021 (en %)

a) En montant



b) En volume

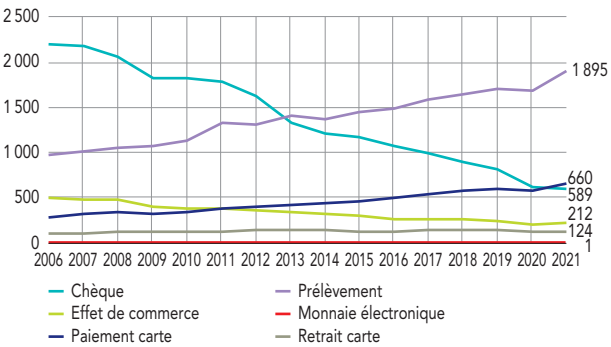


Note : VGM – virement de gros montant.

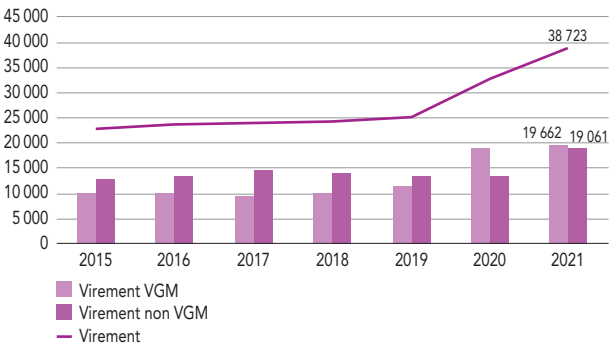
Source : Observatoire de la sécurité des moyens de paiement.

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

a) Par instrument (hors virement)



b) Par virement



Note : VGM – virement de gros montant.

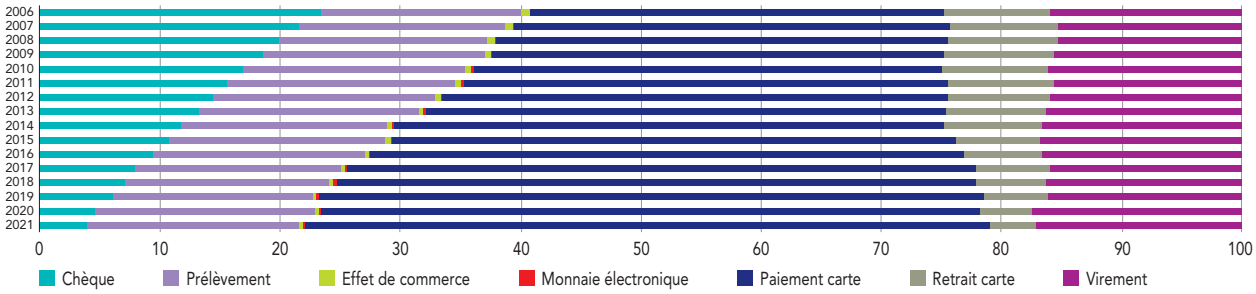
Source : Observatoire de la sécurité des moyens de paiement.

Dans un contexte d'allègement des mesures sanitaires et de reprise économique associée, les opérations scripturales réalisées par les particuliers, les entreprises et les administrations ont atteint 28,4 milliards de transactions en 2021 (+ 12 % par rapport à 2020), pour un total de 42 204 milliards d'euros (+ 17,5 %).

La part des virements dans les flux en montant reste prépondérante, à 92 %. Ceci s'explique principalement par le poids des virements de gros montant (VGM), c'est-à-dire de flux émis au travers de systèmes de paiement de montant élevé (Target 2 et Euro1) réservés à des paiements professionnels. Ces derniers représentent 51 % des montants de virement, pour seulement 0,2 % du nombre de ces transactions.

La carte bancaire conforte son statut de mode de paiement scriptural le plus utilisé en nombre de transactions, et voit sa part, hors retraits par carte, dans les volumes de transactions encore augmenter de 54,7 % en 2020 à 56,9 % en 2021. À l'inverse, le déclin du chèque se poursuit, tant en volume qu'en montant. Pour la première fois en 2021, les paiements par carte ont dépassé en montant les échanges par chèque (660 milliards d'euros, contre 58 milliards d'euros).

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

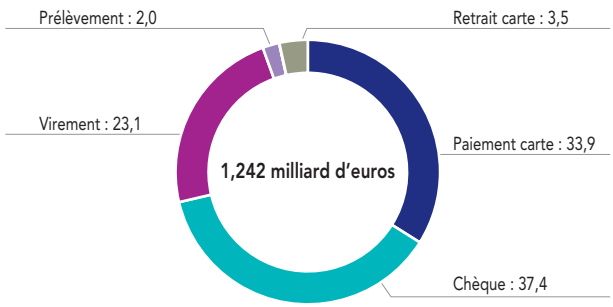


Source : Observatoire de la sécurité des moyens de paiement.

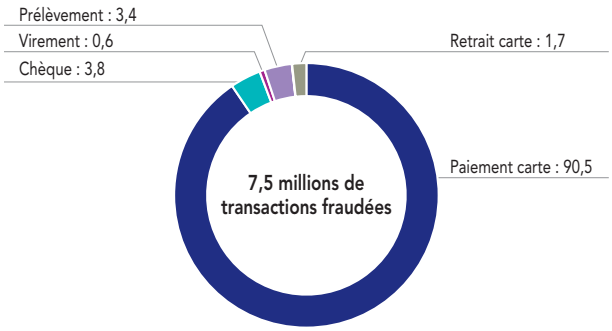
1.1.2 Panorama de la fraude aux moyens de paiement

G7 Répartition de la fraude (en %)

a) En montant

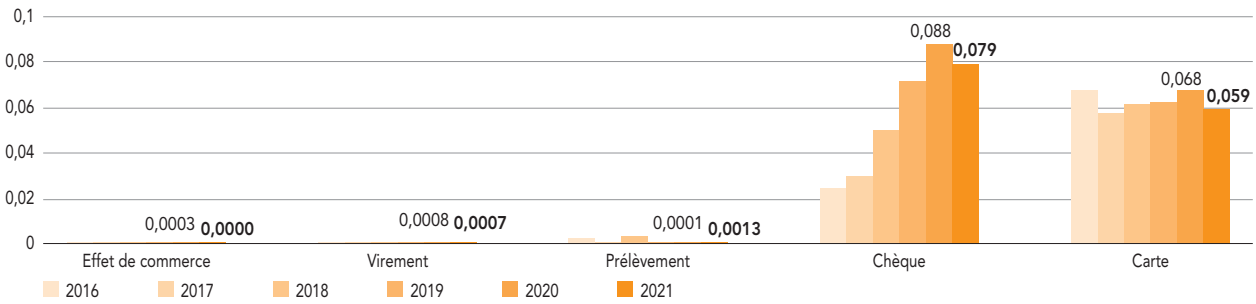


b) En volume



Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

En 2021, la fraude aux transactions scripturales s'est élevée à 1,242 milliard d'euros, en hausse de 8,5 % à méthodologie et périmètre constants, pour 7,5 millions d'opérations frauduleuses, soit un recul de 3,8 % par rapport à 2020.

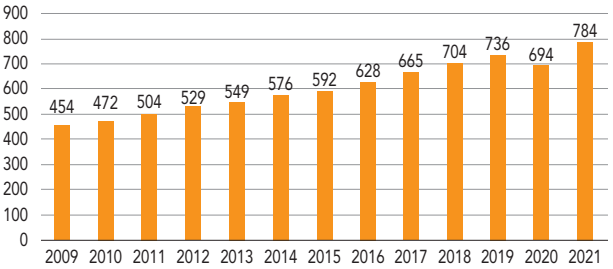
Le chèque reste le moyen de paiement le plus fraudé avec une part dans les montants fraudés qui diminue toutefois à 37 % en 2021 contre 42 % en 2020, en raison d'une nouvelle approche de la fraude plus proche de la réalité des préjudices subis. La part de la carte – retraits compris – reste stable à 37 %, à égalité avec le chèque, malgré une évolution des flux vers les canaux plus risqués de vente sur Internet. La carte – retraits compris – concentre toujours la majeure partie du nombre de transactions fraudées, avec une part qui diminue cependant, passant de 97 % en 2020 à 92 % en 2021.

1.2 État de la fraude sur la carte de paiement

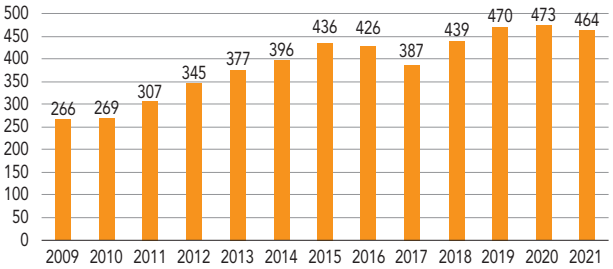
1.2.1 Vue d'ensemble – Cartes émises en France

G9 Les cartes émises en France en 2021

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



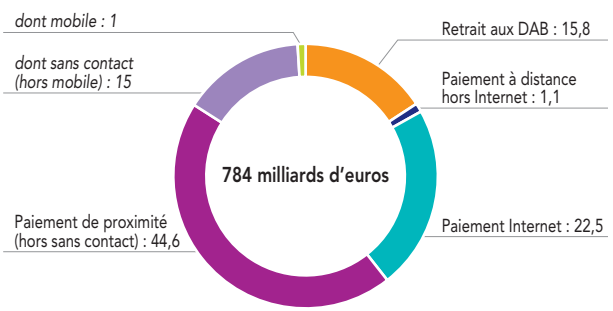
b) Montant total de la fraude (en millions d'euros)



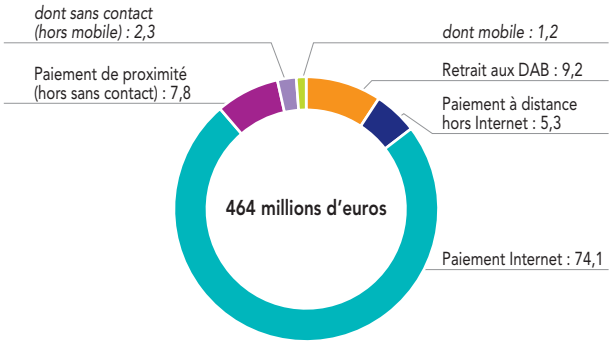
Source : Observatoire de la sécurité des moyens de paiement.

G10 Le canal d'utilisation des cartes émises en France en 2021 (en %)

a) Répartition du montant des opérations



b) Répartition du montant de la fraude



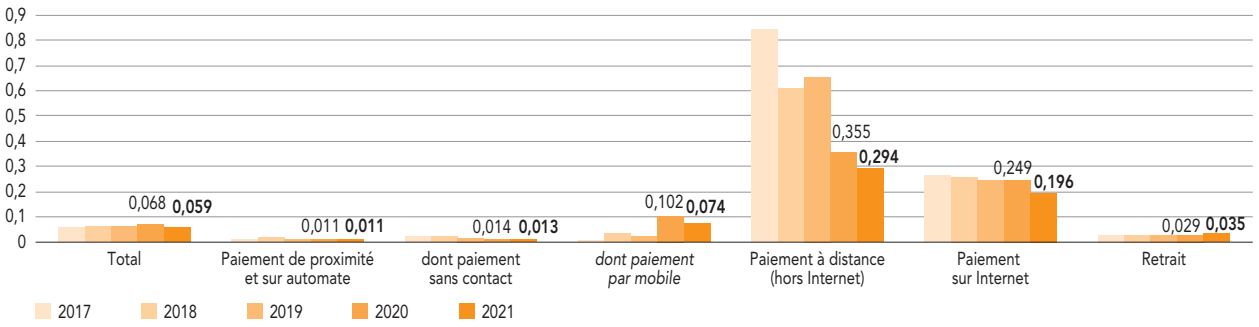
Note : DAB – distributeur automatique de billets.

Source : Observatoire de la sécurité des moyens de paiement.

Après un ralentissement marqué en 2020 du fait de la crise sanitaire, l'assouplissement des restrictions associé au fort développement de l'usage du paiement sans contact ont relancé la dynamique des transactions par cartes. Ainsi, le nombre de flux est en nette progression : + 15,4 % en 2021.

Dans le même temps, le renforcement de la sécurisation, notamment par la généralisation progressive des règles d'authentification forte pour les transactions à distance, a permis de faire décroître de 1,9 % le montant total de la fraude sur les cartes françaises.

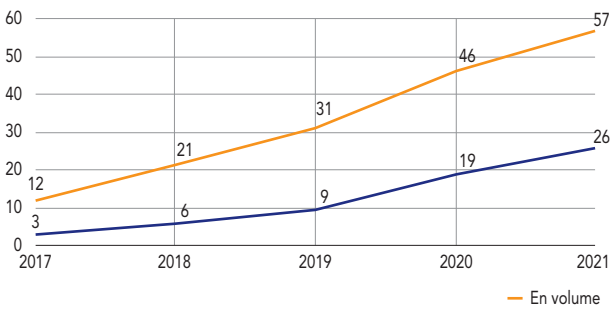
G11 Évolution des taux de fraude en montant sur les cartes françaises par canal d'initiation (en %)



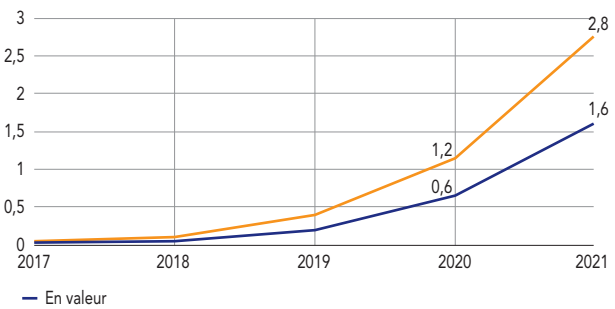
Source : Observatoire de la sécurité des moyens de paiement.

G12 Paiements par carte de proximité (en %)

a) Part des paiements sans contact



b) Part des paiements par mobile



Source : Observatoire de la sécurité des moyens de paiement.

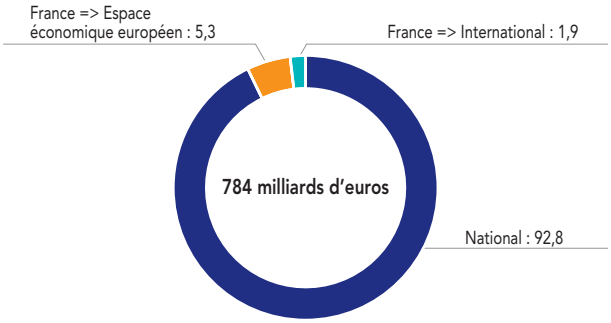
Le taux de fraude sur les transactions par carte émises en France a baissé significativement de 0,068 % en 2020 à 0,059 % en 2021, soit une baisse substantielle de 13 %. Les principaux faits marquants sont :

- La chute sensible du taux de fraude sur les paiements à distance : de 0,249 % en 2020 à 0,196 % en 2021 pour les paiements sur Internet (– 22 %), mais aussi de 0,355 % à 0,294 % pour les paiements à distance hors Internet (– 17 %), soit leur plus bas niveau historique ;
- La fraude sur les paiements sans contact a atteint son plus bas niveau historique : 0,013 %, dans un contexte de forte hausse de leur usage. Parmi eux, le taux de fraude sur le paiement par téléphone mobile reste sensiblement plus élevé mais diminue, passant de 0,102 % en 2020 à 0,074 % en 2021, également dans un contexte de rapide développement. La pandémie a accéléré l'usage du paiement sans contact en proximité, où il est désormais utilisé dans 57 % des transactions pour 26 % des montants. Dans ce mouvement, la part du paiement sans contact par mobile reste modeste mais a triplé en 2021, passant de 1,2 % des paiements de proximité en 2020 à 2,8 % en nombre d'opérations, et de 0,6 % à 1,6 % en montant.

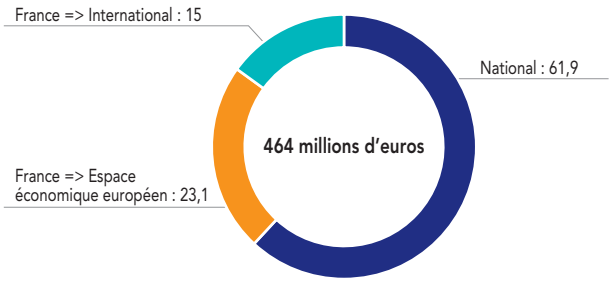
1.2.2 Répartition de la fraude par zone géographique – Cartes émises en France

G13 Cartes émises en France par zone géographique (%)

a) Répartition du montant des opérations

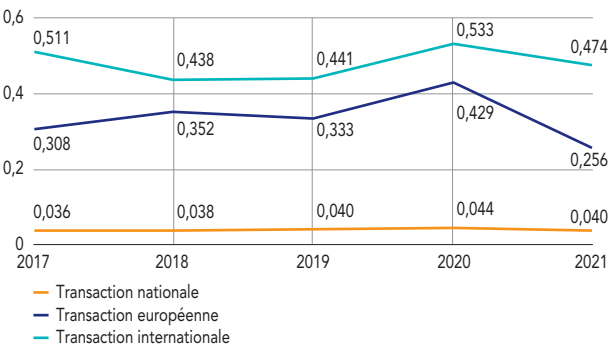


b) Répartition du montant de la fraude



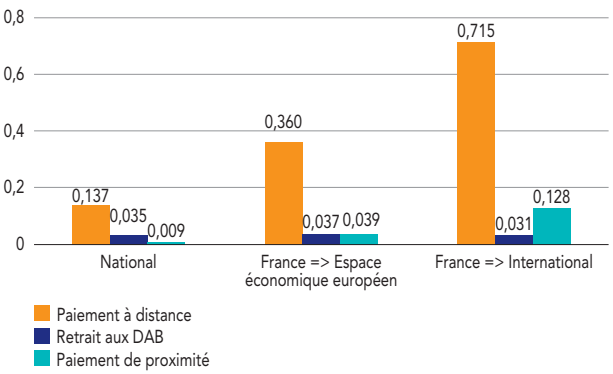
Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

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



Note : DAB – distributeur automatique de billets.

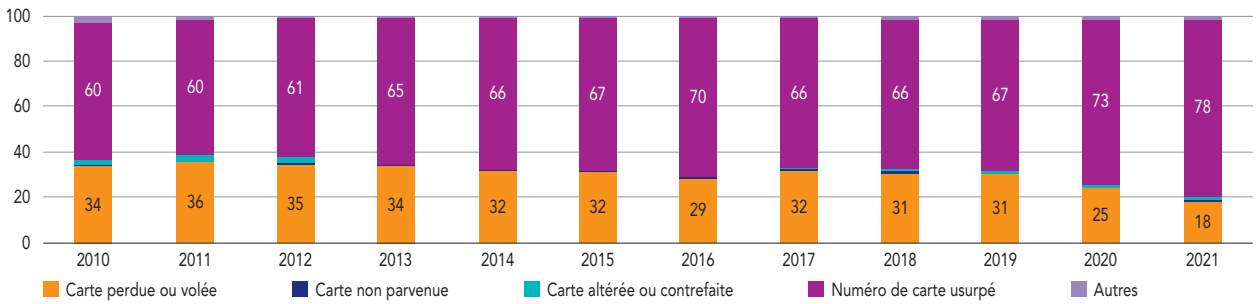
Source : Observatoire de la sécurité des moyens de paiement.

Dans les opérations réalisées au moyen de cartes émises en France, la part des transactions internationales n'est que de 7 % en 2021, mais ces dernières pèsent pour 38 % dans la fraude, soit 177 millions d'euros. En ne tenant compte que des transactions hors Espace économique européen, le déséquilibre est encore plus marqué. En effet, ces transactions ne représentent que 2 % des flux, mais concentrent 15 % de la fraude, soit 70 millions d'euros. Toutefois, si les transactions vers les pays de l'Union européenne et à l'international sont structurellement plus sujettes à la fraude, leur taux de fraude respectif a significativement diminué en 2021.

Enfin, quelle que soit la zone géographique, les taux de fraude sont plus élevés sur les paiements à distance, essentiellement des paiements sur Internet. La fraude s'opère en réutilisant les cartes volées ou perdues ou les numéros de carte usurpés sur des sites moins sécurisés à l'étranger. On constate également que le taux de fraude sur les paiements de proximité à l'international sont plus élevés que ceux des transactions européennes, du fait de l'utilisation de technologies moins robustes et donc plus vulnérables à la contrefaçon, comme la lecture de la piste magnétique ou la prise d'empreinte physique de la carte.

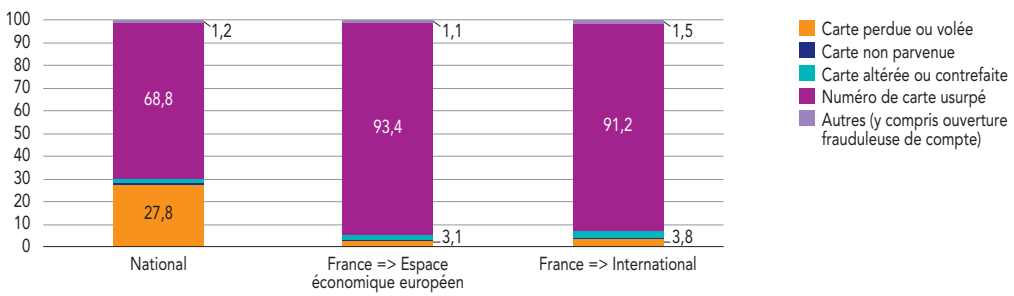
1.2.3 Répartition de la fraude par mode opératoire – Cartes émises en France

G16 Évolution des typologies dans les montants de fraude depuis 2010 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G17 Typologies dans les montants de fraude par zone géographique en 2021 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

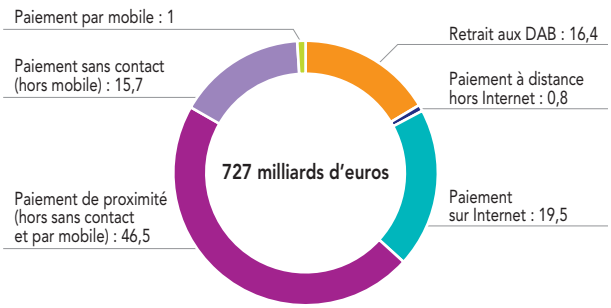
La part de la fraude associée à l'usurpation des numéros de carte a régulièrement augmenté depuis 2010, parallèlement au développement du e-commerce. Ce phénomène est lié au développement de techniques d'attaque de plus en plus sophistiquées, allant de l'hameçonnage à la fraude par manipulation du porteur de carte. En contrepartie, la part de la fraude liée à la perte ou au vol de la carte diminue pour représenter moins d'un cinquième de la fraude en 2021. Les autres types de fraude, comme les cartes non parvenues ou contrefaites, restent marginaux.

La fraude par usurpation du numéro de carte, qui peut se faire à distance, est structurellement plus élevée dans la fraude sur les transactions européennes (93 %) et à l'international (91 %), que sur les transactions nationales (69 %). En contrepartie, la fraude relative au vol ou à la perte de carte est plus élevée sur les transactions nationales (28 %).

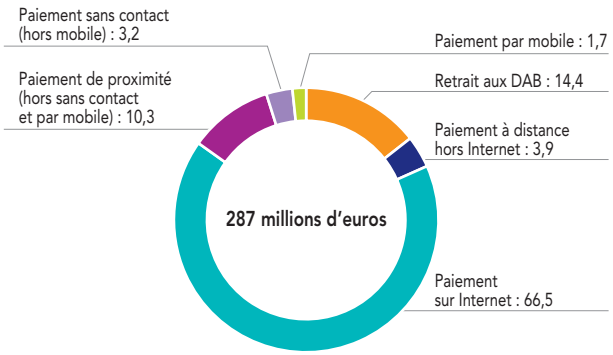
1.2.3 Répartition de la fraude sur les opérations nationales

G18 Transactions nationales par carte en montant (en %)

a) Répartition des transactions



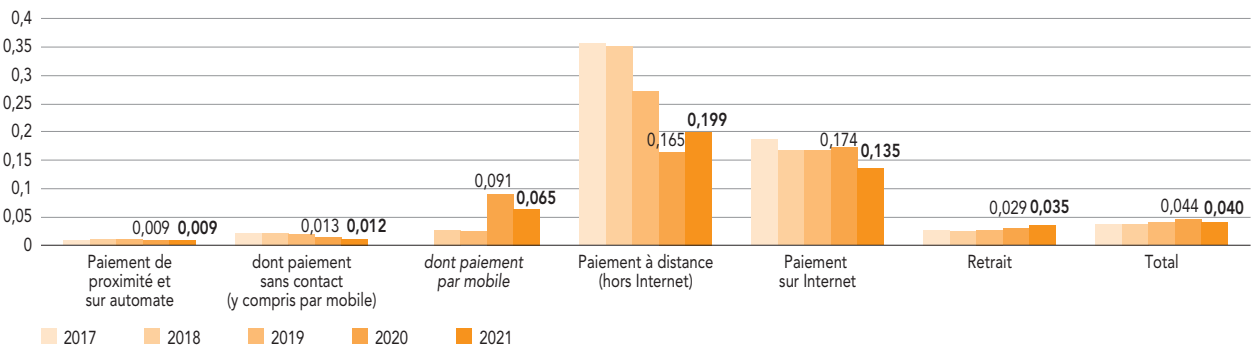
b) Répartition de la fraude



Note : DAB – distributeur automatique de billets.

Source : Observatoire de la sécurité des moyens de paiement.

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



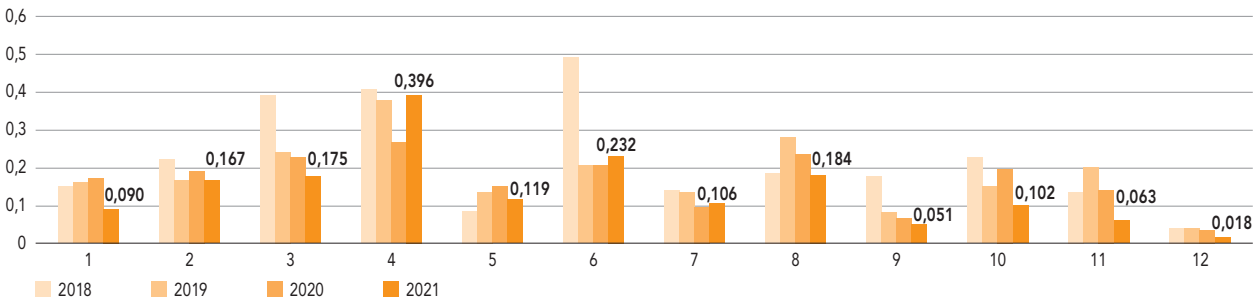
Source : Observatoire de la sécurité des moyens de paiement.

Si les paiements à distance ne représentent que 20 % des transactions nationales, et essentiellement des paiements sur Internet (96 %), ils concentrent à eux seuls 70 % de la fraude (67 % pour les paiements sur Internet). Toutefois, grâce au déploiement progressif de l'authentification forte tout au long de l'année le taux de fraude sur les paiements Internet a d'ores et déjà baissé très significativement, de 0,174 % en 2020 à 0,135 % en 2021 (– 22 %), soit son plus bas niveau historique. Dans le même temps, le taux de fraude sur les paiements sans contact atteint 0,012 %, dans un contexte de forte progression des flux (+ 55 %).

Au total, le taux de fraude des transactions nationales par carte diminue, de 0,044 % en 2020 à 0,040 % en 2021, après trois années consécutives de légère hausse.

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

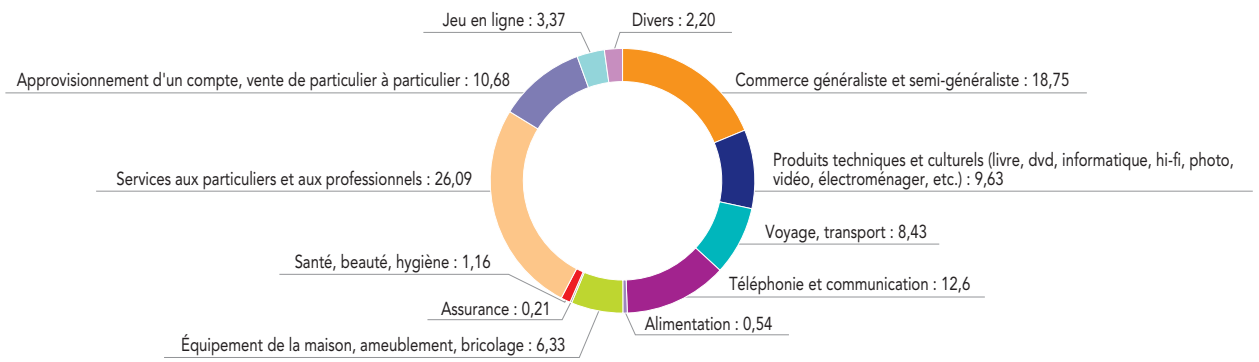
G20 Évolution du taux de fraude sur les paiements nationaux par carte sur Internet, par secteur (en %)



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

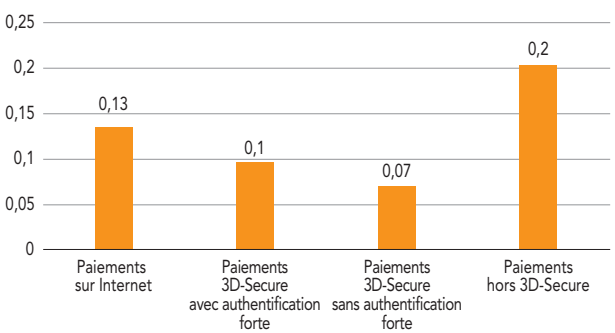
Source : Observatoire de la sécurité des moyens de paiement.

G21 Répartition de la fraude sur les paiements nationaux par carte sur Internet en montant, par secteur en 2021 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

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

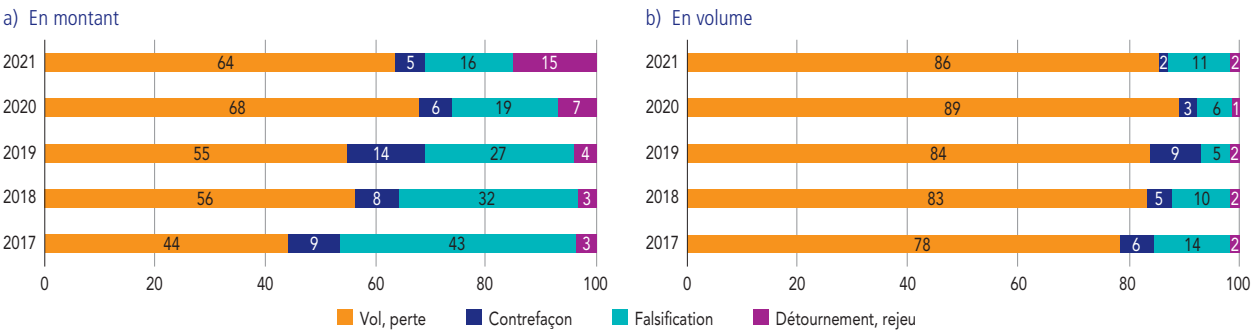


Source : Observatoire de la sécurité des moyens de paiement.

Le déploiement de l'authentification forte a permis de renforcer significativement la sécurité des paiements sur Internet. Au niveau national, les transactions sécurisées sont proportionnellement deux fois moins fraudées que celles hors 3D-Secure (0,10 %, contre 0,20 %). En outre, les exemptions ciblent bien des transactions moins risquées par nature (0,07 %).

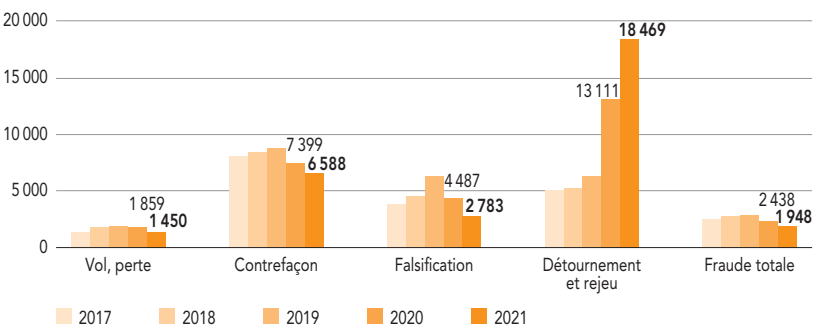
1.3 État de la fraude sur le chèque

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



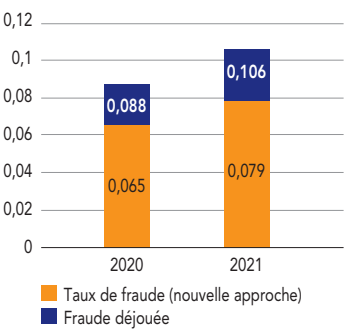
Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

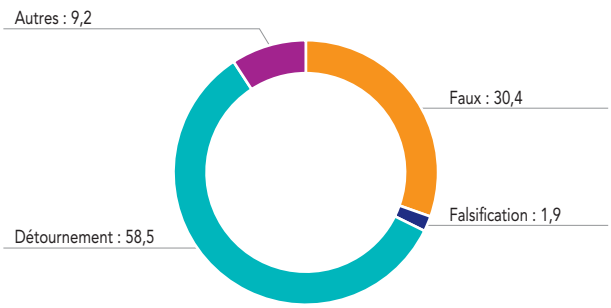
En 2021, le montant total des opérations frauduleuses par chèque progresse à 625 millions d'euros (+ 16,3 % par rapport à 2020). Néanmoins, les mécanismes de prévention contre la fraude déployés par les banques, conformément à la feuille de route de l'Observatoire *(cf. chapitre 2)* ont permis de neutraliser 161 millions d'euros de remises frauduleuses. Ainsi, la fraude brute, dans sa nouvelle approche, s'établit à 465 millions d'euros. Selon cette nouvelle approche, le taux de fraude est en hausse, à 0,079 % en 2021, contre 0,065 % en 2020, alors qu'il aurait atteint 0,106 % sans ces mécanismes de prévention, contre 0,088 % en 2020.

Dans ce contexte, les typologies de fraude sur le chèque évoluent. La part en montant de la perte et du vol s'est accrue substantiellement, passant de 44 % en 2017 à 64 % en 2021, alors que sa progression est plus modeste en volume (78 % en 2017, contre 86 % en 2021). De même, la part du détournement et du rejeu a progressé significativement passant de 3 % en 2017 à 15 % des montants fraudés en 2021. En contrepartie, la falsification a chuté en montant de 43 % en 2017 à 16 % en 2021.

Le montant moyen de fraude par chèque diminue globalement depuis 2019 pour atteindre 1 948 euros en 2021. La fraude par détournement et rejeu se distingue toutefois par son montant moyen en progression continue, et qui s'établit à 18 469 euros en 2021.

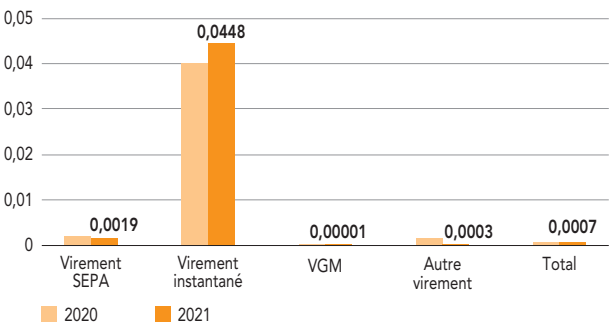
1.4 État de la fraude sur le virement

G26 Répartition de la fraude au virement en montant par typologie de fraude en 2021 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

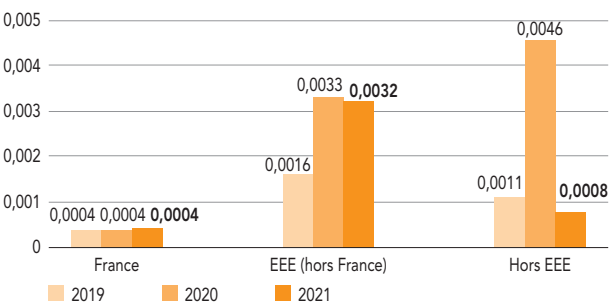
G27 Taux de fraude par type de virement (en %)



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

Source : Observatoire de la sécurité des moyens de paiement.

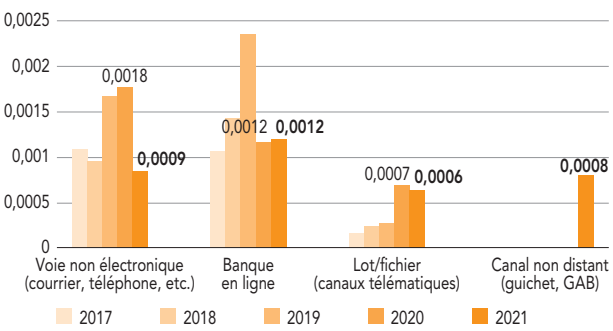
G28 Évolution du taux de fraude au virement par zone géographique (en %)



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'inititation (en %)



Note : GAB – guichet automatique bancaire.

Source : Observatoire de la sécurité des moyens de paiement.

Dans l'ensemble, la fraude sur le virement progresse légèrement à 287 millions d'euros en 2021, contre 267 millions d'euros en 2020. Toutefois, son taux de fraude baisse légèrement de 0,0007 % sous l'effet de flux croissants. Hors virements de gros montant, ce taux de fraude s'améliore aussi et s'établit à 0,0015 % en 2021, contre 0,0019 % en 2020. Le montant moyen d'un virement fraudé est de 6 149 euros en 2021, en baisse de plus de 50 % en trois ans. Avec des volumes multipliés, qui ont plus que doublé en un an, le virement instantané connaît une légère hausse de son taux de fraude (à 0,0448 %).

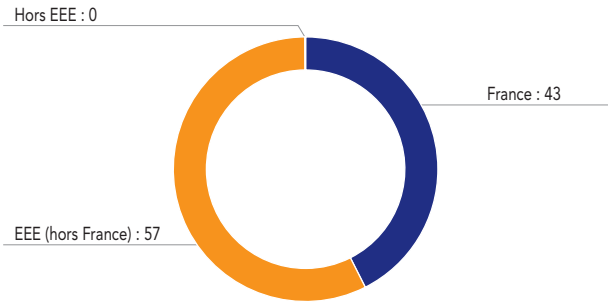
Le taux de fraude est en baisse ou constant sur l'ensemble des canaux d'initiation. Il a notamment été divisé par deux sur les virements par voie non électronique, qui étaient jusqu'alors les plus vulnérables à la fraude. Il reste stable pour les virements de banque en ligne, principalement utilisés par les particuliers (0,0012 %) et en légère baisse pour les virements par canaux télématiques, principalement utilisés par les entreprises et les administrations (0,0006 %).

Le taux de fraude sur les virements transfrontaliers régresse sur les transactions hors Espace économique européen (EEE), et se stabilise au sein de l'EEE. Les virements transfrontaliers pèsent pour 52 % des montants de fraude au virement.

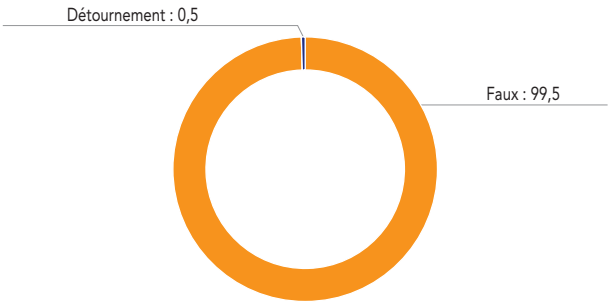
1.5 État de la fraude sur le prélèvement

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

a) Par zone géographique



b) Par typologie de fraude

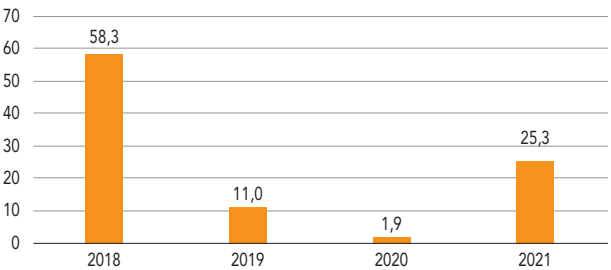


Note : EEE – Espace économique européen.

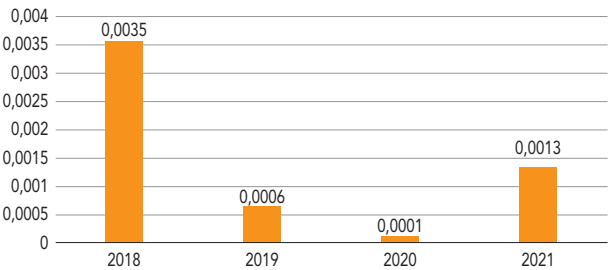
Source : Observatoire de la sécurité des moyens de paiement.

G31 Fraude au prélèvement

a) En montant (en millions d'euros)



b) Taux (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La fraude au prélèvement est extrêmement volatile avec un montant de 25 millions d'euros en 2021, contre 11 millions d'euros en 2019 et 2 millions d'euros en 2020. Le taux de fraude s'accroît ainsi nettement, de 0,0001 % en 2020 à 0,0013 % en 2021.

Néanmoins, cette hausse est à relativiser dans la mesure où le prélèvement est le moyen de paiement qui présente le montant annuel de fraude le plus bas parmi les instruments de paiement accessibles aux particuliers.

Le montant moyen de fraude sur un prélèvement est de 101 euros, un montant presque divisé par trois par rapport à l'année 2020 (dont le montant moyen était de 292 euros).

La typologie de cette fraude évolue : elle touche désormais majoritairement des comptes situés dans l'Espace économique européen (57 %, contre 25 % en 2020) ; elle repose presqu'exclusivement sur l'émission de faux ordres de prélèvement par un créancier fraudeur, c'est-à-dire sans mandat de prélèvement, ni relation économique sous-jacente avec la victime.

ENCADRÉS

❶

Indicateurs, enseignements et préconisations des services de police et de gendarmerie sur la fraude aux moyens de paiement en 2021

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 à l'Observatoire leurs principales observations sur les fraudes aux moyens de paiement constatées en 2021.

1. Les fraudes à la carte bancaire

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. La falsification et la contrefaçon de cartes de paiement ou de retrait font également partie des agrégats pris en compte. À cette fin, trois sources sont principalement suivies par les forces de l'ordre :

- les chiffres du service statistique ministériel de la Sécurité intérieure (SSMSI) répertoriant l'ensemble des remontées chiffrées des services de police et de gendarmerie ;
- le nombre de procédures judiciaires ouvertes remontées dans le fichier de Traitement des antécédents judiciaires (TAJ), base commune à la police et à la gendarmerie ;
- les chiffres provenant de recherches par nature d'infractions (NATINF), qui est un indicateur de qualification pénale des infractions par le ministère de la Justice.

Ainsi, selon les trois indicateurs, une hausse comprise entre 20 % et 25 % des faits de fraude à la carte bancaire est constatée entre 2020 et 2021. Elle pourrait s'expliquer par les allègements successifs des mesures relatives à la crise sanitaire liée à l'épidémie de Covid-19, qui ont notamment pu avoir une incidence sur l'ampleur des vols de carte.

La plateforme Perceval, qui est une plateforme nationale de recueil de signalement des usages frauduleux de cartes bancaires sur Internet, destinée aux particuliers victimes fait état de 324 594 signalements en 2021 (contre 318 804 en 2020, + 1,8 %) pour un préjudice total de 140 millions d'euros (contre 137 millions d'euros en 2020, + 2,6 %), soit un préjudice moyen par signalement de 432 euros (contre 428 euros en 2020). Il convient de noter qu'un signalement sur la plateforme Perceval peut couvrir plusieurs transactions initiées frauduleusement à partir des mêmes données de carte usurpées.

En ce qui concerne l'utilisation frauduleuse de carte bancaire réalisée par « paiement sans contact », le TAJ mentionne 2 779 procédures initiées sur l'ensemble du territoire national pour l'année 2021, chiffre qui traduit une tendance légèrement à la hausse par rapport aux années antérieures (respectivement 2 530 en 2020 et 2 484 procédures en 2019), mais qu'il faut relativiser compte tenu de l'augmentation de la volumétrie de ces transactions. Dans ces procédures, les forces de l'ordre constatent principalement une utilisation de

Nombre de faits de fraude à la carte bancaire recensés par la police et la gendarmerie

	2018	2019	2020	2021 (évolution 2020-2021)
Source SSMSI	57 708	67 037	60 824	73 757 (+ 21 %)
Source TAJ	53 703	58 537	53 221	66 497 (+ 25 %)
Source NATINF	53 276	64 168	58 414	70 425 (+ 21 %)

Source : Service statistique ministériel de la Sécurité intérieure (SSMSI).

la fonctionnalité sans contact des cartes après un vol. **L'utilisation de technologies avancées de fraude reposant sur la captation des données à distance par le système de communication en champ proche (NFC, *Near-Field Communication*) n'est pas constatée.**

2. Les piratages de terminaux de paiement et de retrait par carte

Considérée comme une des priorités européennes en matière de cybercriminalité, la captation des données bancaires demeure un fait criminel bien implanté sur le territoire national. Les modes opératoires s'étendent désormais à tous les types d'automates de paiement ou de retrait d'argent (distributeurs de billets, distributeurs automatiques de carburant, automates d'autoroutes, dispositifs de règlement de parking, etc.), sur lesquels *skimmers* [1] et *shimmers* [2] continuent d'être implantés, ainsi qu'aux terminaux de paiement portatifs, c'est-à-dire tout type de terminal sans fil qui n'est pas fixé à la caisse du magasin, qui sont également compromis ou détournés de leurs finalités.

La fraude par *skimmer* consiste à récupérer, par le biais de terminaux de paiement trafiqués ou usurpés, les données bancaires stockées sur la bande magnétique de la carte. La fraude par *shimmer* repose sur des procédés similaires, mais récupère les données contenues dans la puce 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, où la lecture de la puce est facultative comme pour les paiements sur les péages d'autoroute ou dans les pays où la carte à puce est encore peu déployée, comme dans les 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 commerce électronique non européens qui n'ont pas mis en œuvre l'authentification forte du porteur de la carte.

Pour l'année 2021, le nombre de compromissions d'automates et terminaux par *skimmers* ou *shimmers* recensées demeure stable, avec 28 cas. Les forces de l'ordre en avaient recensé 30 en 2020, 26 en 2019, 19 en 2018, 35 en 2017 et 82 en 2016. Parmi les 28 cas recensés en 2021, 13 concernaient des distributeurs automatiques de carburant (DAC) et 15 concernant des distributeurs automatiques de billets (DAB). Les gestionnaires de station essence comme les gestionnaires de DAB doivent par conséquent rester vigilants pour prévenir les tentatives de substitution d'un terminal de paiement légitime par un terminal trafiqué ou toute installation par un tiers d'un dispositif externe frauduleux (lecteur, caméra, clavier, etc.).

Les forces de l'ordre ont notamment constaté un nombre encore non évalué, mais significatif, de plaintes déposées par des entreprises de transport par poids lourds à la suite de l'utilisation frauduleuse de leurs cartes de carburants. Les cartes de carburants piratées en France seraient ensuite utilisées sur les péages autoroutiers en France ou en Europe de l'Est, notamment en Pologne, République tchèque et Slovénie. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), rattaché à la DCPJ, coopère par l'intermédiaire d'Europol, avec le *Fuel Industry Card Fraud Bureau* (FICFIB) [3].

3. Les attaques par *jackpotting* contre les distributeurs automatiques de billets (DAB)

Les forces de l'ordre continuent leurs investigations contre les attaques de distributeur automatique 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 actionner les mécanismes de délivrance des billets. Il s'agit de techniques très sophistiquées qui ne peuvent être mises en œuvre que par des réseaux organisés ou des délinquants spécialisés.

1 Matériel se glissant dans la bouche/fente d'un automate tout en laissant de l'espace pour qu'une carte bancaire puisse y être glissée naturellement. Une copie des données de la piste magnétique sera alors réalisée par le matériel sans que cela 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 FICFIB a été créé en 2003 pour établir et maintenir un réseau destiné à échanger des informations relatives à la réduction et à la prévention de la fraude aux cartes de carburant et pour élaborer des stratégies communes pour prévenir et réduire ces fraudes à l'échelle européenne. C'est une organisation similaire à l'*European Association for Secure Transactions* (EAST), engagée dans la lutte contre les fraudes aux distributeurs automatiques de billets. L'adhésion au FICFIB est ouverte aux entreprises qui émettent des cartes de carburant ou exploitent un réseau de distribution et qui ont un intérêt bien défini à prévenir et à combattre les fraudes aux cartes de carburant.

Les préjudices par *jackpotting* sont en sensible baisse en 2021 par rapport à 2020 : 32 faits ont été recensés en 2021 pour un montant total de 335 370 euros, contre 95 en 2020 pour un montant total de 681 170 euros. Parmi ces 32 faits, 22 concernaient un nouveau mode opératoire ciblant un modèle spécifique de distributeur automatique de billets. Cette baisse notable peut s'expliquer par l'identification et l'interpellation par les agents de l'OCLCTIC de douze délinquants spécialisés dans le *jackpotting* et du démantèlement de cinq équipes de malfaiteurs responsables de plus de la moitié des attaques recensées en 2020.

Au regard des constations sur les cas de *jackpotting*, l'OCLCTIC note que l'obsolescence du matériel et des logiciels aide encore trop souvent à la réussite des attaques. Par conséquent, il préconise aux gestionnaires de DAB des mesures minimales de sécurité, notamment de procéder à une mise à jour systématique des systèmes d'exploitation, de chiffrer le disque dur pour prévenir les attaques ne passant pas par le système d'exploitation, d'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.

Ainsi, au-delà des mesures de protection physique et logique des DAB déployés par les professionnels des paiements, l'action répressive des forces de l'ordre (infiltration, exploitation des images de vidéosurveillance, mises sur écoute, etc.) permet de démanteler ces réseaux et de contenir cette typologie de fraude [4].

4. Les faux ordres de virement au préjudice des secteurs privé et public

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 vers un compte bancaire géré par l'escroc. Dans la méthodologie statistique de l'Observatoire, les « faux ordres de virement » (FOVI) sont classés comme étant des détournements de virement. 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 (PME, TPE, des artisans) ou d'une administration publique afin de faire réaliser des déplacements de fonds non autorisés à des fins frauduleuses.

L'arrivée du Covid-19 et la généralisation du télétravail ont permis, en 2020, une forte recrudescence exponentielle des cas de FOVI, avec le déploiement rapide de nouveaux modes de fonctionnement et d'organisation, qui ont permis l'exploitation, par des acteurs malveillants, de vulnérabilités nouvelles ou préexistantes. **En 2021, les forces de l'ordre ont relevé 517 affaires de FOVI pour un montant total de 101,2 millions d'euros, incluant un cas exceptionnel ayant causé un préjudice de 33 millions d'euros.**

Les forces de l'ordre ont distingué plusieurs modes opératoires utilisés par les escrocs :

- changement de RIB (68,5 % des cas) ;
- fraude au faux président (19,5 % des cas) ;
- prise de contrôle à distance (8,5 % des cas) [5] ;
- mode opératoire inconnu (3,5 % des cas).

Un nouveau phénomène a également été observé en 2021. Jusqu'à alors, plus de la moitié des faits de FOVI commis créditaient des comptes détenus dans des banques françaises de la Place. En 2021, les trois quarts des comptes de première destination étaient liés à un IBAN français par des prestataires de services de paiement offrant des services de type « banque en ligne » ou « banque mobile ».

La Fédération bancaire française, le club des directeurs de Sécurité et de Sûreté des entreprises (CDSE) et la direction centrale de la Police judiciaire (DCPJ) se sont ainsi associés pour lutter contre les escroqueries aux faux ordres de virement par changement de coordonnées bancaires et proposer un module de *e-learning* aux entreprises et administrations [6].

4 Les attaques par *jackpotting* visant les équipements bancaires et non les opérations de retrait ne sont pas catégorisées dans la fraude sur les paiements par carte recensés par l'Observatoire.

5 La prise de contrôle à distance s'effectue généralement par le piratage et l'utilisation d'une messagerie électronique, l'escroc pouvant ainsi donner ses instructions et faire réaliser des virements bancaires avec l'identité volée d'une personne physique ou morale ; par l'installation d'un « logiciel espion » qui permet à l'escroc de récupérer les codes d'accès aux interfaces de banque en ligne, mais aussi d'assister et d'accompagner la victime sur l'application bancaire en l'incitant à réaliser des virements bancaires sur un compte qu'il a lui-même fourni.

6 Le module d'*e-learning* est accessible sur la page Internet suivante : *https://www.lesclesdelabanque.com/entreprise/prevenir-escroquerie-aux-coordonnees-bancaires/*

2

ACTIONS CONDUITES PAR L'OBSERVATOIRE EN 2021

2.1 Le bilan positif de la mise en place de l'authentification forte des paiements sur Internet

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, introduite par la deuxième directive européenne sur les services de paiement (DSP 2). 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 qui a ensuite été déployé sur une période de deux ans environ.

2.1.1 Le plan de migration de la Place française

Le plan de migration vers l'authentification forte des paiements comportait deux volets :

- un volet à l'attention des consommateurs : l'enrôlement des porteurs de carte dans des dispositifs d'authentification conformes à la définition de l'authentification forte de la DSP 2, en remplacement de l'usage du code SMS à usage unique (ou SMS OTP – *one time password*) comme facteur unique d'authentification ;
- un volet à l'attention des acteurs professionnels de la chaîne des paiements, y compris les e-commerçants : la mise à niveau des infrastructures d'authentification afin d'assurer la gestion des règles de responsabilité et des cas d'exemption d'authentification forte prévus par la directive.

Ces deux volets ont fait l'objet d'indicateurs de suivi assortis de cibles et d'échéances, ainsi que de plans d'action visant à accompagner la mise en conformité de la Place française. L'Observatoire a acté, lors de sa session plénière du 17 décembre 2021, l'aboutissement du plan de migration, compte tenu du haut niveau de conformité observé sur le marché français.

2.1.2 Le déploiement des solutions d'authentification forte auprès des porteurs de carte

Pour mémoire, l'authentification forte repose sur l'utilisation de deux éléments ou plus appartenant au moins à deux catégories différentes de facteur 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) : une carte, un *smartphone*, une montre ou un bracelet connecté, un porte-clés, etc. ;
- « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique.

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 un requis 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. Ainsi :

- 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 invalide le code d'authentification.

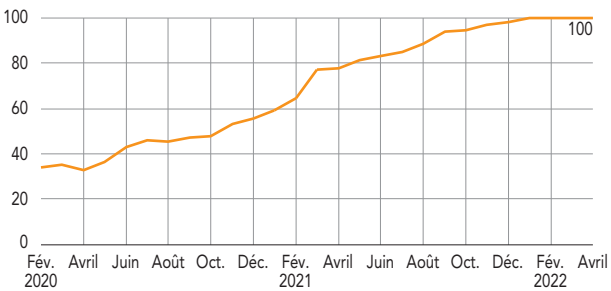
Dans le cas du recours à un facteur biométrique, la clé de validation de l'opération de paiement générée après lecture de l'empreinte devra être également à usage unique.

À juin 2022, l'Observatoire estime que 100 % des porteurs de carte actifs sur Internet (c'est-à-dire ayant réalisé au moins un paiement en ligne au cours des trois derniers mois) sont équipés et utilisent désormais ce mode d'authentification en remplacement du SMS OTP. Cela représente plus de 90 % du nombre total de porteurs de cartes.

Les solutions d'authentification forte qui équipent les porteurs français sont :

- pour les deux tiers d'entre eux, une solution de type application mobile sécurisée : au moment d'un paiement par carte sur Internet, l'utilisateur valide la transaction via son application de banque en ligne sur son *smartphone* préenregistré de façon sécurisée (reconnu comme facteur de possession), au moyen soit d'un code personnel (facteur de connaissance), soit d'une empreinte biométrique (facteur d'inhérence) ;

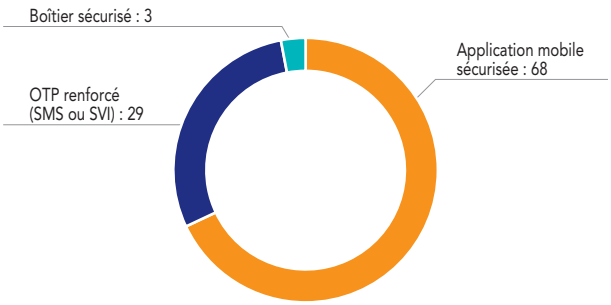
G1 Suivi de la trajectoire d'équipement des porteurs : part des porteurs équipés dans les porteurs actifs sur Internet (en %)



Note : Porteur actif : porteur ayant réalisé au moins une transaction en ligne au cours des trois derniers mois.

Source : Observatoire de la sécurité des moyens de paiement.

G2 Répartition de l'équipement des porteurs (en %)



Note : OTP – *one time password* (mot de passe à usage unique), SVI – serveur vocal interactif.

Source : Observatoire de la sécurité des moyens de paiement.

- pour 28 % d'entre eux, une solution de type « OTP renforcé » : l'utilisateur s'authentifie au moyen d'un code à usage unique reçu par SMS ou par serveur vocal interactif (la ligne téléphonique faisant office de facteur de possession) et d'un mot de passe statique (facteur de connaissance : code d'accès à la banque en ligne ou mot de passe dédié) ;
- pour les 3 % restants, une solution de type boîtier physique mis à disposition par la banque (facteur de possession), et intégrant un moyen d'authentification supplémentaire (généralement un facteur de connaissance).

2.1.3 La mise en conformité des pratiques des e-commerçants

Du point de vue des commerçants et de leurs prestataires, la DSP 2 a défini des règles précises en matière d'authentification des transactions :

- les commerçants doivent recourir à une authentification forte, et ce à chaque paiement accepté sur Internet, sauf en cas d'exemption applicable ;
- l'activation d'un des cinq motifs d'exemption prévus par les textes pour fluidifier le parcours de paiement et tenir compte de niveaux de risque différenciés peut être sollicitée par le commerçant, mais reste soumise à l'accord de la banque émettrice de la carte.

Pour mémoire, **les cinq motifs d'exemption à l'authentification forte** prévus par les normes techniques de réglementation (*regulatory technical standards* – RTS)[1] pour les transactions en présence active de l'utilisateur sont :

- **Les paiements 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 de paiement 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, à compter de la deuxième transaction ;
- L**es paiements vers un bénéficiaire de confiance** (article 13), c'est-à-dire vers un bénéficiaire désigné comme étant de confiance par le porteur de la carte, cette désignation ayant elle-même fait l'objet d'une authentification forte du porteur de la carte ;
- **Les paiements initiés électroniquement via des processus ou protocoles de paiement sécurisés réservés à un usage entre professionnels** (article 17).

Cette exemption nécessite une évaluation préalable des processus et des protocoles par l'autorité nationale compétente (en France, par la Banque de France). Celle-ci s'assure que le niveau de sécurité offert est au moins équivalent à celui d'une authentification forte.

Le recours à l'authentification forte par les commerçants a été très progressif, en raison du besoin de fiabiliser les nouvelles infrastructures d'authentification fondées sur le protocole 3D-Secure v2. Il s'est toutefois accéléré sous l'effet du plan de montée en régime du mécanisme de *soft decline* [2]. Ainsi, fin avril 2022, tous les flux de paiement soumis à la DSP 2 sont conformes aux dispositions. En effet, soit ils transitent par les protocoles 3D-Secure (permettant l'authentification forte ou l'activation d'une exemption), soit ils font l'objet d'une demande d'exemption accordée hors 3D-Secure (en particulier pour les paiements de petit montant). La mise en conformité, au premier trimestre 2022, des flux des secteurs du voyage et de l'événementiel a finalisé le processus de mise en conformité. Ces secteurs d'activité durement touchés par la crise sanitaire avaient bénéficié, à titre transitoire, d'une dérogation accordée par l'Observatoire.

En complément, l'Observatoire s'est attaché à renforcer le cadre d'émission des paiements des transactions dites MIT (*Merchant Initiated Transactions*). Celles-ci sont émises par le commerçant sans connexion active de l'utilisateur, et correspondent notamment aux paiements fractionnés (en plusieurs fois) ou différés (par exemple, paiement au moment de l'envoi ou à réception de la commande), aux abonnements (presse, vidéo à la demande, etc.) et aux paiements à l'usage (par exemple, transports urbains) :

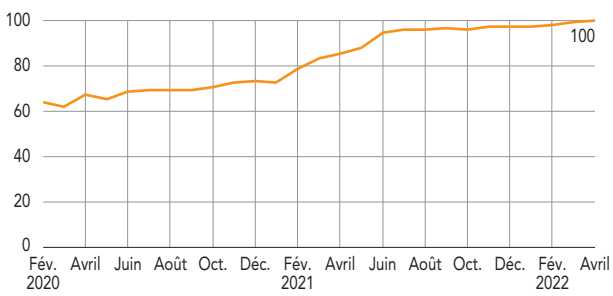
- les transactions MIT issues de nouvelles souscriptions doivent comporter la trace technique (ou « chaînage ») d'une authentification forte réalisée au moment de la prise du numéro de carte du souscripteur, matérialisée par un mandat formalisant l'engagement à payer et les conditions de ces paiements (montant, plafond, fréquence, etc.) ;
- les transactions MIT issues de souscriptions antérieures à la mise en place du chaînage bénéficient d'une clause d'antériorité, dite de *grandfathering*, et doivent comporter une référence de chaînage standard prédéfinie par le système de paiement par carte.

À la fin du premier trimestre 2022, la totalité des commerçants et de leurs prestataires techniques d'acceptation pouvaient ainsi émettre des MIT répondant à l'obligation de chaînage. D'après les banques émettrices de cartes, la part des transactions MIT chaînées atteignait 93 % en nombre d'opérations en avril.

Dans le régime post-DSP 2, les flux de paiement en ligne des porteurs français se répartissent schématiquement ainsi :

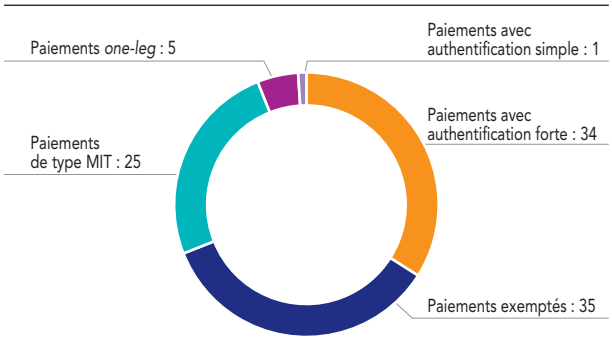
- un tiers de transactions ayant fait l'objet d'une authentification forte ;
- 35 % de transactions bénéficiant d'une exemption ;
- un quart de transactions de type MIT ;
- le solde (5 %), d'opérations sans authentification forte dites « *one-leg* », c'est-à-dire avec un commerçant hors Espace économique européen, non soumises à l'obligation d'authentification forte.

G3 Suivi de la trajectoire de mise en conformité des flux par les commerçants : part des flux CIT conformes en valeur (en %)



Note : CIT – *Customer Initiated Transaction*: opération initiée par le porteur.
Source : Observatoire de la sécurité des moyens de paiement.

G4 Répartition des flux par moyen de sécurisation (en %)



Note : 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 ; MIT – *Merchant Initiated Transactions*: transactions émises par le commerçant sans connexion active de l'utilisateur.
Source : Observatoire de la sécurité des moyens de paiement.

1 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.

2 Ces messages correspondent à des rejets d'autorisation par l'émetteur de la carte d'une transaction qui n'est pas conforme à la DSP 2 avec la possibilité pour le commerçant ou son prestataire d'acceptation technique de soumettre une nouvelle fois la transaction via le protocole 3D-Secure (opération dite de *retry*).

2.1.4 Perspectives

Au-delà de cette bonne mise en conformité du marché français, l'Observatoire continuera à veiller à la bonne application des règles prévues par la DSP 2, tout en préservant un fonctionnement aussi fluide que possible du e-commerce. Il jouera également son rôle de coordination avec l'ensemble du marché sur différents sujets :

- la poursuite des actions de pédagogie à l'attention des consommateurs, afin de veiller à la bonne appropriation des nouvelles solutions d'authentification, mais aussi à l'adoption de bons réflexes en matière de sécurité lors de leurs opérations sur Internet ;
- la lutte contre les nouveaux procédés de fraude visant à contourner l'authentification forte, notamment par manipulation du payeur, et en relation avec les opérateurs de téléphonie, la recherche de moyens de prévention des failles technologiques exploitées (usurpation de numéro de téléphone par *spoofing*, piratage de ligne mobile par *SIM-swapping*, etc.) ;
- le suivi de la performance des solutions et infrastructures d'authentification, ainsi que des mécanismes de continuité associés, afin d'assurer un haut niveau de fluidité et de résilience du e-commerce ;
- le développement des fonctionnalités du protocole 3D-Secure pour permettre l'intégration de l'ensemble des exemptions prévues par la réglementation, notamment celle relative aux bénéficiaires de confiance (article 13 du RTS), dans des conditions de sécurité équivalentes aux autres exemptions ;
- la lutte contre les usages inappropriés des moyens et infrastructures d'authentification, comme cela a été observé par certains professionnels de la vente flash (recours à une authentification forte pour accéder à l'espace de vente en ligne), voire par certains particuliers (influenceurs sur les réseaux sociaux qui partagent leurs données de carte avec leurs *followers*).

Ces différents sujets continueront à faire l'objet de travaux de consolidation au second semestre 2022, sous le pilotage du groupe de travail multipartite qui a assuré le pilotage de la migration.

2.2 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 2020 [3]. 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.

Un an après la publication de ses recommandations, l'Observatoire dresse un premier point d'étape encourageant avec la réalisation de plusieurs actions

T1 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 surveillance 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 surveillance 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 surveillance 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 surveillance 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)	En cours de mise en œuvre par le service Vérifiance-FNCI-Banque de France
Recommandation n°7 : renforcer la surveillance de la Banque de France sur la résistance physique des formules de chèques contre la falsification et la contrefaçon	Réalisée
Recommandation n°8 : assurer l'efficacité du service Vérifiance-FNCI-Banque de France contre la contrefaçon de chèque	Réalisée
Recommandation n°9 : structurer durablement la coopération entre les acteurs dans la lutte contre la fraude et soutenir l'action des forces de l'ordre	Réalisée
Recommandation n°10 : soutenir par un plan de communication la vigilance des utilisateurs dans l'usage du chèque	Réalisée

concrètes tant du côté des autorités publiques que du côté des professionnels de la filière. Toutefois, au regard des niveaux toujours élevés de fraude, l'Observatoire appelle les acteurs de la filière à poursuivre et amplifier leurs efforts pour améliorer la sécurité de ce moyen de paiement en décroissance. En tenant compte des contrôles déjà effectués et de la politique de risques de chaque établissement, la Banque de France s'assurera de la bonne mise en œuvre de ces recommandations par les établissements bancaires dans le cadre de ses actions de surveillance.

2.2.1 La révision du référentiel de sécurité du chèque de la Banque de France

Au titre de sa mission de surveillance sur la sécurité des moyens de paiement [4], la Banque de France s'assure de la pertinence des normes applicables au chèque. Alors que la plupart des instruments de paiement, européens par nature, sont encadrés par la réglementation européenne, notamment la deuxième directive européenne sur les services de paiement (DSP 2) et que leurs autorités de gouvernance sont surveillées par l'Eurosystème [5], le chèque reste un instrument de paiement essentiellement national. Son usage à l'international reste toutefois encadré par la convention de Genève de 1935.

En complément des dispositions législatives et réglementaires, rassemblées dans le Code monétaire et financier [6], 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 bancaires (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). La première version est entrée en vigueur en juillet 2005, alors que le système de paiement par chèque était profondément réformé par la dématérialisation des échanges et de la compensation interbancaires (le système d'échange d'images-chèques – EIC) [7]. Il s'agissait notamment de s'assurer de la bonne application des traitements bancaires sur les chèques du fait de la réforme de la compensation. 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 de lui remettre un questionnaire annuel d'auto-évaluation.

Le RSC avait déjà connu une première révision d'ampleur en 2016 qui avait abouti à un référentiel plus simple axé sur de grands principes de sécurité. Compte tenu des nouvelles recommandations de l'Observatoire formulées sur le chèque 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. À travers ce nouveau référentiel de sécurité, la Banque de France appelle notamment les établissements bancaires à :

- renforcer la surveillance des remises frauduleuses de chèque, notamment au regard des risques d'escroquerie sur les encaissements de chèque ;
- améliorer la lutte contre les chèques perdus et volés, en renforçant la sécurité de l'acheminement des chéquiers (par exemple, en alertant le client par SMS de l'envoi du chéquier tout en lui demandant de réagir au plus vite s'il ne l'a pas reçu sous un certain délai), la qualité des procédures de mise en opposition et la diffusion d'outils de contrôle de la régularité des chèques ;
- maintenir la vigilance sur la sécurité physique des formules, en intégrant des éléments de sécurité qui doivent limiter les risques de falsification et de contrefaçon.

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

4 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 de sécurité 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.* »

5 Le nouveau référentiel de sécurité (cadre de surveillance) de l'Eurosystème pour les instruments, les systèmes et les dispositifs de paiement électronique (*Payment Instruments Schemes and Arrangements* – PISA *framework*) a été publié en décembre 2021. Il fusionne les référentiels précédents respectivement applicables aux réseaux de paiement par carte, aux virements, aux prélèvements et à la monnaie électronique. Il étend le champ de surveillance de l'Eurosystème aux solutions de paiement qui servent à initier des opérations en s'appuyant sur un autre instrument de paiement (par exemple solutions de paiement mobile).

6 La législation à propos du chèque est restée très stable depuis de nombreuses années, mis à part quelques évolutions visant la réglementation en matière de chèques sans provision. Le chèque reste le seul moyen de paiement soumis à des sanctions pour son émetteur.

7 La dématérialisation de la compensation interbancaire du chèque a été permise par i) le règlement du CRBF n°2001-04 du 29 octobre 2001 relatif à la compensation des chèques, homologué par un arrêté du 17 décembre 2001, puis par ii) la convention professionnelle sur l'échange d'images-chèques (EIC) du 9 juillet 2003 et par iii) les règles de l'échange d'images-chèques de juillet 2000 complétées en 2005, qui sont sous la responsabilité du CFONB. Les règles de l'EIC peuvent faire l'objet de révisions ou de communications supplémentaires, ce qui a été le cas en 2021.

Ce nouveau RSC sera utilisé comme un élément de référence pour l'évaluation de 2023 sur l'exercice 2022. À partir de 2023, il est également prévu que la Banque de France renforce sa surveillance des formules de chèques en demandant aux établissements de lui fournir un spécimen des formules mises à disposition de leurs clientèles et que soit notifié tout incident grave affectant le système de paiement par chèque. Ces procédures, annexées au nouveau RSC, entreront en application en janvier 2023.

2.2.2 La révision du cadre statistique de déclaration de la fraude au chèque de la Banque de France

Pour améliorer la connaissance des phénomènes de fraude et renforcer sa surveillance, la Banque de France a également révisé sa collecte statistique « Recensement de la fraude aux moyens de paiement scripturaux » en complétant ses indicateurs de recensement des fraudes sur le chèque. Jusqu'en 2021, les fraudes au chèque étaient uniquement déclarées par les « établissements remettants », c'est-à-dire ceux du bénéficiaire qui remet un chèque à l'encaissement. À partir des données 2022, les établissements tirés de chèque, c'est-à-dire ceux du débiteur qui a émis un chèque, devront également déclarer les fraudes au chèque. Cette déclaration par un établissement tiré sera similaire à celle faite par l'établissement remettant. Les fraudes seront déclarées en montant et en valeur selon les quatre typologies identifiées par l'Observatoire. En parallèle des chèques rejetés pour perte ou vol et pour contrefaçon, les établissements devront également déclarer la part des chèques ayant été automatiquement rejetés par l'établissement en raison de leur inscription au Fichier national des chèques irréguliers (FNCI). Cela devrait permettre à l'Observatoire à moyen terme d'apprécier la capacité du FNCI à jouer un rôle préventif dans la lutte contre la fraude au chèque.

Les établissements remettants ont par ailleurs développé des mécanismes de temporisation ou de blocage des remises de chèques permettant dans certains cas d'empêcher la réalisation de la fraude. La Banque de France a donc intégré un nouvel indicateur de statistique appelé à mesurer la part de la fraude déjouée malgré la présentation du chèque au système d'échange. La fraude déjouée ainsi mesurée devra 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 (exemple : utilisation d'un compte d'attente ou d'un compte technique). Dans ce dernier cas, cela comprend les rejets 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.

Sans attendre l'intégration de cet indicateur dans les collectes relatives à l'exercice 2022, la Banque de France a demandé aux principaux groupes bancaires de la Place de lui remonter cet indicateur de façon *ad hoc*. Les premiers résultats déclarés par les établissements montrent une efficacité de ces outils de temporisation ou de blocage avec **161 millions d'euros de fraude déjouée** portant sur 40 693 chèques remis à l'encaissement, ce qui permet ainsi de **déjouer 26 % de la fraude au chèque**.

2.2.3 La promotion du Fichier national des chèques irréguliers (FNCI) et de sa consultation via le service Vérifiance

Outre la révision des cadres de surveillance, l'Observatoire a exprimé la nécessité de promouvoir la consultation du Fichier national des chèques irréguliers (FNCI) tenu par la Banque de France et consultable via le service Vérifiance. En effet, sa contribution préventive dans la lutte contre la fraude s'est amoindrie au fil des années en raison d'une baisse des consultations plus rapide que la baisse des paiements par chèque.

Au-delà des chèques rattachés à des comptes en interdit bancaire ou judiciaire et 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).

Pour préserver l'efficacité de ce service contre la contrefaçon de chèques, la Banque de France a diffusé en mai 2022 via le Comité français d'organisation et de normalisation bancaires (CFONB) une nouvelle procédure de déclaration des faux chèques au FNCI. Celle-ci vise à garantir la réactivité des établissements bancaires qui détectent de faux chèques. Dans le même objectif de lutte contre la

contrefaçon, l'Association du paiement a révisé le protocole CHPN (Chèque – Protocole normalisé), afin de véhiculer sur les terminaux de caisse des commerçants accepteurs de chèques et utilisateurs du service Vérifiance, une information complémentaire permettant aux commerçants d'identifier certains chèques contrefaits. Enfin, en lien avec le prestataire en charge du service Vérifiance, la Banque de France poursuit ses travaux visant à faciliter la consultation du FNCI à une palette plus diversifiée d'accepteurs de chèques (particuliers, autoentrepreneurs, professionnels, etc.).

2.2.4 Un effort constant de communication à destination des utilisateurs

L'Observatoire rappelle régulièrement la vigilance indispensable des utilisateurs dans la sécurité des paiements par chèque. Dans le cadre du rapport annuel 2020 publié en juillet 2021, l'Observatoire avait d'ailleurs formulé cinq conseils de prudence pour l'utilisation du chèque, s'adressant tant aux émetteurs qu'aux accepteurs de chèques. Par exemple, l'Observatoire préconise aux utilisateurs de privilégier le retrait de leurs formules de chèques en agence bancaire et pour ceux qui ne peuvent pas ou ne souhaitent pas se déplacer, d'être particulièrement vigilants quant à la bonne réception du chéquier par voie postale. De même, les utilisateurs sont invités à conserver leurs chéquiers en sécurité.

En complément des actions de sensibilisation de la clientèle portées par les établissements bancaires et les associations, plusieurs communications spécifiques ont été portées par l'Observatoire et la Banque de France en tant qu'opérateur de la stratégie nationale d'éducation financière :

- en juillet 2021, la Banque de France diffuse une vidéo [8] ciblée sur les escroqueries à l'encaissement de chèque, qui a été réalisée en partenariat avec l'Institut national de la consommation (plus de 23 000 vues à la date de publication de ce rapport).
- en décembre 2021, dans le contexte des fêtes de fin d'année, l'Observatoire alerte le grand public sur les risques de fraude au chèque et rappelle les bonnes pratiques [9] à suivre pour s'en prémunir, en invitant plusieurs organismes de presse à un événement dédié.

Les rubriques liées au chèque ont par ailleurs été enrichies sur les sites institutionnels de la Banque de France [10] (février 2022) et sur le site Assurance Banque Épargne – Info Service (mars 2022) pour mieux sensibiliser les particuliers sur les spécificités du chèque, qui n'est pas un moyen de paiement garanti, et les risques de fraude.

Les rencontres organisées dans le cadre des forums et des programmes d'éducation financière de la Banque de France (programme EDUCFI) ont permis de recueillir des témoignages de particuliers. Ils confirment la présence d'escrocs sur les réseaux sociaux et les forums qui ciblent et démarchent des personnes pour encaisser des chèques frauduleux, souvent contre une promesse de rémunération. Ces personnes encourent alors le risque d'être débitrices de sommes importantes à l'égard de leurs banques et d'être reconnues complices de fraude. Grâce à la multiplication des actions d'éducation financière, les phénomènes d'escroquerie au chèque bancaire semblent aujourd'hui mieux connus du grand public.

Afin de poursuivre et amplifier ces efforts de sensibilisation, la Banque de France a proposé l'intégration d'une fiche spécifique sur les escroqueries au chèque bancaire dans le prochain guide de prévention contre les arnaques. Celui-ci est le fruit d'une coopération inédite des pouvoirs publics et est largement diffusé au sein des administrations centrales, sociales et territoriales. La Banque de France étudiera, en lien avec les autres pouvoirs publics, la possibilité d'une action auprès des plateformes de réseaux sociaux pour assurer leur coopération dans la lutte contre toutes formes d'escroquerie.

L'encadré 3 du présent chapitre fournit quelques informations pratiques pour orienter les victimes de fraude au chèque dans leurs démarches.

2.2.5 Une coopération renforcée des acteurs de la filière chèque grâce à la pérennisation du groupe de travail sur le chèque

Les travaux de lutte contre la fraude avaient mis en exergue la nécessité de structurer la coopération entre les acteurs dans la lutte contre la fraude et de soutenir l'action des forces de l'ordre.

À cette fin, le groupe de travail sur la fraude au chèque a été pérennisé par l'Observatoire dans le cadre d'un mandat de groupe permanent. Ses objectifs sont : i) suivre dans le temps la correcte mise en œuvre des recommandations formulées dans le rapport annuel 2020 de l'Observatoire et leur résultat, ii) structurer la coopération entre les acteurs de la filière et iii) engager les actions de communication à l'attention des utilisateurs de chèques. Le mandat de ce groupe de travail est donné à l'encadré 2.

8 Cf. *https://www.youtube.com/*

9 Cf. *https://www.banque-france.fr/*

10 Cf. *https://particuliers.banque-france.fr/*

Ce groupe de travail veillera notamment à ce qu'un partenariat structuré se mette en place, par l'identification de points de contact principaux, entre les professionnels du traitement de chèque et les forces de l'ordre pour soutenir ces dernières dans leurs actions répressives.

2.3 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.

2.3.1 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 de l'Observatoire de la sécurité des moyens de paiement* 2020.

Dans un contexte de développement rapide du virement instantané, qui pourrait progressivement se substituer au virement classique, voire à d'autres moyens de paiement, l'Observatoire reste particulièrement attentif à la sécurité des paiements en temps réel. En 2021, le virement instantané représentait 2,5 % du nombre total de virements et 0,9 % 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 ainsi été multiplié par près de trois par rapport à 2020. L'augmentation devrait se poursuivre dans les prochaines années, soutenue par les stratégies nationales et européennes pour les moyens de paiement. 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 se rapproche de celui mesuré pour les paiements par carte sans contact (0,014 %, contre 0,013 %). Avec 22 millions d'euros de fraude sur le virement instantané en 2021, soit près de 8 % du total de la fraude recensée sur les virements, l'Observatoire appelle 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.

2.3.2 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 de l'Observatoire de la sécurité des moyens de paiement* 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.

T2 Recommandations de l'Observatoire relatives à la sécurité des paiements en temps réels

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 par des technologies basées 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 plafond et limitation, 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

T3 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 dans le registre des agents financiers – l'annuaire Regafi – ou dans le registre de l'Autorité bancaire européenne)	Utilisateurs
S'informer régulièrement sur les risques numériques et leurs évolutions, par exemple, sur le site du gouvernement *www.cybermalveillance.gouv.fr*	Utilisateurs

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

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

2.3.3 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 de l'Observatoire de la sécurité des moyens de paiement* 2018.

T4 Recommandations de l'Observatoire relatives à la sécurité des paiements par mobile

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

Le paiement par carte au point de vente par l'intermédiaire d'une solution mobile a connu un net développement ces deux dernières années, porté par la crise sanitaire et la possibilité de payer en sans contact au-delà de la limite de cinquante euros. Le nombre de paiements de ce type a ainsi été multiplié par 7,5 entre 2019 et 2021, pour représenter, en 2021, 3 % du nombre de paiements par carte de proximité et 5 % 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 %, a reflué en 2021 pour se rapprocher du niveau moyen des paiements par carte, à 0,074 %. Cette baisse 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.

❷ Mandat du groupe de travail sur le chèque de l'Observatoire

Dans un contexte de baisse rapide des flux de paiement par chèque et de risques toujours élevés en matière de fraude, l'Observatoire a conduit une étude sur la sécurité des paiements par chèque. Elle a été publiée en juillet 2021 dans son rapport annuel 2020. Celle-ci comporte dix recommandations à l'attention des professionnels de la filière, des autorités publiques et des utilisateurs de ce moyen de paiement.

L'Observatoire appelait ainsi à « *structurer durablement la coopération entre les acteurs dans la lutte contre la fraude au chèque et soutenir l'action des forces de l'ordre* » et décidait, pour ce faire, de « *pérenniser le groupe de travail sur la fraude au chèque* » (recommandation n° 9). L'Observatoire appelait également à « *soutenir par un plan de communication la vigilance des utilisateurs dans l'usage du chèque* » (recommandation n° 10). Le présent mandat vise à fixer les objectifs et les moyens de ce groupe de travail permanent de l'Observatoire.

Le groupe de travail sur la fraude au chèque, rattaché à l'Observatoire, aura pour objectifs de :

- suivre dans le temps la correcte mise en œuvre des recommandations formulées par l'Observatoire dans son rapport 2020 ;
- structurer la coopération entre les acteurs de la filière, notamment avec les forces de l'ordre et les plateformes de réseaux sociaux, contre les escroqueries liées à l'encaissement de chèque ;
- engager des actions de communication et de sensibilisation à l'attention des utilisateurs du chèque pour mieux prévenir la fraude.

L'Observatoire donne mandat à la Banque de France, agissant comme secrétaire de l'Observatoire, pour mettre à jour la composition de ce groupe de travail. Celui-ci devra réunir, à l'instar du groupe de travail *ad hoc* chargé de conduire l'étude initiale, des représentants nommés par les membres de l'Observatoire, mais également des établissements et prestataires essentiels de la filière (par exemple : prestataires de fabrication et de traitement des chèques, La Poste, Vérifiance, etc.).

Le groupe de travail « Chèque » se réunira au moins une fois par semestre et rendra compte de ses actions aux réunions plénières de l'Observatoire.

❸

Vous êtes victimes d'une fraude au chèque : que faire ?

1. Contacter sa banque

Que vous soyez un particulier, commerçant ou artisan, vous devez avant toute chose prévenir au plus vite votre établissement bancaire pour étudier avec lui les modalités de limitation du préjudice (mise en opposition des chèques, blocage des opérations, rappel des fonds, changement des données d'authentification, etc.).

2. Déposer une pré-plainte en ligne

Faire une déclaration sur le site du ministère de l'Intérieur « pré-plainte en ligne » pour être reçu ultérieurement par un commissariat ou une unité de gendarmerie.

3. Etre accompagné

- en prenant contact avec Info Escroqueries par téléphone au numéro vert 08 05 80 58 17 (ouvert du lundi au vendredi de 9h à 18h30) ;
- en contactant l'aide aux victimes (écoute, informe et conseille les victimes d'infractions) au numéro 116 006 (appel gratuit) ou au 01 80 52 33 76 (tarification normale) ouvert 7 jours sur 7 de 9h à 19h ou par courriel « victimes@france-victimes.fr » et/ou les associations en mesure de vous aider dans vos démarches (UFC-Que Choisir, Association Force ouvrière consommateurs – AFOC, Association Léo Lagrange pour la défense des consommateurs – ALLDC, Union nationale des associations familiales – UNAF, Association de défense, d'éducation et d'information du consommateur – ADEIC, Prévention Océane, etc.) ;

L'Observatoire appelle les victimes d'escroquerie au chèque à porter systématiquement plainte contre les personnes qui les ont sollicités pour encaisser des chèques frauduleux.

1 Cf. *https://www.pre-plainte-en-ligne.gouv.fr/*

3

L'IDENTITÉ NUMÉRIQUE ET LA SÉCURITÉ DES PAIEMENTS

3.1 Introduction

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 les phénomènes de fraude suivants :

- les usurpations d'identité au moment de **l'entrée en relation**, par exemple dans le cas de l'ouverture d'un compte bancaire sous une fausse identité, avec utilisation ultérieure des moyens de paiement rattachés (chèque, carte bancaire, virement, etc.) [1] ou utilisation comme compte destinataire des fonds frauduleusement acquis ou détournés par ailleurs (par exemple escroquerie aux faux ordres de virement, etc.) ;
- les usurpations de **l'identité du payeur** au moment de l'acte d'achat, malgré les procédures d'authentification, comme l'utilisation frauduleuse d'un espace client commerçant sur lequel une carte bancaire est enregistrée (*card-on-file*), ou encore la souscription par prélèvement à un service en utilisant l'identité et les coordonnées bancaires d'un tiers ;
- les usurpations de **l'identité du bénéficiaire** d'un paiement ou de tout autre interlocuteur pour tromper et manipuler l'initiateur d'une opération de paiement, comme les fraudes sur les sites de vente entre particuliers, les fraudes dites « au président » ou « faux fournisseur », ou plus récemment les fraudes au « notaire ».

La très forte croissance des usages numériques ne s'est en effet pas toujours accompagnée d'une mise à niveau équivalente des processus d'identification et d'authentification. L'identification repose encore souvent sur la vérification d'une copie d'un document officiel d'identité, et l'authentification sur la vérification de la signature manuscrite ou du cachet de l'entreprise. Ce décalage, qui ne s'est pas résorbé avec la crise de la Covid-19 qui a encore accru la dématérialisation des relations administratives et commerciales, crée de nouvelles vulnérabilités qui sont exploitées par les fraudeurs. L'Agence nationale de la sécurité des systèmes d'information (Anssi) estime à environ 400 000 le nombre de déclarations d'usurpation d'identité par an en France, même si toutes ne concernent pas que la sphère financière, et à 6,6 % le nombre d'internautes victimes d'une fraude identitaire sur Internet.

Les utilisateurs possèdent aujourd'hui de nombreuses identités numériques vis-à-vis d'une grande diversité d'établissements publics et privés qui multiplient le nombre d'identifiants et de mots de passe. Pour autant, les utilisateurs ont souvent recours aux mêmes identifiants et aux mêmes mots de passe, si bien que la compromission de l'un de ces espaces utilisateur compromet la sécurité des autres services en ligne. Les fraudeurs réussissent ainsi, par des techniques d'hameçonnage ou de piratage, à collecter de nombreuses données personnelles, y compris des copies des documents officiels d'identité ou des données bancaires. Toutes ces informations leur permettent ensuite de construire un ensemble cohérent de données d'identité qu'ils peuvent utiliser pour leur propre compte ou vendre sur l'Internet caché (*darknet*).

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

1 Selon les données déclarées à la Banque de France, la fraude liée à l'ouverture frauduleuse des comptes bancaires avait concerné 14 748 cas de fraude en 2020 pour un montant total de 19,3 millions d'euros, soit un montant moyen de fraude de 1 311 euros.

électroniques, peuvent aider à améliorer la sécurité générale des moyens de paiement. Au moment de l'entrée en relation, l'identité numérique peut tout d'abord servir à identifier le futur client de manière univoque, même en cas d'homonymie, et créer ainsi un ensemble vérifié d'attributs d'identité. Après l'entrée en relation, l'identité numérique peut servir à authentifier l'utilisateur, pour garantir que le payeur ou le bénéficiaire est bien celui qu'il prétend être. Il existe ainsi un continuum entre l'identité numérique, servant à vérifier les données d'identité déclarées par le client, et les moyens d'authentification, y compris les services de confiance, qui servent à vérifier la régularité de l'usage d'un moyen de paiement ou d'une opération connexe à une transaction.

Au-delà du renforcement de la sécurité des moyens de paiement, l'identité numérique répond aussi à d'autres objectifs d'intérêt général. C'est d'abord un enjeu de protection des utilisateurs dans leurs usages en ligne. L'identité numérique peut ainsi concourir à une meilleure maîtrise et sécurité des données personnelles. C'est ensuite un enjeu économique quand l'identité numérique participe à la confiance et à la sécurisation des échanges administratifs et commerciaux. C'est enfin un enjeu de souveraineté, l'État étant attendu comme le garant ultime de l'identité des personnes dans l'espace numérique comme il l'est dans l'espace physique.

Il existe naturellement une tension entre la multiplication ou la centralisation des identités numériques, chacune des deux approches présentant des avantages et des inconvénients en matière de sécurité et de commodité. La multiplication des identités numériques offre certaines garanties en matière de continuité d'activité et de gestion du risque cyber, mais elle pose la question de l'interopérabilité des solutions. La concentration des solutions d'identité numérique sur un nombre limité de fournisseurs soutient leur usage à grande échelle, mais augmente les risques en cas de compromission de l'identité. En fin de compte, ces choix stratégiques doivent conduire vers des solutions fiables, sécurisées, idéalement interopérables, mais surtout pérennes sur le plan économique afin de garantir un niveau d'adoption satisfaisant par les utilisateurs.

Certains schémas de fraude reposent toujours sur l'usurpation d'identité de personnes morales, comme dans le cas de la fraude au « faux fournisseur » ou plus récemment de la fraude aux dispositifs d'aide exceptionnelle aux entreprises durant la crise. Toutefois, aujourd'hui, les risques d'usurpation d'identité portent principalement sur l'identité de personnes physiques. Pour cette raison, la présente étude de veille de l'Observatoire porte sur l'identité numérique des personnes physiques.

3.2 Les standards de l'identité numérique et l'écosystème français et européen

3.2.1 Définitions

L'identité numérique fait généralement intervenir trois acteurs : l'utilisateur, le fournisseur de services et enfin le fournisseur d'identité agissant comme tiers de confiance. Pour assurer leur mise en relation et fournir la passerelle technique, un quatrième type d'acteur peut intervenir : il s'agit des fédérateurs d'identité, comme FranceConnect en France. Au préalable, il convient de toujours bien distinguer **l'identification**, qui consiste à vérifier l'identité de l'utilisateur en rattachant un ensemble d'attributs d'identité à une personne unique, de **l'authentification**, qui permet à l'utilisateur d'utiliser un service en s'appuyant sur une identification préalablement réalisée et par conséquent vérifiée. En fonction de sa conception et des cas d'usage, une solution d'identité numérique peut à la fois être utilisée comme moyen d'identification et comme moyen d'authentification.

L'utilisateur

L'utilisateur est la personne physique souhaitant accéder à un ensemble de services en ligne aussi bien publics que privés. Son identité est définie par l'état civil. Elle peut en apporter la preuve par l'intermédiaire de ses documents officiels d'identité, délivrés par les services de l'État, comme le passeport, la carte nationale d'identité ou le titre de séjour[2]. L'utilisateur peut aussi apporter la preuve de son identité par des documents administratifs, comme la carte vitale ou les cartes professionnelles, même si ces documents ne sont pas des titres d'identité officiels.

Le fournisseur de services

Le fournisseur de services est l'opérateur public ou privé qui met à la disposition de l'utilisateur, ou le lui vend, un ensemble de services en ligne (administrations, commerçants, applications mobiles, réseaux sociaux, etc.). L'accès à ces services est souvent conditionné à une identification préalable de l'utilisateur. Cette phase passe, le plus souvent, par la création d'un compte utilisateur unique, propre à ce service et à ce fournisseur. Le niveau de sécurité de ces identités numériques varie en fonction de la nature du service proposé. C'est la raison pour laquelle la loi du 7 octobre 2016 pour une République numérique a réservé l'imputabilité juridique de l'identité

numérique aux seuls « *moyens d'identification électronique présumés fiables* » [3].

Toutefois, l'usage de ces moyens d'identification électronique présumés fiables est aujourd'hui marginal. De plus, pour la plupart des sites Internet et des fournisseurs de services, les identités numériques reposent sur des processus d'identification faiblement sécurisés pour lesquels l'identification reste déclarative. Ces identifications déclaratives permettent de constituer et d'enrichir le fichier utilisateur ou le fichier client, mais le fournisseur de services ne vérifie pas les attributs d'identité présentés par l'utilisateur. La vérification d'identité est beaucoup plus développée chez des opérateurs comme les banques ou les administrations, en réponse aux exigences réglementaires de lutte contre le blanchiment d'argent et de lutte contre la fraude. Toutefois, même chez ces opérateurs, la vérification d'identité repose encore souvent sur la vérification d'une copie du document officiel d'identité. Ensuite, selon le domaine métier, l'utilisateur est authentifié :

- soit avec une authentification multifacteur, c'est-à-dire avec plusieurs facteurs d'authentification différents comme dans le cas des banques, des autres prestataires de services de paiement et de quelques rares fournisseurs de services comme certaines messageries électroniques ou réseaux sociaux ;
- soit à l'aide d'un simple identifiant et d'un mot de passe, c'est le cas de la plupart des administrations, des commerçants et des applications mobiles.

Le fournisseur d'identité ou tiers de confiance

Le fournisseur d'identité, qui est un tiers de confiance, va permettre de faire le lien entre le fournisseur de services et l'utilisateur. Sa fonction est de s'assurer de la correspondance entre les attributs présentés par l'utilisateur et leur véracité [4]. Le tiers de confiance peut assurer les deux fonctions suivantes, distinctes ou cumulées :

- **Autorité de délivrance ou fournisseur d'identité originelle** : elle attribue l'identité originelle en vérifiant notamment l'état civil de l'utilisateur, par exemple via le répertoire national d'identification des personnes physiques (RNIPP) tenu par l'Institut national de la statistique et des études économiques (Insee). À titre d'exemple, l'autorité de délivrance de la carte nationale d'identité est l'État, via la chaîne de délivrance et les outils mis en œuvre par l'Agence nationale des titres sécurisés (ANTS), placée sous la tutelle du ministère de l'Intérieur. La délivrance en mairie, qui intervient après la validation du dossier au niveau de la préfecture (centre d'expertise et de ressources titres), permet ainsi de vérifier et sécuriser le lien entre l'identité physique de la personne (photographie, empreinte digitale) et son état civil.
- **Fournisseur d'identité vérifiée** : le tiers de confiance assure alors la gestion au quotidien de cette identité numérique et procède à sa confirmation auprès du fournisseur de services. L'identité attestée auprès du fournisseur de services dérive nécessairement d'une identité originelle. Le fournisseur d'identité confirme donc auprès du fournisseur de services les données fondamentales d'état civil que prétend détenir l'utilisateur du service (nom, prénom, sexe, date et lieu de naissance).

Afin d'enrichir un profil et de garantir une identification encore plus fortement sécurisée, un tiers de confiance peut également fournir des attributs supplémentaires concernant l'utilisateur, qui ne sont pas à proprement parler des attributs d'identité. Cela peut être, par exemple, un diplôme, l'exercice d'une profession, la valeur d'un revenu fiscal, l'adresse du domicile, etc. Parmi ces tiers de confiance, certains sont autorisés comme prestataires de service d'information sur les comptes (PSIC) à récupérer des données sensibles auprès des banques, telles que l'IBAN *(international bank account number)*, le numéro de téléphone ou encore l'adresse du domicile.

Le fédérateur d'identité

Le fédérateur d'identité offre la possibilité aux utilisateurs de choisir parmi plusieurs fournisseurs d'identité. Les fournisseurs de services donnent ainsi accès à leurs services par l'intermédiaire de plusieurs fournisseurs d'identité, grâce à un seul dispositif assurant le rôle de passerelle technique et la promotion d'une même identité visuelle. En France, cette fonction est principalement assurée par FranceConnect, qui donne accès à deux plateformes distinctes : FranceConnect qui fédère des fournisseurs d'identité de niveau de garantie eIDAS [5] faible, et FranceConnect+ qui fédère des fournisseurs d'identité de niveaux de garantie eIDAS substantiel et élevé. FranceConnect joue également le rôle de vérificateur des états civils : à chaque utilisation d'une identité, et, quel que soit son fournisseur, la plateforme consulte le RNIPP afin de s'assurer de l'existence de l'utilisateur et de l'absence d'homonymie.

2 Le permis de conduire est également considéré comme une pièce d'identité officielle puisqu'il est délivré par l'État. Toutefois, il n'a pas la même valeur que la carte nationale d'identité ou le passeport, qui sont les seuls à certifier à la fois l'identité et la nationalité de leur titulaire.

3 Article L. 136 du Code des Postes et des Communications électroniques : « *La preuve d'identité pour un service public en ligne peut être apportée par un moyen d'identification électronique présumé fiable*. »

4 Il existe en France des acteurs économiques spécialisés dans le domaine de la vérification de l'identité électronique. Ces acteurs appartiennent au secteur économique dit de la « confiance numérique » et sont représentés au sein de l'Alliance pour la confiance numérique.

5 *Electronic IDentification Authentication and trust Services.*

3.2.2 Normes et standards

Le règlement eIDAS

Le règlement de l'Union européenne n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance, dit règlement « eIDAS » (*Electronic IDentification Authentication and trust Services*), établit un cadre d'interopérabilité. Il formule ainsi des exigences relatives à la reconnaissance mutuelle entre États membres des moyens d'identification électronique et des services de confiance pour l'accès aux services publics et à leurs effets juridiques. Il n'est donc pas directement applicable pour l'utilisation des services marchands, y compris l'utilisation des moyens de paiement.

Pour **l'identification électronique (eID)**, le règlement prévoit que chaque État membre puisse notifier à la Commission européenne des moyens d'identification électronique délivrés dans le cadre de schémas. Ceux-ci sont évalués par les pairs et sont ensuite qualifiés selon les trois niveaux de robustesse définis par le règlement : faible, substantiel et élevé. Un premier schéma français d'identité constitué du tandem FranceConnect+ et L'Identité Numérique La Poste est en cours de notification au niveau de confiance substantiel *(cf. encadré 4* infra*)*.

Pour les **services de confiance**, le règlement en reconnaît cinq[6] et leur associe certains effets juridiques notamment en matière de présomption d'intégrité. Le règlement instaure un régime de qualification des prestataires de services de confiance (PSCQ). Cette qualification est décernée par un organe de contrôle – l'Agence nationale de sécurité des systèmes d'information (Anssi) en France – et prend en compte les résultats d'un audit de conformité effectué par un organisme accrédité. Le règlement eIDAS aboutit ainsi à différents niveaux de sécurité pour les services de confiance (simple, avancé ou qualifié). Les services de confiance qualifiés sont nécessairement fournis par un PSCQ, tandis que les signatures électroniques avancées doivent satisfaire à quatre exigences définies à l'article 26 du règlement eIDAS.

La reconnaissance par le droit bancaire et financier de l'identité numérique

La réglementation bancaire et financière reconnaît progressivement l'intérêt de ces moyens d'identification électronique et de ces services de confiance. Ainsi l'article R. 561-5-1 du Code monétaire et financier modifié par le décret n° 2021-387 du 2 avril 2021 indique qu'un moyen d'identification électronique certifié de niveau substantiel ou élevé par l'Anssi suffit pour vérifier l'identité du client lors d'une entrée en relation. Il s'agit d'une évolution réglementaire structurante pour les procédures d'ouverture de compte bancaire, et donc de fourniture de moyens de paiement. Lorsque de telles solutions ne peuvent être mises en œuvre, l'article R. 561-5-2 créé par le décret n° 2020-118 du 12 février 2020 permet aux établissements financiers de recourir à des services de confiance qualifiés ou à des services d'entrée en relation d'affaires à distance certifiés conformes par l'Anssi.

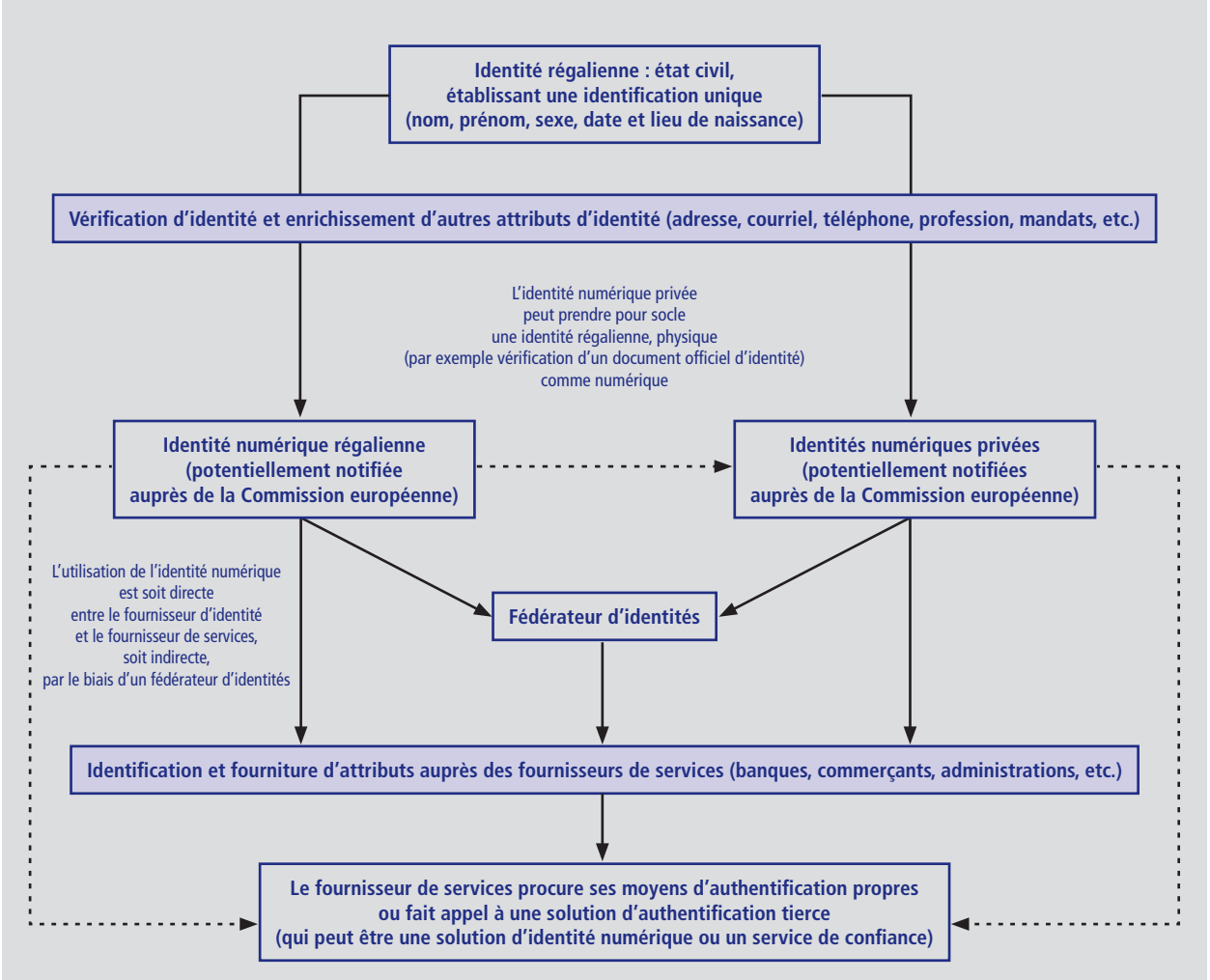
La deuxième directive européenne sur les services de paiement (DSP 2) a introduit le principe d'authentification forte pour les opérations de paiement électronique, qui doit reposer sur l'utilisation d'au moins deux éléments indépendants appartenant aux trois catégories que sont la connaissance, la possession et l'inhérence. Le cadre réglementaire édifié par la DSP 2 et par les textes de second niveau prévoit également la possibilité pour l'émetteur du moyen de paiement de déléguer l'authentification forte à un tiers, à condition de respecter les règles applicables en matière d'externalisation dans le domaine bancaire[7]. Dans les faits, cette délégation s'accompagne d'un transfert d'une partie des risques et des responsabilités. Dans ce contexte, les solutions d'identité numérique peuvent constituer un moyen d'authentification des utilisateurs de moyens de paiement, à condition d'être reconnues comme telles par les établissements bancaires et de satisfaire aux exigences de la DSP 2.

3.2.3 Panorama des identités numériques

L'identité régalienne

Organisé par la loi et prérogative de souveraineté, l'état civil permet l'individualisation des personnes tout en maintenant un socle commun puisque chacun est identifié selon les mêmes caractéristiques (nom de naissance, prénom(s), date et lieu de naissance, sexe). L'identité se comprend donc comme un ensemble stable de données d'identité permettant d'établir qu'une personne est bien celle qu'elle prétend être ou que l'on présume être. L'identité numérique régalienne est la capacité à prouver de façon numérique et sécurisée les attributs de son identité civile. Tout comme on peut, dans l'espace physique, recourir aux documents officiels d'identité pour prouver son identité (par exemple : présenter sa carte nationale d'identité pour un paiement par chèque), l'identité numérique régalienne permettrait de prouver son identité dans l'espace numérique et sécuriser les démarches administratives et commerciales, de plus en plus dématérialisées.

Le projet d'identité numérique porté par le programme France Identité Numérique vise à répondre à ce besoin. Le déploiement de la carte nationale d'identité électronique (CNIe), à partir de 2021, constitue le socle de la solution d'identité numérique régalienne qui



pourrait être proposée à l'ensemble des Français et dont les contours ont été définis par le décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN). Dérivée de ce titre d'identité, l'activation de cette identité numérique sera proposée à l'utilisateur au moment du retrait de la CNIe. Cette identité numérique fonctionnerait en lien avec le fédérateur d'identité FranceConnect+ et constituerait un moyen d'atteindre un niveau de sécurité élevé au regard des normes européennes. D'autres pays européens disposent d'ores et déjà d'une identité numérique régalienne de niveau élevé, à l'image de l'Estonie [8].

6 1) La délivrance de certificats qualifiés pour la signature électronique, le cachet électronique et l'authentification de sites Internet ; 2) la validation des signatures/cachets électroniques qualifiés ; 3) la conservation qualifiée des signatures/cachets électroniques qualifiés ; 4) l'horodatage électronique qualifié ; et 5) l'envoi recommandé électronique qualifié.

7 Notamment les orientations relatives à l'externalisation de l'Autorité bancaire européenne (ABE, *European Banking Authority* – EBA) du 25 février 2019, EBA/GL/2019/02, reprises dans l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur bancaire et soumis au contrôle de l'Autorité de contrôle prudentiel et de résolution (ACPR).

8 La liste des moyens d'identification électroniques prénotifiés et notifiés à la Commission européenne est accessible par le lien Internet suivant :

Overview of pre-notified and notified eID schemes under eIDAS - eID User Community - CEF Digital (europa.eu)

La carte nationale d'identité électronique (CNIe)

Le règlement (UE) 2019/1157 du Parlement et du Conseil du 20 juin 2019 oblige les États membres à mettre en circulation des cartes d'identité comportant des données biométriques, empreintes digitales et photographies, dans un composant électronique hautement sécurisé. Ce composant électronique prend la forme d'une puce, comme celle des cartes bancaires avec ses processeurs et ses mémoires. Un tel dispositif, qui existe déjà sur les passeports biométriques, permet de renforcer la lutte contre la fraude documentaire et l'usurpation d'identité, en vérifiant la cohérence entre les données qui sont lisibles sur le titre, celles qui sont inscrites dans la puce et celles que présente son porteur (par exemple son empreinte biométrique). La délivrance de la CNIe est permise par le décret n° 2021-279 du 13 mars 2021. Dans le détail, la puce de la CNIe inclut deux compartiments complètement indépendants comportant chacun son propre jeu de données et sa propre application :

- **Le premier compartiment, communément appelé « application ICAO [9] »**, est associé à un usage régalien de contrôle d'identité. Ce contrôle peut se faire sur présentation physique de la CNIe et ne peut être réalisé qu'avec le consentement du porteur, et dans le cas des empreintes, que par des personnes habilitées à réaliser des contrôles d'identité comme les forces de police. Ce compartiment est disponible et actif pour toutes les CNIe actuellement délivrées aux citoyens.
- **Le deuxième compartiment, communément nommé « application Pace + PIN »**, est associé à un usage d'identification et d'authentification numériques. Il ne contient pas de données biométriques. Il contient les seules données nécessaires pour l'usage de services à distance comme le commerce en ligne ou des démarches administratives. Son mode de fonctionnement est similaire à une carte bancaire, car il utilise un code PIN à six chiffres comme facteur d'authentification du citoyen. Cette application est aussi possible, mais actuellement bloquée en matière d'accès pour toutes les CNIe actuellement livrées en France [10].

La CNIe comporte également un cachet électronique visible (CEV), qui est un code à barres à deux dimensions comportant les informations clés du titre d'identité. Ces données sont verrouillées par une signature électronique du *hash* de ces données, garantissant l'origine et l'intégrité de l'ensemble formé du nom, du prénom et du numéro de titre. Les données contenues dans le CEV doivent ensuite correspondre à celles lisibles à l'œil nu. La lecture du CEV suppose le recours à une application sécurisée capable de contrôler la signature au moyen de la clé publique

CNIe

Face avant de la carte

Face arrière de la carte

Crédits : Ministère de l'Intérieur.

mise à disposition par l'organisme émetteur. Cette lecture n'est toutefois pas limitée, grâce à son standard ouvert, qu'aux personnes autorisées par la loi à faire des contrôles d'identité.

Le service de garantie de l'identité numérique, la future identité numérique française

Le service de garantie de l'identité numérique (SGIN) est conçu par les services du ministère de l'Intérieur et de l'Agence nationale des titres sécurisés (ANTS). Une version d'essai est disponible pour 1000 bêta-testeurs depuis le 11 mai 2022. Le SGIN doit permettre aux citoyens de s'authentifier fortement pour l'accès aux services en ligne (justificatif d'identité, procuration pour un retrait de colis, preuve de majorité, authentification sur les sites publics accessibles, etc.). Cette identité numérique sera sécurisée par la puce d'un titre d'identité, la carte d'identité nationale électronique dans un premier temps, le passeport ou le titre de séjour électronique ultérieurement.

Concrètement, le SGIN va prendre la forme d'une application mobile. La création d'un compte dans le SGIN repose sur la lecture des données de la puce du titre d'identité avec un *smartphone* équipé de la technologie sans contact NFC. Lorsque l'utilisateur s'authentifiera par cette application,

les données pouvant être transmises aux fournisseurs de services liés par convention à FranceConnect seront le nom, le nom d'usage, les prénoms, la date et le lieu de naissance, le sexe ainsi que le courrier électronique si cette dernière information est renseignée par l'usager.

Les données les plus sensibles sont réservées à des fournisseurs de services liés par convention au ministère de l'Intérieur et à l'Agence nationale des titres sécurisés (ANTS). Ce service n'est pas à caractère obligatoire et les usagers déjà enrôlés auront la possibilité de le résilier à tout moment en désinstallant simplement l'application. Il s'agira toutefois du seul dispositif, pour les prochaines années, accessible à tous les citoyens français fournissant une identité numérique de niveau élevé au sens des normes européennes.

Les fournisseurs d'identité numérique privés

Il existe quatre catégories de fournisseurs d'identité numérique privés sur le marché français aujourd'hui.

Les **fournisseurs d'identité déclarative** sont principalement des acteurs internationaux du numérique comme Google, Facebook, LinkedIn ou Apple. Leurs solutions de « *single sign-on* » ou SSO permettent à un utilisateur de s'identifier sur un site commercial ou un service en ligne avec les identifiants de son compte. L'identité est celle déclarée par l'utilisateur. Elle est très rarement vérifiée. Un utilisateur peut même détenir plusieurs identités en créant des comptes différents auprès d'un même fournisseur. Malgré ces faiblesses, le SSO reste fréquemment utilisé aujourd'hui pour s'identifier auprès des fournisseurs de services privés (par exemple sites marchands, sites d'information, réseaux sociaux, etc.).

Les **fournisseurs d'identité faible** correspondent au premier niveau du règlement eIDAS. Ils effectuent un contrôle de l'identité du demandeur et de sa validité en vérifiant la conformité d'une copie de la pièce d'identité avec une photographie du demandeur. La majorité des solutions d'identité référencées par le fédérateur FranceConnect, comme les Impôts, l'Assurance Maladie ou la Mutuelle sociale agricole, se trouvent aujourd'hui dans cette catégorie, car elles sont associées à des processus d'authentification à un seul facteur, de type « identifiant » et « mot de passe ».

Les **fournisseurs d'identité substantielle** correspondent au deuxième niveau du règlement eIDAS avec une vérification robuste de l'identité du demandeur pour réduire substantiellement le risque d'utilisation abusive ou d'altération d'identité. Le niveau substantiel est en principe équivalent à une vérification d'identité en présentiel. L'utilisation d'une identité substantielle requiert une authentification multifacteur. Ces solutions doivent obtenir l'agrément de l'Anssi et se conformer aux exigences applicables aux prestataires de vérification d'identité à distance (PVID) lorsque la vérification de l'identité se fait à distance. La seule solution d'identité substantielle disponible en France actuellement est L'Identité Numérique La Poste.

Les initiatives d'identité numérique en lien avec les paiements à l'extérieur de la France

BankID

BankID a été lancée en 2003 en Suède en tant que solution d'identification numérique. BankID est proposée par les banques scandinaves participant au consortium dans un cadre réglementaire commun qui répond aux exigences de l'Autorité suédoise d'administration numérique. Cette solution est utilisable via le *smartphone* de l'utilisateur et exploitée par une entité centralisée (eID *scheme*). Les banques agissant comme entités de confiance (*trusted entities*) sont responsables de l'utilisation du *scheme*. Une signature avec BankID relève des services de confiance du règlement eIDAS en tant que signature électronique avancée. BankID offre aux sites e-commerce et aux banques une solution d'authentification forte des paiements conforme à la directive DSP 2, dès lors que cette solution est reconnue par la banque du payeur et que l'authentification contient le lien dynamique de la transaction. En Suède, BankID représenterait plus de la moitié des authentifications pour l'accès aux comptes bancaires.

itsme

Introduite en 2017, itsme est une application mobile d'identité numérique en Belgique. Belgian Mobile ID, un consortium réunissant les trois plus grands opérateurs télécoms de Belgique et quatre grandes banques, est à l'origine de cette application. Elle permet aux utilisateurs de s'identifier et de s'authentifier en ligne à l'aide de leur *smartphone* de manière sécurisée. L'application a été accréditée par le gouvernement belge en tant que forme officielle d'identité numérique en 2018, et notifiée au niveau européen en décembre 2019 avec le niveau de garantie élevé. itsme propose ainsi une solution d'authentification forte conforme à la directive DSP 2.

9 *International Civil Aviation Organization* – ICAO, Organisation de l'aviation civile internationale – OACI.

10 En revanche, la Principauté de Monaco a intégré cette possibilité avec l'identité numérique MConnect où le titre d'identité est lu en mode NFC (*Near Field Communication*) par le *smartphone*, le code PIN étant tapé sur ce dernier pour fiabiliser la création de l'identité numérique.

3.2.4 Les outils

Les services de vérification d'identité à distance

Une vérification d'identité à distance possède la même finalité qu'une vérification d'identité en face-à-face. À ce titre, un service de vérification d'identité à distance permet de vérifier que le titre d'identité présenté par l'utilisateur est authentique et que l'utilisateur en est le détenteur légitime. La principale menace lors d'une vérification d'identité, qu'elle ait lieu en face-à-face ou à distance, est l'usurpation d'identité. Un service de vérification d'identité à distance est ainsi exposé aux mêmes risques qu'une vérification d'identité en présentiel (pièces d'identité contrefaites). Mais, de par sa nature, il est également exposé à des risques spécifiques : manipulation numérique des images (*deepfakes*), injection de données frauduleuses, tentatives répétées et massives d'usurpation, utilisation de masques, etc.

Pour répondre à ces risques, l'Anssi a élaboré et publié en 2021 un ensemble de règles et de recommandations rassemblées dans le référentiel des prestataires de vérification d'identité à distance (PVID). Les exigences formulées par ce référentiel portent sur le prestataire et la sécurité du système d'information permettant de fournir le service de vérification d'identité à distance. Il vise à créer une offre de services de vérification d'identité à distance robuste et répondant aux besoins des utilisateurs, des fournisseurs de services et des régulateurs. Ce référentiel permet aussi d'attester la mise en œuvre de mesures pertinentes de réduction de la fraude. L'élaboration de ce référentiel s'inscrit dans le cadre de travaux menés en collaboration avec la direction générale du Trésor pour la certification des services d'entrée en relation d'affaires à distance des établissements financiers. **Six prestataires de vérification d'identité à distance sont en cours de certification par l'Anssi. Toutefois, aucun n'est encore certifié à ce jour [11].**

Les moyens d'authentification et les signatures électroniques qualifiées

La procédure d'authentification doit permettre de prouver au fournisseur de services que l'utilisateur qui se connecte est bien le même que celui qui s'est initialement identifié lors de la procédure d'enrôlement. Cette authentification peut être faible (un seul facteur d'authentification, par exemple identifiant/mot de passe) ou multifacteur (plusieurs facteurs indépendants les uns des autres parmi trois catégories : ce que je suis, ce que je sais, ce que je possède). Une solution d'identité numérique peut être utilisée comme moyen d'authentification mono- ou multifacteur.

Les moyens d'authentification peuvent s'appuyer sur des signatures électroniques qualifiées, dont les règles sont encadrées par le règlement eIDAS. Ces signatures doivent reposer sur un certificat de signature électronique qualifié, mis en œuvre grâce à un dispositif de création de signature électronique qualifiée (*Qualified electronic Signature Creation Device* – QSCD). Ce dispositif fait l'objet d'une décision de certification par une autorité nationale, l'Anssi en France. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite (article 25 du règlement eIDAS) [12]. Les signatures électroniques qualifiées selon le règlement eIDAS permettent de garantir, avec un haut niveau de confiance, qu'elles ne peuvent être réalisées que par leur signataire légitime. Les processus de vérification de l'identité du demandeur, de délivrance et de gestion du cycle de vie d'un certificat de signature électronique qualifiée répondent à des exigences de sécurité correspondant au niveau substantiel. Ces processus permettent de garantir que ce certificat est uniquement délivré au signataire légitime.

Il existe d'autres moyens d'authentification tels que les jetons à usage unique sur la base d'un secret partagé appelé *seed*. Le jeton est généré sur une clé USB dédiée à cet usage ou sur une application sur *smartphone*. Lors d'une authentification, le serveur d'authentification forte calcule le même jeton que le client à partir de son horloge (temps universel coordonné – UTC). Il y ajoute le code PIN de l'utilisateur enregistré dans sa base de données, puis compare ces données avec celles fournies par l'utilisateur, à savoir le code PIN suivi du jeton généré.

Devant l'hétérogénéité des solutions d'authentification, des industriels ont formé l'Alliance FIDO (*Fast Identity Online*) dans le but de définir des standards pour l'authentification qui soient simples, sûrs et standardisés. L'Alliance FIDO a été créée en 2013 pour transformer l'authentification en ligne en développant des standards ouverts et interopérables qui exploitent la cryptographie à clé publique [13]. L'Alliance FIDO a publié plusieurs standards dont le dernier, FIDO2, élaboré conjointement avec le *World Wide Web Consortium* (W3C). Il intègre l'authentification multifacteur nativement dans les navigateurs web et différents systèmes d'exploitation comme Android, iOS, Windows ou macOS. L'authentification FIDO s'appuie sur un premier facteur de possession, l'appareil authentificateur, et sur un second facteur de connaissance ou d'inhérence. La biométrie est particulièrement utilisée dans les solutions FIDO proposées par le marché aux particuliers, tandis que la clé USB physique est la forme la plus adoptée par le marché à destination des entreprises.

L'authentification FIDO se déroule en deux étapes. D'abord, l'**étape de vérification de l'utilisateur** consiste en la mise

en œuvre du facteur de connaissance ou d'inhérence (entrer un code porteur, scanner son visage ou apposer l'empreinte digitale). Ces informations sont transmises à l'authentificateur pour vérification locale, afin de limiter les risques de piratage de bases centrales de données et le cas échéant de répondre aux exigences de protection des données biométriques. Ensuite, l'**étape d'authentification en ligne** prouve la possession de l'authentificateur FIDO. Lors de cette étape, le serveur du prestataire envoie un message à l'authentificateur qui est ensuite signé par une clé privée stockée dans l'authentificateur. La réponse signée est retournée au prestataire et sa vérification positive complète l'authentification multifacteur de l'utilisateur. Dans le domaine du paiement, une banque espagnole a utilisé le standard FIDO pour utiliser la biométrie lors de l'enrôlement des nouveaux clients via différents canaux en comparant une capture dynamique du visage de l'utilisateur et les photos de ses pièces d'identité. Un fournisseur de cartes de crédit en Allemagne a déployé une solution FIDO compatible avec les standards EMV (Europay Mastercard Visa) sur ses cartes de paiement pour une authentification forte à base de jetons FIDO, sans recours à un mot de passe ou un code à usage unique.

3.3 Les usages de l'identité numérique pour renforcer la sécurité des paiements

3.3.1 Les pratiques actuelles en matière d'identification et d'authentification

L'identification, l'enrôlement, et l'entrée en relation

Selon le règlement eIDAS (article 3), l'identification électronique est « *le processus consistant à utiliser des données d'identification personnelles sous une forme électronique représentant de manière univoque une personne physique* ». Ainsi, un moyen d'identification électronique est un « *élément matériel ou immatériel contenant des données d'identification personnelles et utilisé pour s'authentifier pour un service en ligne* ».

Intégrée dans un processus de connaissance du client (KYC – *Know Your Customer*), l'identification électronique permettrait de pallier les risques liés à la vérification d'identité à distance, principalement l'usurpation d'identité et la fraude documentaire. Les tentatives de fraude lors d'un enrôlement à distance sont plus nombreuses que lors d'une entrée en relation en face-à-face, en raison de la simplicité des démarches numériques et des difficultés de contrôle à distance de la concordance entre un document d'identité et la personne réalisant la démarche.

Dans le cadre des récentes évolutions du dispositif législatif et réglementaire relatif à la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT), l'usage de l'identité numérique et des services de confiance qualifiés pour l'entrée en relation est en rapide développement dans les services financiers, en lien avec le nouveau référentiel de l'Anssi sur les prestataires de vérification d'identité à distance.

Toutefois, cela ne traite pas l'ensemble des enjeux de sécurité des moyens de paiement. D'une part, les exigences en matière d'entrée en relation ne sont applicables qu'aux seules personnes assujetties aux obligations de LCB-FT, c'est-à-dire principalement les établissements financiers. Elles ne sont pas applicables aux autres fournisseurs de services (opérateurs téléphoniques, commerçants, administrations, etc.). D'autre part, contrairement à d'autres communautés bancaires, les établissements financiers en France ne se sont pas positionnés comme fournisseurs d'identité ou de moyens d'authentification. Ils pourraient toutefois jouer ce rôle à l'avenir, de façon à ce que leurs standards élevés de sécurité soient accessibles à d'autres acteurs de la chaîne des paiements.

Recommandation de l'Observatoire

Au moment de l'entrée en relation, l'Observatoire encourage les établissements financiers à recourir, dans le cadre des règles applicables en matière de lutte contre le blanchiment 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'Anssi applicables aux prestataires de vérification d'identité à distance (PVID).

L'Observatoire invite également les établissements non assujettis aux obligations de lutte contre le blanchiment et le financement du terrorisme, qui concourent à la sécurité des paiements, comme les opérateurs téléphoniques ou les commerçants, à recourir à des moyens d'identification

…/…

11 La liste des prestataires candidats à la certification de l'Anssi est disponible à l'adresse Internet suivante : *https://www.ssi.gouv.fr*

12 En droit français, l'article 1367 du code civil dispose aussi que la signature électronique est équivalente à une signature manuscrite, si elle repose sur un « *procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* » étant noté que « *la fiabilité du procédé est présumée lorsque la signature est créée, l'identité de la signature assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* ». Le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique indique qu'un procédé est présumé fiable s'il met en œuvre une signature électronique qualifiée au sens du règlement eIDAS.

13 Aujourd'hui, FIDO compte plus de 250 membres appartenant aux secteurs des technologies de l'information, des communications, du matériel et des logiciels, des services financiers, des soins de santé, du gouvernement, etc.

électroniques de niveau substantiel ou à des solutions d'identité numérique apportant un niveau de sécurité équivalent pour authentifier leurs utilisateurs :

- pour les opérateurs téléphoniques, cela permettrait de sécuriser l'entrée en relation et les opérations ultérieures, notamment les changements de carte SIM ou les demandes de eSIM pour prévenir les fraudes reposant sur des techniques de *SIM-swapping*, qui affectent encore la sécurité des dispositifs d'authentification forte des établissements financiers ;
- pour les commerçants, les places de marché et les plateformes de vente entre particuliers, leurs transactions seraient dans l'ensemble mieux sécurisées si l'accès aux espaces clients reposait sur des solutions d'identité numérique de niveau substantiel, en particulier quand ces espaces client permettent de réaliser des opérations de paiement (par exemple achat par *card-on-file* ou virement sur un compte bancaire des opérations de vente réalisées).

L'Observatoire note que la diffusion de ces usages plus sécurisés peut être facilitée et soutenue par des fédérateurs d'identité comme FranceConnect+.

L'authentification des opérations de paiement ou des opérations connexes

À la différence de l'identification, l'authentification vise à prouver une identité et non à l'établir. L'identification désigne le fait de créer une identité numérique, en matière de paiement. L'authentification, quant à elle, est une procédure visant à vérifier la légitimité de l'utilisateur utilisant un instrument de paiement. La DSP 2 pose le principe de l'authentification forte pour toute opération de paiement électronique et pour toute opération sensible réalisée à distance. À l'heure actuelle, l'usage d'une identité numérique pour réaliser une authentification forte sous le régime DSP 2 reste plutôt limité en Europe (*cf. les usages de BankID en Suède ou de itsme en Belgique*) et quasi inexistant en France, les solutions d'authentification fortes étant souvent des solutions propriétaires déployées par les émetteurs de moyens de paiement. Néanmoins, ce cas d'usage porte des perspectives intéressantes en matière de fluidité des parcours clients, à condition que le niveau de sécurité de ces identités numériques soit au moins équivalent à celui obtenu par les solutions propriétaires, c'est-à-dire de niveau substantiel selon l'Anssi.

Les autres opportunités pour la sécurité des paiements

Dans certains cas d'usage tels que la mise en place de mandats de prélèvement, le recours à la signature électronique devient peu à peu la norme à mesure que les entreprises se numérisent. La réglementation SEPA (*Single Euro Payments Area*) ne précise pas explicitement comment un mandat doit être signé par le payeur. Le Conseil européen des paiements (*European Payments Council* – EPC) exige une forme de signature contraignante sans imposer de solutions techniques sur les signatures électroniques. Utiliser une solution d'identité numérique ou une solution de signature électronique avancée ou qualifiée reconnue par le règlement eIDAS, pour signer un mandat de prélèvement permettrait d'avoir des données plus solides sur le payeur qui a autorisé la transaction en cas d'opposition ou de contestation du paiement. De telles solutions ont également un intérêt pour sécuriser la communication des coordonnées bancaires, de façon à ce que la personne qui les reçoit puisse s'assurer de l'authenticité de celles-ci.

Recommandation de l'Observatoire

L'Observatoire encourage les administrations et les entreprises à 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 comme :

- la signature d'un mandat de prélèvement, de façon à sécuriser les transactions en cas d'opposition ou de contestation du paiement ;
- la communication de nouvelles coordonnées bancaires (par exemple changement d'IBAN – *international bank account numbers*, communication d'un nouveau relevé d'identité bancaire), de façon à prévenir les risques de détournement de fonds.

3.3.2 La vigilance des utilisateurs

En parallèle des solutions d'identité numérique, la vigilance des utilisateurs reste essentielle pour prévenir les risques d'usurpation d'identité, qui affectent la sécurité générale des moyens de paiement.

Principe 1 : limiter la diffusion des données personnelles sensibles au strict nécessaire

- Ne donnez que le minimum d'informations personnelles nécessaires sur un site ou service en ligne et lorsque cela est possible utilisez des pseudonymes au lieu de vos nom et prénom.
- Vérifiez les paramètres de confidentialité de vos informations personnelles données sur Internet et les réseaux sociaux pour que celles-ci ne soient pas publiques.

Principe 2 : vérifier toujours la légitimité de votre interlocuteur

- Vérifier que le canal de communication est habituel et n'ouvrez pas les messages suspects ni leurs pièces jointes, et ne cliquez jamais sur les liens.
- Ne communiquez jamais d'informations personnelles sensibles (mots de passe, numéro de sécurité sociale,

pièces d'identité, avis d'imposition, relevé d'identité bancaire) à des personnes ou organismes que vous n'avez pas authentifiés avec certitude.
- Faites attention à qui vous parlez sur Internet ou par téléphone, car les cybercriminels se font souvent passer pour des organismes officiels ou des contacts connus pour vous dérober vos informations d'identité.
- Si votre interlocuteur connaît déjà certaines de vos données personnelles (votre numéro de téléphone, adresse, etc.), demander la source de ces informations et vérifier qu'elles ont été collectées dans un cadre que vous avez autorisé.

Principe 3 : si nécessaire, utiliser des canaux sécurisés pour la transmission de vos données personnelles

- Privilégiez les messageries et espaces sécurisés, par exemple fournis par les établissements financiers, pour la communication de ces données.

Principe 4 : protéger vos environnements de stockage des données personnelles sensibles

- Utilisez des mots de passe différents et complexes pour chaque site et application en tenant compte des nouvelles recommandations relatives à l'authentification multifacteur de l'Anssi diffusées en octobre 2021 [14].
- Conservez vos informations personnelles et bancaires ainsi que vos documents d'identité en lieu sûr, à la fois en format physique et électronique (coffres-forts électroniques).
- Détruisez tous les documents qui contiennent des informations personnelles avant de les jeter (en papier comme en format électronique).
- Activez la double authentification lorsque le site ou le service le permet.
- Mettez régulièrement à jour vos appareils et leurs logiciels ou applications.

Principe 5 : Agissez vite en cas d'usurpation d'identité

Le site cybermalveillance.gouv.fr diffuse une fiche pratique [15] préconisant les actions à mener lorsqu'on est victime d'une usurpation d'identité.

Recommandation de l'Observatoire

Au-delà des conseils de prudence destinés à limiter les risques d'usurpation d'identité, l'Observatoire invite les citoyens à 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.

3.4 Évolutions futures de l'identité numérique

3.4.1 À moyen terme, vers une identité numérique européenne

Le règlement eIDAS a fait l'objet en 2020 d'une étude d'impact et d'une consultation publique conduites par la Commission européenne. Ces travaux ont mis en lumière les limites du cadre réglementaire actuel, alors que la forte augmentation des usages à distance, induite par la crise sanitaire, a renforcé le besoin de recourir à des identités numériques mieux sécurisées.

Le 3 juin 2021, la Commission européenne a présenté une proposition de révision du règlement eIDAS pour répondre à ces nouveaux besoins. Elle propose notamment de construire une identité numérique européenne accessible aux citoyens, résidents et entreprises de l'Union européenne. Cette identité numérique devrait offrir la possibilité de s'identifier et d'attester certains attributs (par exemple, diplômes), tout en permettant à ses utilisateurs de choisir les données et les attributs qu'ils souhaitent partager avec des tiers, et de conserver l'historique de ces interactions. Cette identité numérique prendra la forme d'un portefeuille d'identité numérique (*Digital Identity Wallet* – DIW) et pourrait jouer un rôle dans la chaîne du paiement comme moyen d'authentification reconnu par les établissements financiers.

Dans les faits, cette identité numérique européenne devra s'appuyer au maximum sur les infrastructures existantes, c'est-à-dire les schémas d'identification électronique déjà notifiés à la Commission européenne. Elle sera fournie par chaque État membre, qui aura la possibilité de s'appuyer sur des acteurs privés pour sa conception. Pour en faire une réalité le plus rapidement possible, la proposition de règlement est accompagnée d'une recommandation : la Commission européenne invite ainsi les États membres à établir une boîte à outils commune d'ici septembre 2022 et à commencer immédiatement les travaux préparatoires. Cette boîte à outils commune devrait notamment contenir l'architecture technique, les normes et standards utilisés, les lignes directrices et les bonnes pratiques. **Compte tenu des effets de bord que pourrait avoir l'identité numérique européenne dans la sécurité des paiements, l'Observatoire appelle les acteurs français des paiements à participer activement à ces travaux de préparation et de conception, de façon à maîtriser durablement la sécurité des moyens de paiement.**

14 Les recommandations de l'Anssi sont accessibles sur le lien suivant : *https://www.ssi.gouv.fr/*

15 *https://www.cybermalveillance.gouv.fr/*

3.4.2 Potentiellement à plus long terme, vers une identité numérique décentralisée

Les systèmes actuels de gestion numérique des identités reposent sur une centralisation auprès de tiers de confiance. Cette centralisation des données implique une confiance indispensable envers ces acteurs, et tout particulièrement au regard de leurs méthodes de gestion des identités numériques. Cette notion de confiance numérique – et celle adjacente de souveraineté – pourrait à terme être revisitée grâce à l'émergence d'une nouvelle méthode de gestion décentralisée de l'identité numérique : « l'identité décentralisée ». Celle-ci introduit un nouveau schéma d'identité numérique, fondée sur les principes de souveraineté, portabilité, sécurité et centrée sur l'utilisateur final.

Évoquée pour la première fois en 2015 [16], l'identité numérique décentralisée proposerait à l'utilisateur de réifier tout ou partie de ses attributs d'identité (attestation bancaire, de diplôme, d'assurance, de cursus professionnel, etc.) sur une même application numérique nommée « portefeuille numérique » [17]. Concrètement, un individu pourrait recevoir des attestations numériques vérifiables, puis les partager à des tiers vérificateurs de façon physique (QR code en version papier), numérique (courriel, SMS) et avec ou sans accès à Internet (Bluetooth par exemple) [18]. De cette façon, l'utilisateur serait en mesure de prouver efficacement certaines informations racines ou étendues qui sont rattachées à son identité.

Ces « attestations vérifiables » (*verifiable credentials* – VCs [19]) représenteraient des certificats numériques standardisés qui faciliteraient le partage d'informations en ligne de manière instantanée, souveraine, fiable et pérenne. Celles-ci seraient sauvegardées localement dans le téléphone de l'utilisateur ou dans un *cloud* de confiance (c'est-à-dire sur des serveurs externes [20]). En associant des attestations vérifiables provenant d'autorités reconnues [21] à des utilisateurs qui les réceptionneraient puis les administreraient avec autonomie, ces derniers disposeraient des « homologues numériques » [22] de leurs attestations physiques traditionnelles. Une carte nationale d'identité posséderait ainsi un « jumeau numérique » tout aussi recevable que sa version physique et officielle.

Appliquée au secteur des paiements, l'identité décentralisée pourrait bénéficier à tous les acteurs de sa chaîne de valeur. Grâce à la certification de ses attestations vérifiables, un utilisateur pourrait s'identifier ou s'authentifier auprès d'une multitude de fournisseurs de services, comme le requiert une banque pour l'ouverture d'un compte bancaire ou encore un commerce en ligne pour l'achat d'un bien ou d'un service. Néanmoins, ces deux exemples ne nécessitent pas un niveau d'identification strictement similaire : l'ouverture d'un compte en banque nécessite un niveau important de sécurité pour répondre aux exigences réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme alors qu'un achat en ligne appelle de simples preuves de solvabilité et de légitimité de l'achat. Dans un cas comme dans l'autre, l'identité décentralisée permettrait au client de partager en toute confiance par voie numérique les seules informations requises par l'usage.

Les perspectives de développement de l'identité numérique décentralisée ont été explorées dans un livre blanc du ministère de l'Intérieur d'octobre 2020 intitulé *Blockchain et identité numérique*, et d'un projet initié par le partenariat européen pour la *blockchain* (*European Blockchain Parternship* – EBP) : l'*European Blockchain Service Infrastructure* (EBSI). Un premier pas vers ce modèle d'identité numérique décentralisée pourrait être franchi dans le cadre de la révision du règlement eIDAS, qui semble s'orienter vers la reconnaissance des registres électroniques comme un nouveau service de confiance. **L'Observatoire poursuivra ses travaux de veille sur les perspectives d'une identité numérique décentralisée, si celles-ci venaient à se concrétiser, pour y étudier les risques et les opportunités pour la sécurité des moyens de paiement.**

16 Guy Zyskind, Oz Nathan, *et al.*, *Decentralizing privacy : Using blockchain to protect personal data. In Security and Privacy Workshops (SPW)*, consulté en ligne le 10 août 2021, pages 180 à 184, Institut des ingénieurs électriciens et électroniciens, 2015.

17 Cette application numérique est accessible pour l'utilisateur non exclusivement sur un *smartphone* comme sur un ordinateur.

18 Cette liste est non exhaustive, mais représente différents moyens envisagés pour qu'un utilisateur puisse partager le plus largement possible ses attestations vérifiables.

19 Pour plus d'informations concernant ces standards, cf. l'article rédigé par Thibault Langlois-Berthelot, « Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique », L'Observatoire en ligne d'IN Groupe, rédigé le 13 avril 2021.

20 La gestion de ces serveurs peut être au choix centralisée, distribuée ou décentralisée selon les besoins techniques ainsi que le contexte d'usage.

21 Par exemple : gouvernements ou sociétés sources de confiance et de crédibilité dans l'écosystème numérique.

22 Par analogie, une attestation vérifiable est au numérique ce qu'une carte de visite palpable est au monde physique. Toutefois, si l'intégrité des informations d'une attestation vérifiable peut être simplement vérifiée grâce à des mécanismes cryptographiques, leur véracité ne peut l'être : un tiers vérificateur est obligé de faire confiance à l'émetteur d'une assertion pour la considérer comme valide, c'est pourquoi la mise en place de cadres de confiance communs est primordiale pour que les acteurs de ce marché implémentent une identité décentralisée transparente et de confiance.

ENCADRÉS

❹ Exemples de solutions privées d'identité numérique en France

Mobile Connect et Moi

Lancée en 2017, Mobile Connect et Moi est le fruit d'un partenariat entre le fournisseur de solutions d'identité Ariadnext, porteur de la solution, et l'opérateur téléphonique Orange, agissant comme prestataire. L'application, que seul un abonné mobile Orange peut télécharger sur un *smartphone*, permet la création d'une identité faible en trois étapes : 1) le choix d'un code confidentiel à quatre chiffres pour l'authentification, 2) la copie d'une pièce d'identité, et 3) la prise d'une photographie du demandeur. Pour sécuriser l'accès à chaque usage, Mobile Connect et Moi s'appuie sur Mobile Connect, une solution d'authentification à deux facteurs basée sur des standards GSMA *(Global System for Mobile Communications)*. Elle allie la vérification par le réseau mobile du numéro de téléphone à la connaissance d'un code confidentiel. Mobile Connect et Moi est référencée sur le portail FranceConnect qui donne accès à plus de 1 100 sites de services publics ou privés. La solution compte 165 000 utilisateurs à l'heure actuelle. La création d'une identité est gratuite pour le demandeur.

L'Identité Numérique La Poste

La Poste a lancé L'Identité Numérique La Poste en février 2020, première identité électronique attestée conforme au niveau de garantie substantiel par l'Agence nationale de la sécurité des systèmes d'information (Anssi). Cette solution vise à proposer dans l'espace numérique un usage aussi simple que celui de montrer sa pièce d'identité physique dans la vie courante, en dehors des usages régaliens (contrôles d'identité, passage aux frontières, etc.). Cette solution s'adresse à toutes les personnes majeures, détenant un titre d'identité émis par le ministère de l'Intérieur français. Elle compte 500 000 personnes enrôlées aujourd'hui, avec un objectif de 2 millions en 2022, comptant sur les usages postaux « phygitaux » comme les retraits de colis ou les réexpéditions qui nécessitent de savoir que la personne est bien celle qu'elle prétend être.

Après une vérification d'identité, entièrement faite à distance ou en physique auprès d'un facteur à domicile ou en bureau de poste, l'application est activée sur le *smartphone*. Cette vérification d'identité est valable cinq ans. Elle est référencée sur le portail FranceConnect qui donne accès à plus de 1 100 sites de services publics ou privés, sur FranceConnect+ ou directement auprès des fournisseurs qui ont choisi de référencer L'Identité Numérique La Poste. Elle peut sécuriser les entrées en relation bancaire en ligne conformément aux exigences réglementaires de vérification d'identité, les opérations sensibles (ajouts de bénéficiaires, authentification de transactions, etc.) ou encore être associée à un dispositif de signature électronique. Le modèle économique de L'Identité Numérique La Poste repose sur une monétisation auprès des fournisseurs de services. Le service est par conséquent gratuit pour les utilisateurs finaux, aussi bien pour l'enrôlement que dans son utilisation.

La procédure d'enrôlement au sein de L'Identité Numérique La Poste

Source : Groupe La Poste.

ANNEXES

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

Face à l'ingéniosité des fraudeurs qui cherchent des moyens de contournement au fur et à mesure du durcissement des dispositifs de sécurité, les utilisateurs des instruments de paiement scripturaux (carte, chèque, virement et prélèvement) doivent renforcer leur vigilance et s'informer régulièrement sur les dispositifs de protection en vigueur et les comportements à adopter en matière de sécurité.

On recense à ce jour plusieurs typologies de fraude visant les moyens de paiement scripturaux :

- **la fraude par établissement de faux ordres de paiement**, soit après le vol ou la contrefaçon d'un instrument physique, soit par détournement de données ou d'identifiants bancaires par un tiers ;
- **la fraude par détournement ou falsification d'un ordre de paiement régulier**, en manipulant le payeur qui croit de bonne foi faire un paiement à un bénéficiaire légitime ou en modifiant ses attributs (montant, nom du bénéficiaire ou du donneur d'ordre, etc.) ;
- **la fraude par utilisation ou répudiation abusive** par le titulaire légitime d'un moyen de paiement, caractérisée par la contestation infondée d'un ordre de paiement valablement émis, aboutissant ainsi à l'annulation de l'encaissement des fonds.

Les types de fraudes ne s'appliquent pas de la même façon aux différents instruments de paiement et varient selon les canaux d'initiation de paiement utilisés (paiement de proximité, paiement à distance sur Internet, banque en ligne, etc.).

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

SOYEZ RESPONSABLES

- Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, pas même à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.
- Soyez particulièrement attentif à la récupération de vos moyens de paiement matériels par courrier en vérifiant que les courriers n'ont pas été altérés ou ouverts. Dans le cas du chéquier, il faut dans la mesure du possible privilégier le retrait sécurisé du chéquier en agence.
- Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile, etc.), gardez-le secret, ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui.

En particulier, ne communiquez vos mots de passe, codes confidentiels et identifiants personnels ni à des autorités administratives ou judiciaires, ni à votre banque, surtout par téléphone ou par courriel. Ils ne sont jamais susceptibles de vous demander cette information.

- Lorsque vous composez un code ou un mot de passe confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal, du distributeur ou du téléphone avec votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.
- Pensez à consulter régulièrement les consignes de sécurité publiées sur le site de votre banque et assurez-vous qu'elle dispose de vos coordonnées afin de vous contacter rapidement en cas d'opérations douteuses sur votre compte. En cas de contact de votre banque, par téléphone ou par courriel pour de telles opérations, rappelez-vous que vous n'avez pas à lui communiquer vos mots de passe et identifiants personnels.
- N'acceptez jamais de payer un vendeur ou loueur de biens que vous ne connaissez pas par transfert d'argent préalable à la mise à disposition ou la livraison du bien. Il peut s'agir de fraudeurs qui, après avoir récupéré les fonds transférés, font disparaître tout lien de communication (adresse e-mail, compte de réseau social, etc.).

SOYEZ ATTENTIFS

Lors de votre enrôlement pour bénéficier de l'authentification forte (conformément à la DSP 2)

Pour les actions relatives à la mise en place du nouveau dispositif d'authentification forte, le porteur doit suivre strictement les consignes reçues de sa banque au travers des canaux de communication habituels.

En cas de doute sur l'origine des consignes reçues, il est préférable de se référer aux informations accessibles via son espace client ou de contacter directement son conseiller bancaire.

Lors de la connexion à votre espace client de banque en ligne

- Choisissez un fournisseur d'accès Internet reconnu et suivez ses conseils de sécurité.
- Vérifiez la présence de https (« s » pour *secure*) devant l'adresse du site et l'icône d'une clé ou d'un cadenas dans la barre d'état du navigateur Internet.

- Contrôlez qu'aucune autre fenêtre Internet n'est ouverte, saisissez vous-même l'adresse exacte fournie par votre banque.
- N'accédez pas à votre banque en ligne depuis un ordinateur public ou connecté à un réseau Wi-Fi public.
- N'accédez jamais à votre banque en ligne depuis un courrier électronique ou un SMS.
- Si vous pensez avoir fourni vos codes d'accès de banque en ligne à un tiers via un site Internet, un lien SMS ou directement par téléphone, contactez immédiatement votre banque, aux coordonnées habituelles, pour lui signaler (n'utilisez pas celles des messages que vous venez de recevoir).

Lors des paiements à un professionnel ou à un particulier

- Vérifiez l'utilisation qui est faite de votre carte bancaire par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider une transaction.
- Lorsqu'un chèque est automatiquement rempli par le commerçant, soyez attentif aux mentions indiquées avant de le signer et vérifiez plus particulièrement le montant.
- Quelques précautions lors du remplissage d'un chèque permettent de réduire les risques de fraude : remplissez vos chèques à l'encre noire non effaçable, évitez les ratures ou surcharges, inscrivez le nom du bénéficiaire du chèque et les montants en chiffres et en lettres sans laisser d'espace libre, puis tirez un trait sur l'espace restant non utilisé. Le lieu de paiement et la date doivent être renseignés en même temps que les autres mentions. La signature du chèque ne doit pas déborder sur la ligne de chiffres en bas du chèque. En aucun cas, la signature ne doit être apposée seule sur un chèque, c'est-à-dire sans les mentions relatives au montant et au bénéficiaire préalablement renseignées.

Lors des retraits aux distributeurs de billets

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

Lors des paiements sur Internet

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

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

- Lors de la réception d'un mandat de prélèvement, vérifiez que les informations relatives au créancier (nom/raison sociale et adresse) sont en cohérence avec vos engagements contractuels. Si votre banque a mis en place une liste des créanciers autorisés à effectuer des prélèvements sur votre compte (appelée aussi « liste blanche »), pensez à la mettre à jour.
- Si vous êtes bénéficiaire d'un paiement à distance et que vous ne connaissez pas personnellement le payeur (par exemple, en situation de vente sur Internet), vérifiez la cohérence des informations fournies (nom, adresse, identifiant du payeur, etc.) avant de donner votre accord à la transaction. En cas de doute, vérifiez auprès de la banque du payeur la régularité du moyen de paiement proposé et la qualité du payeur.
- Si vous êtes bénéficiaire d'un chèque de banque (par exemple, en cas de vente d'un véhicule), contactez la banque émettrice en recherchant par vous-même ses coordonnées (sans vous fier aux mentions présentes sur le chèque) pour en confirmer la validité avant de finaliser la transaction.
- Vérifiez la présence effective des mentions obligatoires d'un chèque, notamment la signature de l'émetteur du chèque, le nom de la banque qui doit payer, une indication de la date et du lieu où le chèque est

établi, ainsi que la cohérence des informations (bénéficiaire, montant, zone numéro de chèque de la ligne magnétique) et l'absence de ratures ou surcharges pouvant indiquer une origine frauduleuse.
- N'acceptez jamais d'encaisser un chèque qui ne vous est pas destiné ou qui ne correspond pas à ce qui a été convenu. Refusez de reverser des fonds à quiconque contre la remise d'un chèque.
- Professionnels et commerçants, renseignez-vous sur le service Vérifiance-FNCI-Banque de France [1] ou sur les solutions de sécurisations proposées par votre établissement bancaire ou d'autres acteurs spécialisés pour sécuriser vos encaissements par chèque.

Lors de vos déplacements à l'étranger

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

SACHEZ RÉAGIR

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

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

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

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

N'hésitez pas à contacter votre banque afin d'évaluer la régularité des opérations de paiement non identifiées ou pour lesquelles vous avez un doute. Contactez plus particulièrement votre banque lorsque vous recevez des notifications par téléphone, courriel ou sur vos applications mobiles confirmant ou demandant la validation d'opérations de paiement en cours, que vous n'auriez pas initiées.

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

N'hésitez pas également à faire opposition afin de vous prémunir contre toute nouvelle tentative de fraude qui utiliserait les données usurpées de votre instrument de paiement.

Si, dans un délai de treize mois à compter de la date de débit de l'opération contestée (délai fixé par la loi), vous déposez une réclamation auprès de votre prestataire de services de paiement (PSP) gestionnaire de compte, les sommes contestées doivent vous être remboursées immédiatement et au plus tard dans le délai d'un jour ouvré sans frais. Dans ces conditions, votre responsabilité ne peut être engagée. Néanmoins ceci ne vaut pas en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un tiers le numéro et/ou le code confidentiel de votre moyen de paiement et celui-ci en a fait usage sans vous prévenir).

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

1 FNCI – Fichier national des chèques irréguliers.

A2 PROTECTION DU PAYEUR EN CAS DE PAIEMENT NON AUTORISÉ

L'ordonnance de transposition de la deuxième directive concernant les services de paiement au sein du marché intérieur (DSP 2), entrée en vigueur le 13 janvier 2018, a modifié le cadre législatif concernant la responsabilité du payeur en cas d'opération de paiement non autorisée (cf. notamment les articles L. 133-18 et L. 133-19 du Code monétaire et financier). Les grands principes issus de la première directive concernant les services de paiement restent toutefois inchangés. **Ces dispositions ne sont pas applicables aux instruments de paiement, exclus du champ d'application de la DSP 2, à savoir principalement le chèque, la lettre de change et le billet à ordre.**

La charge de la preuve incombe au prestataire de services de paiement (PSP). Ainsi, lorsqu'un payeur nie avoir autorisé une opération de paiement, il incombe à son PSP de prouver que l'opération de paiement en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre. La loi encadre désormais strictement les conventions de preuve puisqu'elle prévoit que l'utilisation de l'instrument de paiement, telle qu'enregistrée par le PSP, ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait, par négligence grave, aux obligations lui incombant en la matière.

La transposition de la deuxième directive concernant les services de paiement (DSP 2) prévoit que si l'opération de paiement contestée a impliqué un prestataire de service d'initiation de paiement, le payeur doit contester l'opération de paiement auprès de son PSP gestionnaire de comptes, qui aura la charge de le rembourser. Ce dernier se retourne ensuite vers le prestataire de service d'initiation de paiement qui doit prouver que l'opération de paiement en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

Il convient toutefois de distinguer si l'opération de paiement contestée est effectuée ou non sur le territoire de la République française ou au sein de l'Espace économique européen [1] (EEE) afin de déterminer l'étendue de la responsabilité du payeur.

OPÉRATIONS NATIONALES OU INTRACOMMUNAUTAIRES

Ces dispositions de protection du payeur couvrent :

- les opérations de paiement effectuées en euros ou en francs CFP [2] sur le territoire de la République française [3] ;
- les opérations intracommunautaires dans lesquelles le PSP du bénéficiaire et celui du payeur sont situés :
  - l'un sur le territoire de la France métropolitaine, dans les départements d'outre-mer ou à Saint-Martin,
  - l'autre dans un autre État partie à l'accord sur l'EEE, et réalisées en euros ou dans la devise nationale de l'un de ces États.

Concernant les opérations de paiement non autorisées, c'est-à-dire en pratique dans les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, l'utilisateur de services de paiement doit contester, auprès de son PSP et dans un délai de treize mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son PSP doit alors rembourser l'opération de paiement non autorisée au payeur immédiatement ou au plus tard dans le délai d'un jour ouvrable et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. La transposition de la DSP 2 prévoit que le PSP du payeur peut retarder le remboursement lorsqu'il a de bonnes raisons de soupçonner une fraude du payeur. Dans ce cas, une notification doit être adressée à la Banque de France pour justifier de son refus de remboursement immédiat. Une indemnisation complémentaire peut aussi éventuellement être versée. Nonobstant le délai maximal de contestation de treize mois, le payeur doit, lorsqu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer sans tarder son PSP.

AVANT INFORMATION AUX FINS DE BLOCAGE DE L'INSTRUMENT DE PAIEMENT

Avant l'information aux fins de blocage de l'instrument de paiement, le payeur peut supporter, à concurrence de cinquante euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de l'instrument de paiement. Toutefois, si l'opération de paiement est effectuée sans utilisation des données de sécurité personnalisées (par exemple un paiement par carte sans contact), ou que le payeur ne

1 L'Espace économique européen est constitué de l'Union européenne, du Liechtenstein, de la Norvège et de l'Islande.

2 Franc CFP (Change Franc Pacifique) ou franc Pacifique.

3 L'ordonnance du 9 août 2017 transposant la DSP 2 prévoit qu'une large part de ses dispositions s'applique à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna.

pouvait pas détecter la perte ou le vol de son instrument de paiement, ou que la perte résulte d'une action d'une personne placée sous la responsabilité du PSP, alors le payeur ne voit pas sa responsabilité engagée et il ne supporte aucune perte financière (même en-deçà de cinquante euros).

La responsabilité du payeur n'est pas non plus engagée si l'opération de paiement non autorisée a été effectuée en détournant à son insu l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas plus engagée en cas de contrefaçon de l'instrument de paiement si ce dernier était en possession de son titulaire au moment où l'opération non autorisée a été réalisée. Enfin, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que son PSP n'exige une authentification forte, étant noté que le seul SMS ne suffit plus à constituer une authentification forte pour les paiements par carte en ligne depuis le 14 septembre 2019.

En revanche, le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations de sécurité, d'utilisation ou de blocage de l'instrument de paiement, telles que convenues avec son PSP.

Enfin, si le PSP ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement, le payeur ne supporte aucune conséquence financière, sauf à avoir agi de manière frauduleuse.

APRÈS INFORMATION AUX FINS DE BLOCAGE DE L'INSTRUMENT DE PAIEMENT

Après avoir informé son PSP, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de l'instrument de paiement ou de l'utilisation détournée des données qui lui sont liées.

Là encore, les agissements frauduleux du payeur le privent de toute protection et il demeure responsable des pertes liées à l'utilisation de l'instrument de paiement.

L'information aux fins de blocage peut être effectuée auprès du PSP ou auprès d'une entité que ce dernier aura indiquée à son client, suivant les cas, dans le contrat de services de paiement ou dans la convention de compte de dépôt.

Lorsque l'utilisateur a informé son PSP de la perte, du vol, du détournement ou de la contrefaçon de l'instrument de paiement, ce dernier lui fournit sur demande et pendant dix-huit mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

OPÉRATIONS EXTRAEUROPÉENNES

La DSP 2 élargit partiellement son application aux opérations de paiement qui impliquent un PSP établi dans l'EEE et un autre établi en dehors de l'EEE. Pour ce type d'opération de paiement, souvent appelé « *one leg* », les dispositions protectrices de la directive s'appliquent assez largement à la partie de l'opération de paiement qui s'effectue dans l'EEE. Par exemple, un payeur qui dispose d'un instrument de paiement émis par un PSP établi en France peut bénéficier d'un régime protecteur même si cet instrument de paiement est utilisé aux États-Unis. Ainsi, en cas d'opération de paiement non autorisée effectuée au profit d'un bénéficiaire dont le PSP est établi aux États-Unis (ou ailleurs hors de l'EEE), le payeur peut demander à son PSP établi en France d'être remboursé dans les mêmes conditions que celles applicables aux opérations de paiement nationales ou intracommunautaires.

Des dispositions spécifiques sont prévues pour les opérations de paiement par carte lorsque :

- l'émetteur est situé à Saint-Pierre-et-Miquelon ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le PSP est situé dans un État non européen [4], quelle que soit la devise dans laquelle l'opération de paiement est réalisée ;
- l'émetteur est situé en Nouvelle-Calédonie, en Polynésie française ou à Wallis-et-Futuna, au profit d'un bénéficiaire dont le PSP est situé dans un État autre que la République française, quelle que soit la devise utilisée.

Dans ces cas, le plafond de cinquante euros s'applique pour les opérations de paiement non autorisées effectuées en cas de perte ou de vol de la carte, même si l'opération de paiement a été réalisée sans utilisation des données de sécurité personnalisées.

Par ailleurs, le délai maximal de contestation de l'opération de paiement est ramené à soixante-dix jours et peut être conventionnellement étendu à cent vingt jours. Le remboursement d'une opération de paiement non autorisée doit toujours être effectué dans un délai d'un jour ouvré.

4 Un État non européen est un État qui n'est pas partie à l'accord sur l'Espace économique européen.

A3 MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

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

PÉRIMÈTRE CONCERNÉ

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

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

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

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

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

- **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.

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 4.

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.

A4 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 28 avril 2022.

PRÉSIDENT

François VILLEROY DE GALHAU
Gouverneur de la Banque de France

REPRÉSENTANTS DES ASSEMBLÉES

Éric BOCQUET
Sénateur

Rémi REBEYROTTE
Député

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

- Le Secrétaire général ou son représentant :
  Dominique LABOUREIX
  Olivier FLICHE

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 :
  Grégoire LUNDI

Sur proposition du ministre de l'Économie, de l'Industrie et du Numérique :
- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Christian DUFOUR
- Le directeur général du Trésor ou son représentant :
  Pierre-Olivier CHOTARD
  Clara PAOLONI
- La Présidente de l'Institut d'émission des départements d'outre-mer (IEDOM) et directrice générale de l'Institut d'émission d'outre-mer (IEOM) :
  Marie-Anne POUSSIN-DELMAS
- Le directeur général de la Concurrence, de la Consommation et de la Répression des fraudes ou son représentant :
  Aurélien HAUSER

Sur proposition du garde des Sceaux, ministre de la Justice :
- Le directeur des Affaires criminelles et des Grâces ou son représentant :
  Louise NEYTON
  Marion LE LORRAIN

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 (Afepame)

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)

Carole DELORME D'ARMAILLE
Directrice générale
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)

Philippe MARQUETTY
Directeur – Produits, Paiements et *Cash management*
Société Générale

Évelyne BOTTOLLIER-CURTET
Card scheme relationships manager
Groupe BPCE

Romain BOISSON
Directeur régional
Visa Europe France

Jérôme RAGUÉNÈS
Directeur du département Numérique, Paiements 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)

Mathieu ROBIN
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

Jean-Michel CHANAVAS
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

Claude FRANCE
Directeur général des opérations France
Worldline

David NACCACHE
Professeur
École normale supérieure (ENS)

A5 MÉTHODOLOGIE DE MESURE DE LA FRAUDE AUX MOYENS DE PAIEMENT SCRIPTURAUX

CADRE GÉNÉRAL

Définition de la fraude aux moyens de paiement

La définition de la fraude aux moyens de paiement scripturaux, retenue par l'Observatoire, est 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.

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.

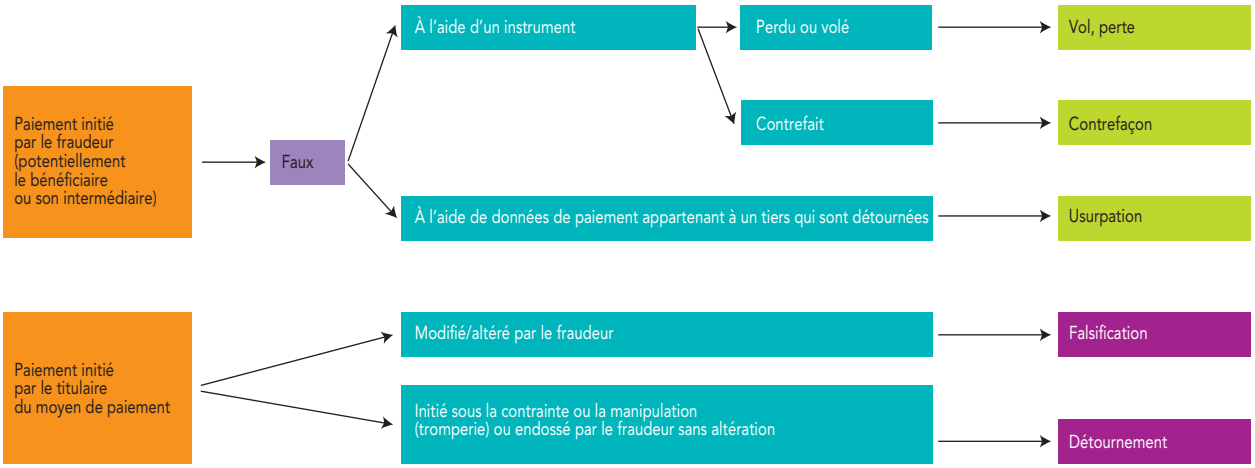
Sont également exclus de la fraude :

- 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 2015 [2] que l'impact des mesures de cette nature réduisait de 5 % l'estimation brute de la fraude pour les paiements par carte.

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.

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) : fraude par l'établissement 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 par l'intermédiaire du détournement de données ou d'identifiants bancaires ;
- **falsification** : altération d'un ordre de paiement régulièrement émis par le titulaire légitime du moyen de paiement, en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.) ;
- **détournement** : transaction initiée par le payeur sous la contrainte ou la manipulation (tromperie), sans altération ou modification d'attribut par le fraudeur.

Ventilation géographique de la fraude aux moyens de paiement

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

MESURE DE LA FRAUDE À LA CARTE DE PAIEMENT

Transactions couvertes

La fraude à la carte de paiement, telle que mesurée dans le présent rapport, porte sur les transactions de paiement (de proximité et à distance) et de retrait effectuées par carte de paiement et réalisées en France et à l'étranger dès lors que l'une des contreparties de la transaction est considérée comme française : carte émise par un établissement français ou accepteur de la transaction (commerçant ou distributeur automatique de billet/guichet automatique bancaire) situé en France. Aucune distinction n'est faite quant à la nature du réseau d'acceptation (interbancaire [3] ou privatif [4]) 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.

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).

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

Modalité du paiement sur Internet	Description
Paiement 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 – *one time password* – seul) sont également comprises dans cette catégorie.
Paiement non authentifié	Tout paiement réalisé en dehors de l'infrastructure 3D-Secure, recouvrant : • paiement non assujetti aux règles européennes sur l'authentification forte (DSP 2) [a], comme le paiement initié par le créancier sur la base d'un accord préexistant entre le payeur et le créancier pour l'effectuer (par exemple : *Merchant Initiated Transaction* – MIT) et le paiement dit « *One leg* » (l'émetteur ou l'acquéreur du paiement est situé hors de l'Union européenne) ; • paiement assujetti aux règles européennes sur l'authentification forte, mais dont le motif d'exemption à l'authentification forte est formalisé dans le flux d'autorisation ; • paiement assujetti aux règles européennes sur l'authentification forte, mais non conforme.

a) Les règles européennes sur l'authentification forte sont notamment précisées dans un acte délégué de la DSP 2 : le règlement (UE) n°2018/389 détaillant pour les transactions assujetties au principe de l'authentification forte les différents motifs d'exemption et les conditions pour les mettre en œuvre.

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

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

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

MESURE DE LA FRAUDE AU VIREMENT

Instruments de paiement couverts

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

Origine des données de fraude

Les données de fraude au virement sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement [5] 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 (*phishing*, *malware*, etc.) ou sous la contrainte.
Falsification	Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime.
Détournement	Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.), le titulaire légitime du compte à émettre régulièrement un virement à destination d'un numéro de compte qui n'est pas celui du bénéficiaire légitime du paiement ou qui ne correspond à aucune réalité économique. Par exemple, sont considérés comme répondant à cette définition les cas de « fraude au Président » ou de fraude au changement de coordonnées bancaires.

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

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

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

MESURE DE LA FRAUDE AU PRÉLÈVEMENT

Instruments de paiement couverts

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

Origine des données de fraude

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

Éléments d'analyse de la fraude

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

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

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

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

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

MESURE DE LA FRAUDE AU CHÈQUE

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

Périmètre de la fraude

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

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

Origines des données de fraude

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

Éléments d'analyse des données de fraude

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

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

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

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

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

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

A6 DOSSIER STATISTIQUE SUR L'USAGE ET LA FRAUDE AUX MOYENS DE PAIEMENT

Des tableaux complémentaires, ainsi que l'ensemble des tableaux contenus dans cette annexe, sont disponibles pour téléchargement à l'adresse suivante :
https://www.banque-france.fr/liste-chronologique/rapports-dactivite?year=2022

PANORAMA DES MOYENS DE PAIEMENT

T1 Cartographie des moyens de paiement scripturaux en 2021

(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
	2021	Variation 2021/2020	Part	2021	Variation 2021/2020	Part	
Paiement carte [a]	16 129	16,4	56,9	660	14,2	1,6	41
dont sans contact	*7 369*	*42,8*	*26,0*	*125*	*57,0*	*0,3*	*17*
dont paiement par mobile	*357*	*176,8*	*1,3*	*8*	*177,8*	*0,0*	*21*
Chèque	1 106	-5,9	3,9	589	-4,2	1,4	532
Virement	4 843	8,0	17,1	38 723	18,4	91,8	7 995
dont VGM [b]	*9*	*4,4*	*0,0*	*19 662*	*3,3*	*46,6*	*2 178 431*
dont virement instantané (SCT Inst)	*107*	*137,7*	*0,4*	*50*	*90,7*	*0,1*	*467*
Prélèvement	5 020	8,6	17,7	1 895	12,5	4,5	378
Effet de commerce	75	5,2	0,3	212	7,4	0,5	2 813
Monnaie électronique	64	78,8	0,2	1	49,0	0,0	16
Transmission de fonds	29	89,9	0,1	1	- 30,4	0,0	42
Total	**27 266**	**12,4**	**96,2**	**42 081**	**17,6**	**99,7**	**1 543**
Retrait par carte [a]	1 086	2,1	3,8	124	6,8	0,3	114
Total transactions	**28 352**	**12,0**	**100,0**	**42 204**	**17,5**	**100,0**	**1 489**

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
Carte	11 134	12 581	13 179	14 485	13 852	16 129
dont sans contact	*635*	*1 300*	*2 374*	*3 779*	*5 159*	*7 369*
dont par mobile	*0*	*5*	*11*	*48*	*129*	*357*
Chèque	2 137	1 927	1 747	1 587	1 175	1 106
Virement	3 753	3 870	4 038	4 269	4 483	4 843
dont virement instantané (SCT inst)	*nd*	*nd*	*0*	*14*	*45*	*107*
Prélèvement	3 963	4 091	4 211	4 370	4 622	5 020
Effet de commerce	82	81	81	78	71	75
Monnaie électronique	38	55	65	62	36	64
Transmission de fonds	20	18	16	16	15	29
Total paiements scripturaux	**21 107**	**22 605**	**23 320**	**24 851**	**24 238**	**27 266**
Retrait par carte	1 491	1 481	1 439	1 392	1 064	1 086

b) En valeur
(en milliards d'euros)

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

Note : nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

T3 Répartition de la fraude sur les moyens de paiement en 2021

(montant en euros, volume en unités, part en pourcentage, taux en pourcentage, montant moyen en euros)

	Volume			Montant			Taux de fraude	Montant moyen
	2021	Variation 2021/2020 c)	Part	2021	Variation 2021/2020 c)	Part	2021	
Paiement carte a)	6 764 752	- 8,8	90,5	421 410 285	- 4,1	33,9	0,064	62
dont sans contact	*604 278*	*12,5*	*8,1*	*16 274 668*	*44,1*	*1,3*	*0,013*	*27*
dont par mobile	*83 266*	*146,6*	*1,1*	*5 610 270*	*100,9*	*0,5*	*0,074*	*67*
Chèque (nouvelle approche) b)	280 521	47,6	3,8	464 942 784	15,8	37,4	0,079	1 657
Chèque (ancienne approche)	321 214	45,5	4,3	625 625 059	16,3	50,4	0,106	1 948
Virement	46 718	30,2	0,6	287 264 068	7,6	23,1	0,001	6 149
dont virement instantané (SCT inst)	*12 913*	*81,1*	*0,2*	*22 406 942*	*112,1*	*1,8*	*0,045*	*1 735*
Prélèvement	251 010	3 770,6	3,4	25 318 677	1 238,9	2,0	0,001	101
Effet de commerce	1	- 98,4	0,0	12 079	- 97,8	0,0	0,000	12 079
Monnaie électronique	2 001	nd	0,0	137 340	nd	0,0	0,013	69
Transmission de fonds	962	nd	0,0	246 362	nd	0,0	0,020	256
Total paiements	**7 345 965**	**- 4,1**	**98,3**	**1 199 331 595**	**8,0**	**96,5**	**0,003**	**163**
Retrait par carte a)	129 083	14,2	1,7	42 950 169	26,5	3,5	0,035	333
Total transactions	**7 475 048**	**- 3,8**	**100,0**	**1 242 281 764**	**8,5**	**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.
c) Les variations annuelles du total de la fraude sont calculées à méthodologie et périmètre constants, c'est-à-dire en appliquant la nouvelle approche de la fraude au chèque pour 2020 et 2021 et en neutralisant l'effet lié à la prise en compte, pour la première fois en 2021, de la fraude sur la monnaie électronique et la transmission de fonds.
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.

T4 Évolution historique de la fraude sur les moyens de paiement

a) En volume
(en unités)

	2016	2017	2018	2019	2020	2021
Carte	5 300 847	5 364 312	6 068 959	7 071 095	7 421 137	6 764 752
dont sans contact	*125 860*	*248 991*	*445 919*	*603 509*	*537 061*	*604 278*
dont par mobile	*nd*	*22*	*2 070*	*3 494*	*33 761*	*83 266*
Chèque (nouvelle approche)	nd	nd	nd	nd	190 001	280 521
Chèque (ancienne approche)	120 295	114 906	166 421	183 488	220 685	321 214
Virement	5 585	4 642	7 736	15 934	35 893	46 718
dont virement instantané (SCT inst)	*nd*	*nd*	*5*	*729*	*7 131*	*12 913*
Prélèvement	1 176	25 801	309 377	43 519	6 485	251 010
Effet de commerce	4	3	5	1	62	1
Monnaie électronique	nd	nd	nd	nd	nd	2 001
Transmission de fonds	nd	nd	nd	nd	nd	962
Total fraude paiements scripturaux	**5 427 907**	**5 509 664**	**6 552 498**	**7 314 037**	**7 684 262**	**7 345 965**
Retrait par carte	202 158	177 562	158 908	165 505	113 067	129 083
Total fraude transactions	**5 630 065**	**5 687 226**	**6 711 406**	**7 479 542**	**7 797 329**	**7 475 048**

b) En valeur
(en euros)

	2016	2017	2018	2019	2020	2021
Carte	378 455 912	344 962 084	401 604 986	428 249 931	439 489 315	421 410 285
dont sans contact	*1 410 566*	*2 748 790*	*5 234 852*	*8 479 354*	*11 292 261*	*16 274 668*
dont par mobile	*nd*	*1 227*	*73 682*	*216 236*	*2 792 574*	*5 610 270*
Chèque (nouvelle approche)	nd	nd	nd	nd	401 611 189	464 942 784
Chèque (ancienne approche)	276 716 554	296 072 847	450 108 464	539 215 175	538 059 139	625 625 059
Virement	86 284 101	78 286 492	97 327 128	161 642 174	266 969 099	287 264 068
dont virement instantané (SCT inst)	*nd*	*nd*	*29 800*	*2 203 240*	*10 562 419*	*22 406 942*
Prélèvement	39 935 882	8 726 403	58 346 253	10 990 025	1 891 051	25 318 677
Effet de commerce	1 018 149	153 100	226 217	74 686	538 918	12 079
Monnaie électronique	nd	nd	nd	nd	nd	137 340
Transmission de fonds	nd	nd	nd	nd	nd	246 362
Total fraude paiements scripturaux	**782 410 598**	**728 200 926**	**1 007 613 048**	**1 140 171 991**	**1 246 947 522**	**1 199 331 595**
Retrait par carte	48 650 966	42 038 924	37 630 659	41 651 788	33 950 879	42 950 169
Total fraude transactions	**831 061 564**	**770 239 850**	**1 045 243 707**	**1 181 823 779**	**1 280 898 401**	**1 242 281 764**

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, valeur en milliers d'euros)

	2017		2018		2019	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
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	
	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**11 193 795**	**424 105 649**	**12 935 438**	**475 079 750**
dont paiements sans contact (y compris paiements par mobile)	5 159 657	79 664 370	7 368 699	125 082 420
dont paiements par mobile	*129 105*	*2 734 667*	*357 355*	*7 596 769*
Paiements à distance (hors Internet)	**134 114**	**7 567 877**	**76 931**	**7 995 010**
Paiements sur Internet	**2 524 317**	**146 563 476**	**3 116 285**	**177 056 237**
dont paiements 3D-Secure avec authentification forte	nd	nd	787 664	85 221 641
dont paiements 3D-Secure sans authentification forte	nd	nd	444 723	19 267 910
dont paiements hors 3D-Secure	nd	nd	1 883 898	72 566 685
Retraits	**1 064 095**	**115 958 207**	**1 086 289**	**123 867 648**
Total	**14 916 322**	**694 195 208**	**17 214 942**	**783 998 644**

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
Paiements 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*
Paiements 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**
Paiements 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		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**972 228**	**47 994 762**	**0,011**	**942 376**	**52 426 587**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	537 061	11 292 261	0,014	604 278	16 274 668	0,013
dont paiements par mobile	*33 761*	*2 792 574*	*0,102*	*83 266*	*5 610 270*	*0,074*
Paiements à distance (hors Internet)	**411 344**	**26 899 103**	**0,355**	**124 596**	**22 193 382**	**0,278**
Paiements sur Internet	**6 037 565**	**364 595 450**	**0,249**	**5 697 780**	**346 790 316**	**0,196**
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	496 017	103 029 680	0,121
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	364 223	26 046 078	0,135
dont paiements hors 3D-Secure	nd	nd	nd	4 837 540	217 714 555	0,300
Retraits	**113 067**	**33 950 879**	**0,029**	**129 083**	**42 950 169**	**0,035**
Total	**7 534 204**	**473 440 194**	**0,068**	**6 893 835**	**464 360 454**	**0,059**

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 2021

(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	**750 738**	**79,7**	**38 087 381**	**72,6**	**9 601**	**1,0**	**1 541 192**	**2,9**	**86 793**	**9,2**	**5 979 840**	**11,4**
dont paiements sans contact (y compris paiements par mobile)	531 907	88,0	11 803 790	72,5	2 567	0,4	47 187	0,3	37 266	6,2	2 861 800	17,6
dont paiements par mobile	*41 639*	*50,0*	*2 762 922*	*49,2*	*71*	*0,1*	*2 866*	*0,1*	*21 833*	*26,2*	*1 717 350*	*30,6*
Paiements à distance (hors Internet)	**1 177**	**0,9**	**305 417**	**1,4**	**34**	**0,0**	**2 917**	**0,0**	**721**	**0,6**	**216 882**	**1,0**
Paiements sur Internet	**93 557**	**1,6**	**6 509 438**	**1,9**	**2 808**	**0,0**	**152 250**	**0,0**	**29 906**	**0,5**	**2 022 572**	**0,6**
dont paiements 3D-Secure avec authentification forte	6 835	1,4	1 633 512	1,6	163	0,0	35 063	0,0	366	0,1	28 091	0,0
dont paiements 3D-Secure sans authentification forte	2 246	0,6	192 609	0,7	466	0,1	46 363	0,2	919	0,3	25 140	0,1
dont paiements hors 3D-Secure	84 476	1,7	4 683 316	2,2	2 179	0,0	70 823	0,0	28 621	0,6	1 969 340	0,9
Retraits	**121 322**	**94,0**	**40 901 239**	**95,2**	**2 812**	**2,2**	**1 217 088**	**2,8**	**1 924**	**1,5**	**347 284**	**0,8**
Total	**966 794**	**14,0**	**85 803 475**	**18,5**	**15 255**	**0,2**	**2 913 447**	**0,6**	**119 344**	**1,7**	**8 566 578**	**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 2021 (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	**57 350**	**6,1**	**3 165 843**	**6,0**	**37 894**	**4,0**	**3 652 331**	**7,0**	**942 376**	**52 426 587**
dont paiements sans contact (y compris paiements par mobile)	8 096	1,3	338 006	2,1	24 442	4,0	1 223 885	7,5	604 278	16 274 668
dont paiements par mobile	*2 405*	*2,9*	*149 918*	*2,7*	*17 318*	*20,8*	*977 214*	*17,4*	*83 266*	*5 610 270*
Paiements à distance (hors Internet)	**122 343**	**98,2**	**21 601 929**	**97,3**	**321**	**0,3**	**66 237**	**0,3**	**124 596**	**22 193 382**
Paiements sur Internet	**5 561 093**	**97,6**	**336 718 736**	**97,1**	**10 416**	**0,2**	**1 387 320**	**0,4**	**5 697 780**	**346 790 316**
dont paiements 3D-Secure avec authentification forte	487 619	98,3	101 052 933	98,1	1 034	0,2	280 081	0,3	496 017	103 029 680
dont paiements 3D-Secure sans authentification forte	359 954	98,8	25 728 529	98,8	638	0,2	53 437	0,2	364 223	26 046 078
dont paiements hors 3D-Secure	4 713 520	97,4	209 937 274	96,4	8 744	0,2	1 053 802	0,5	4 837 540	217 714 555
Retraits	**567**	**0,4**	**45 117**	**0,1**	**2 458**	**1,9**	**439 441**	**1,0**	**129 083**	**42 950 169**
Total	**5 741 353**	**83,3**	**361 531 625**	**77,9**	**51 089**	**0,7**	**5 545 329**	**1,2**	**6 893 835**	**464 360 454**

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2021

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

	Transactions nationales				Transactions européennes			
	Volume		Valeur		Volume		Valeur	
	Nombre	Part	Montant	Part	Nombre	Part	Montant	Part
Paiements de proximité et sur automate	**825 325**	**87,6**	**43 515 617**	**83,0**	**57 435**	**6,1**	**4 396 509**	**8,4**
dont paiements sans contact (y compris paiements par mobile)	576 537	95,4	14 002 613	86,0	19 673	3,3	1 898 428	11,7
dont paiements par mobile	*75 039*	*90,1*	*4 801 997*	*85,6*	*4 866*	*5,8*	*619 983*	*11,1*
Paiements à distance (hors Internet)	**77 941**	**62,6**	**10 604 251**	**47,8**	**25 606**	**20,6**	**6 684 731**	**30,1**
Paiements sur Internet	**2 577 337**	**45,2**	**191 873 234**	**55,3**	**2 058 594**	**36,1**	**95 286 454**	**27,5**
dont paiements 3D-Secure avec authentification forte	267 556	53,9	69 544 332	67,5	161 632	32,6	25 438 244	24,7
dont paiements 3D-Secure sans authentification forte	159 344	43,7	11 208 886	43,0	138 659	38,1	10 588 763	40,7
dont paiements hors 3D-Secure	2 150 437	44,5	111 120 015	51,0	1 758 303	36,3	59 259 445	27,2
Retraits	**121 642**	**94,2**	**41 437 842**	**96,5**	**3 286**	**2,5**	**836 254**	**1,9**
Total	**3 602 245**	**52,3**	**287 430 944**	**61,9**	**2 144 921**	**31,1**	**107 203 948**	**23,1**

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2021 (suite)

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

	Transactions internationales				Total	
	Volume		Valeur		Volume	Valeur
	Nombre	Part	Montant	Part		
Paiements de proximité et sur automate	**59 616**	**6,3**	**4 514 461**	**8,6**	**942 376**	**52 426 587**
dont paiements sans contact (y compris paiements par mobile)	8 068	1,3	373 627	2,3	604 278	16 274 668
dont paiements par mobile	*3 361*	*4,0*	*188 290*	*3,4*	*83 266*	*5 610 270*
Paiements à distance (hors Internet)	**21 049**	**16,9**	**4 904 400**	**22,1**	**124 596**	**22 193 382**
Paiements sur Internet	**1 061 849**	**18,6**	**59 630 628**	**17,2**	**5 697 780**	**346 790 316**
dont paiements 3D-Secure avec authentification forte	66 829	13,5	8 047 104	7,8	496 017	103 029 680
dont paiements 3D-Secure sans authentification forte	66 220	18,2	4 248 429	16,3	364 223	26 046 078
dont paiements hors 3D-Secure	928 800	19,2	47 335 095	21,7	4 837 540	217 714 555
Retraits	**4 155**	**3,2**	**676 073**	**1,6**	**129 083**	**42 950 169**
Total	**1 146 669**	**16,6**	**69 725 562**	**15,0**	**6 893 835**	**464 360 454**

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	2017		2018		2019	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
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	
	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**10 978 602**	**413 760 411**	**12 611 966**	**460 274 895**
dont paiements sans contact (y compris paiements par mobile)	5 081 519	78 386 853	7 202 992	121 694 861
dont paiements par mobile	*126 945*	*2 687 300*	*348 251*	*7 390 633*
Paiements à distance (hors Internet)	**60 243**	**5 428 918**	**56 236**	**5 540 339**
Paiements sur Internet	**2 011 431**	**122 128 921**	**2 399 865**	**142 184 895**
dont paiements 3D-Secure avec authentification forte	nd	nd	661 960	72 184 112
dont paiements 3D-Secure sans authentification forte	nd	nd	389 530	15 797 723
dont paiements hors 3D-Secure	nd	nd	1 348 375	54 203 060
Retraits	**1 038 647**	**112 337 533**	**1 056 936**	**119 485 544**
Total	**14 088 924**	**653 655 783**	**16 125 003**	**727 485 673**

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
Paiements 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*
Paiements 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**
Paiements 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		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**793 350**	**36 280 495**	**0,009**	**825 325**	**43 515 617**	**0,009**
dont paiements sans contact (y compris paiements par mobile)	522 873	10 502 092	0,013	576 537	14 002 613	0,012
dont paiements par mobile	*29 807*	*2 447 707*	*0,091*	*75 039*	*4 801 997*	*0,065*
Paiements à distance (hors Internet)	**74 832**	**8 964 315**	**0,165**	**77 941**	**10 604 251**	**0,191**
Paiements sur Internet	**2 847 769**	**212 962 645**	**0,174**	**2 577 337**	**191 873 234**	**0,135**
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	267 556	69 544 332	0,096
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	159 344	11 208 886	0,071
dont paiements hors 3D-Secure	nd	nd	nd	2 150 437	111 120 015	0,205
Retraits	**102 962**	**32 477 429**	**0,029**	**121 642**	**41 437 842**	**0,035**
Total	**3 818 913**	**290 684 884**	**0,044**	**3 602 245**	**287 430 944**	**0,040**

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 2021

(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	765 957 496	42 012 617 435	451 796	37 974 415	0,590	0,09
Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager, etc.)	107 018 866	4 927 341 394	278 983	19 508 501	2,607	0,40
Voyage, transport	203 485 311	14 295 312 521	253 485	17 072 276	1,246	0,12
Téléphonie et communication	390 920 084	14 591 392 349	418 120	25 516 940	1,070	0,17
Alimentation	22 566 308	1 722 532 406	8 324	1 085 932	0,369	0,06
Équipement de la maison, ameublement, bricolage	79 961 785	12 145 770 274	43 601	12 818 325	0,545	0,11
Assurance	11 554 065	2 331 876 853	3 282	428 310	0,284	0,02
Santé, beauté, hygiène	37 833 536	2 316 225 164	27 758	2 357 014	0,734	0,10
Services aux particuliers et aux professionnels	493 951 467	31 563 992 698	973 699	52 821 511	1,971	0,17
Approvisionnement d'un compte, vente de particulier à particulier	102 986 449	9 333 326 991	100 298	21 615 649	0,974	0,23
Jeux en ligne	114 982 985	3 712 171 437	71 843	6 816 630	0,625	0,18
Divers	124 882 591	8 772 674 589	24 089	4 461 981	0,193	0,05
Total	**2 456 100 943**	**147 725 234 111**	**2 655 278**	**202 477 485**	**1,081**	**0,14**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France

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

	2017		2018		2019	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
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, valeur en milliers d'euros)

	2020		2021	
	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**11 284 433**	**428 180 387**	**13 031 098**	**480 804 099**
dont paiements sans contact (y compris paiements par mobile)	5 187 488	79 877 184	7 437 197	125 344 168
dont paiements par mobile	*145 527*	*2 979 437*	*388 175*	*8 403 747*
Paiements à distance (hors Internet)	**69 950**	**7 087 913**	**64 620**	**7 272 724**
Paiements sur Internet	**2 158 226**	**132 554 575**	**2 565 276**	**155 816 405**
dont paiements 3D-Secure avec authentification forte	nd	nd	708 194	78 650 830
dont paiements 3D-Secure sans authentification forte	nd	nd	409 008	18 152 505
dont paiements hors 3D-Secure	nd	nd	1 448 074	59 013 071
Retraits	**1 062 376**	**116 986 747**	**1 083 643**	**125 105 264**
Total	**14 574 985**	**684 809 622**	**16 744 636**	**768 998 491**

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
Paiements 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*
Paiements 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**
Paiements 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		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**841 280**	**42 883 367**	**0,0100**	**874 166**	**49 441 754**	**0,0103**
dont paiements sans contact (y compris paiements par mobile)	538 313	12 238 895	0,0153	601 803	15 600 613	0,0124
dont paiements par mobile	*35 968*	*3 640 684*	*0,1222*	*84 421*	*5 793 427*	*0,0689*
Paiements à distance (hors Internet)	**105 972**	**17 644 315**	**0,2489**	**96 257**	**15 211 163**	**0,2092**
Paiements sur Internet	**3 176 400**	**248 966 265**	**0,1878**	**2 885 920**	**227 162 875**	**0,1458**
dont paiements 3D-Secure avec authentification forte	nd	nd	nd	306 265	76 891 633	0,0978
dont paiements 3D-Secure sans authentification forte	nd	nd	nd	213 403	20 406 481	0,1124
dont paiements hors 3D-Secure	nd	nd	nd	2 366 252	129 864 761	0,2201
Retraits	**104 960**	**33 084 175**	**0,0283**	**124 077**	**42 256 276**	**0,0338**
Total	**4 228 612**	**342 578 122**	**0,0500**	**3 980 420**	**334 072 068**	**0,0434**

Note : nd, non disponible.

Source : Observatoire de la sécurité des moyens de paiement.

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, valeur en milliards d'euros, montant moyen en euros)

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

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
Volume	**114 906**	**166 421**	**183 488**	**220 685**	**321 214**
Taux de fraude (‰)	0,060	0,095	0,116	0,188	0,290
Valeur	**296 072 847**	**450 108 464**	**539 215 175**	**538 059 139**	**625 625 059**
Taux de fraude (%)	0,030	0,051	0,066	0,088	0,106
Montant moyen	**2 577**	**2 705**	**2 939**	**2 438**	**1 948**

b) Nouvelle approche

	2017	2018	2019	2020	2021
Volume	**nd**	**nd**	**nd**	**190 001**	**280 521**
Taux de fraude (‰)	nd	nd	nd	0,162	0,254
Valeur	**nd**	**nd**	**nd**	**401 611 189**	**464 942 784**
Taux de fraude (%)	nd	nd	nd	0,065	0,079
Montant moyen	**nd**	**nd**	**nd**	**2 114**	**1 657**

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	
	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	274 996	86
Falsification	15 738	13,7	17 178	10,3	16 459	9,0	13 894	6	36 073	11
Contrefaçon	7 234	6,3	8 092	4,9	9 574	5,2	7 207	3	5 119	2
Détournement, rejeu	1 946	1,7	2 793	1,7	3 244	1,8	2 830	1	5 026	2
Valeur										
Vol, perte	130 815 653	44,2	252 890 727	56,2	296 367 562	55,0	365 813 764	68,0	398 698 840	63,7
Falsification	127 157 212	42,9	145 737 424	32,4	145 881 745	27,1	102 801 337	19,1	100 377 757	16,0
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
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

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, valeur en millions d'euros)

	2017		2018		2019		2020		2021	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Total	**3870**	**24069448**	**4038**	**24211142**	**4251**	**25879217**	**4483**	**32713128**	**4843**	**38722734**
dont virements SEPA – SCT	3801	9259478	3974	10846914	4174	9602866	4384	10029108	4668	12980883
dont virements SEPA instantanés – SCT Inst	nd	nd	0	86	14	7074	45	26243	107	50053
dont virements de gros montants – VGM [a]	10	9483487	10	10130586	9	12266316	9	19042030	9	19661685
dont autres virements	59	5326483	53	3233556	54	4002960	45	3615748	59	6030114
Total – hors VGM	**3860**	**14585961**	**4028**	**14080556**	**4242**	**13612900**	**4474**	**13671098**	**4834**	**19061050**

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)

	2018			2019		
	Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude
Total	**7736**	**97327128**	**0,0004**	**15934**	**161642174**	**0,0006**
dont virements SEPA – SCT	6521	78314614	0,0007	13302	127572549	0,0013
dont virements SEPA instantanés – SCT Inst	5	29800	0,0345	729	2203240	0,0311
dont virements de gros montants – VGM [a]	14	4622598	0,0000	15	15476053	0,000
dont autres virements	1196	14360116	0,0004	1888	16390332	0,0004
Total – hors VGM	**7722**	**92704530**	**0,0007**	**15919**	**146166121**	**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		
	Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude
Total	**35893**	**266969099**	**0,0008**	**46718**	**287264068**	**0,0007**
dont virements SEPA – SCT	25254	191474396	0,0019	33199	246527533	0,0019
dont virements SEPA instantanés – SCT Inst	7131	10562419	0,0402	12913	22406942	0,0448
dont virements de gros montants – VGM [a]	51	2439224	0,000	5	1539120	0,0000
dont autres virements	3457	62493060	0,0017	601	16790473	0,0003
Total – hors VGM	**35842**	**264529875**	**0,0019**	**46713**	**285724948**	**0,0015**

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
Volume	**4 642**	**7 736**	**15 934**	**35 893**	**46 718**
Taux (‰)	0,0012	0,0019	0,0037	0,0080	0,0096
Valeur	**78 286 492**	**97 327 128**	**161 642 174**	**266 969 099**	**287 264 068**
Taux (%)	0,0003	0,0004	0,0006	0,0008	0,0007
Montant moyen	**16 865**	**12 581**	**10 144**	**7 438**	**6 149**

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	
	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**
Part	81,9	53,7	71,4	52,5	86,4	61,0	78,6	32,6	76,8	30,4
Falsification	**57**	**1 304 143**	**151**	**485 131**	**125**	**3 438 923**	**203**	**3 377 807**	**875**	**5 387 862**
Part	1,2	1,7	2,0	0,5	1,6	2,1	0,6	1,3	1,9	1,9
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**
Part	10,0	42,1	13,4	41,4	19,8	35,0	16,0	58,9	18,2	58,5
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**
Part	6,9	2,6	13,2	5,7	3,18	1,96	4,87	7,2	3,1	9,2

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.

T21 Prélèvements émis par type de mandat

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

	2017		2018		2019		2020		2021	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
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**
Prélèvements par type de mandat										
dont prélèvements consentis par mandat électronique	nd	nd	nd	nd	nd	nd	nd	nd	1 106	430 781
dont prélèvements consentis par mandat papier	nd	nd	nd	nd	nd	nd	nd	nd	3 914	1 464 317
Prélèvements par mode d'initiation										
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
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

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
Volume	**25 801**	**309 377**	**43 519**	**6 485**	**251 010**
Taux de fraude (‰)	0,0063	0,0735	0,0100	0,0014	0,0500
Valeur	**8 726 403**	**58 346 253**	**10 990 025**	**1 891 051**	**25 318 677**
Taux de fraude (%)	0,0006	0,0035	0,0006	0,0001	0,0013
Montant moyen	**338**	**189**	**253**	**292**	**101**

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	
	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**
Part	92,8	70,4	100,0	100,0	33,6	36,0	92,7	73,4	99,8	99,5
Détournement	**1 832**	**2 305 112**	**72**	**16 703**	**26 223**	**6 677 467**	**62**	**10 720**	**517**	**116 968**
Part	7,1	26,4	0,0	0,0	60,3	60,8	1,0	0,6	0,2	0,5

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

Directrice de la publication
Nathalie Aufauvre
Directrice générale de la Stabilité financière et des Opérations de marché
Banque de France

Rédactrice en chef
Claudine Hurman
Directrice des Infrastructures, de l'Innovation et des Paiements
Banque de France

Secrétariat de rédaction
Pierre Bienvenu, Véronique Bugaj, Olivier Catau, Caroline Corcy, Anne-Marie Fourel, Trân Huynh, Marc-Antoine Jambu, Julien Lasalle, Ibtissam Lesca

Réalisation
Studio Création
Direction de la Communication

Contact
Observatoire de la sécurité des moyens de paiement
Code courrier : 011-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Impression
Banque de France – SG - DISG

Dépôt légal
Juillet 2022
ISSN 2557-1230 (en ligne)
ISSN 2556-4536 (imprimé)

Internet
www.observatoire-paiements.fr

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

www.banque-france.fr