OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2023

BANQUE DE FRANCE
EUROSYSTÈME

www.observatoire-paiements.fr

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2023

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

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

SEPTEMBRE 2024

SOMMAIRE

SYNTHÈSE

L'année 2023 confirme la progression générale de l'usage des moyens de paiement scripturaux (+ 5,4 % en nombre de paiements) observée ces dernières années, portée par une adoption dynamique de nouveaux modes de paiement, tels que le paiement par mobile ou le virement instantané, ainsi que par une croissance toujours vigoureuse du e-commerce.

Le chapitre 1 du rapport, qui présente les évolutions statistiques sur l'usage des moyens de paiement et la fraude, fait état d'une stabilité du montant total de fraude, qui reste sous la barre des 1,2 milliard d'euros. *Le rapport relève toutefois des évolutions différenciées selon les moyens de paiement :*

- ***La carte, qui conforte son statut de moyen de paiement principal du quotidien, voit son taux de fraude se stabiliser à 0,053 %, son niveau le plus bas jamais enregistré par l'Observatoire, pour un montant de 496 millions d'euros.*** *Les taux de fraude sont orientés à la baisse sur tous les canaux d'initiation électronique de paiements et de retraits, avec des plus bas historiques enregistrés sur les segments en plus forte croissance, en particulier sur le sans-contact (0,011 %), sur le paiement par mobile (0,021 %) et sur les paiements sur internet (0,160 %). Le taux de fraude moyen de la carte demeure néanmoins stable, en raison de l'augmentation de la part des paiements sur internet, qui restent proportionnellement plus exposés à la fraude.* ***La sécurité de la carte continue ainsi à bénéficier de l'effet des règles d'authentification forte définies par la deuxième directive européenne sur les services de paiement (DSP 2).*** *La mise en œuvre de ces règles explique en grande partie la poursuite de la baisse de la fraude sur les paiements sur internet, mais aussi sur les paiements mobiles, dont le taux de fraude a été divisé par trois grâce au recours systématique à une authentification forte du porteur au moment de l'enrôlement de sa carte dans une solution mobile. Dans ce contexte général de maîtrise de fraude à la carte, la technique de fraude dominante reste l'usurpation du numéro de la carte par hameçonnage (72 % de la fraude en valeur), parfois associée à de la manipulation par téléphone pour amener la victime à authentifier les transactions frauduleuses ;*

- ***Le montant des opérations frauduleuses par chèque continue à fléchir pour atteindre 364 millions d'euros*** *(– 8 % par rapport à 2022). Cette régression de la fraude s'explique en grande partie par la mise en place de mécanismes de prévention par les banques, conformément à la feuille de route de l'Observatoire, et notamment de* ***dispositifs de blocage ou de temporisation des remises de chèques qui ont permis de neutraliser 222 millions d'euros de transactions frauduleuses en 2023*** *(+ 38 % par rapport à 2022). Toutefois, compte tenu de la baisse continue des montants échangés par chèque (– 13,4 %), le taux de fraude rebondit en 2023 (0,078 %, contre 0,073 % en 2022). La principale typologie de fraude reste, de loin, l'utilisation de chèques perdus ou volés directement remis à l'encaissement par le fraudeur ou utilisés comme moyen de règlement auprès des commerçants ou de particuliers (66 % des montants de fraude et 89 % des transactions frauduleuses) ;*

- ***Le montant de la fraude au virement est globalement stable (– 0,5 %)*** *à 312 millions d'euros en 2023, alors que le volume des transactions frauduleuses progresse de 18 %. En raison des montants importants échangés par virement, le taux de fraude reste très bas à 0,001 %. La fraude touche à la fois les particuliers et les professionnels, principalement par l'utilisation de leur banque en ligne, avec deux modes opératoires principaux : d'un côté, les fraudes par manipulation (notamment au faux conseiller bancaire) pour conduire la victime à valider de faux ordres de virement (43 % des montants fraudés), et de l'autre, les fraudes par détournement dans lesquelles le fraudeur va modifier une facture ou un ordre de paiement légitime pour récupérer les fonds (48 % des montants fraudés).* ***Enfin, l'adoption de l'usage du virement instantané (+ 46 %***

en montant) est favorisée par un contexte de fraude maîtrisée, avec un taux de fraude qui reste orienté à la baisse (0,040 %) et inférieur à celui de la carte.

Le chapitre 2 présente les travaux réalisés par l'Observatoire dans le cadre de la prévention de la fraude, avec un focus sur trois sujets :

- ***L'Observatoire a réalisé un état des lieux des moyens et des meilleures pratiques de sécurisation des paiements par virement et par prélèvement****, assorti d'un premier ensemble de recommandations pour renforcer la sécurité de ces instruments, surtout en matière de partage de données entre établissements et de sensibilisation des utilisateurs ;*

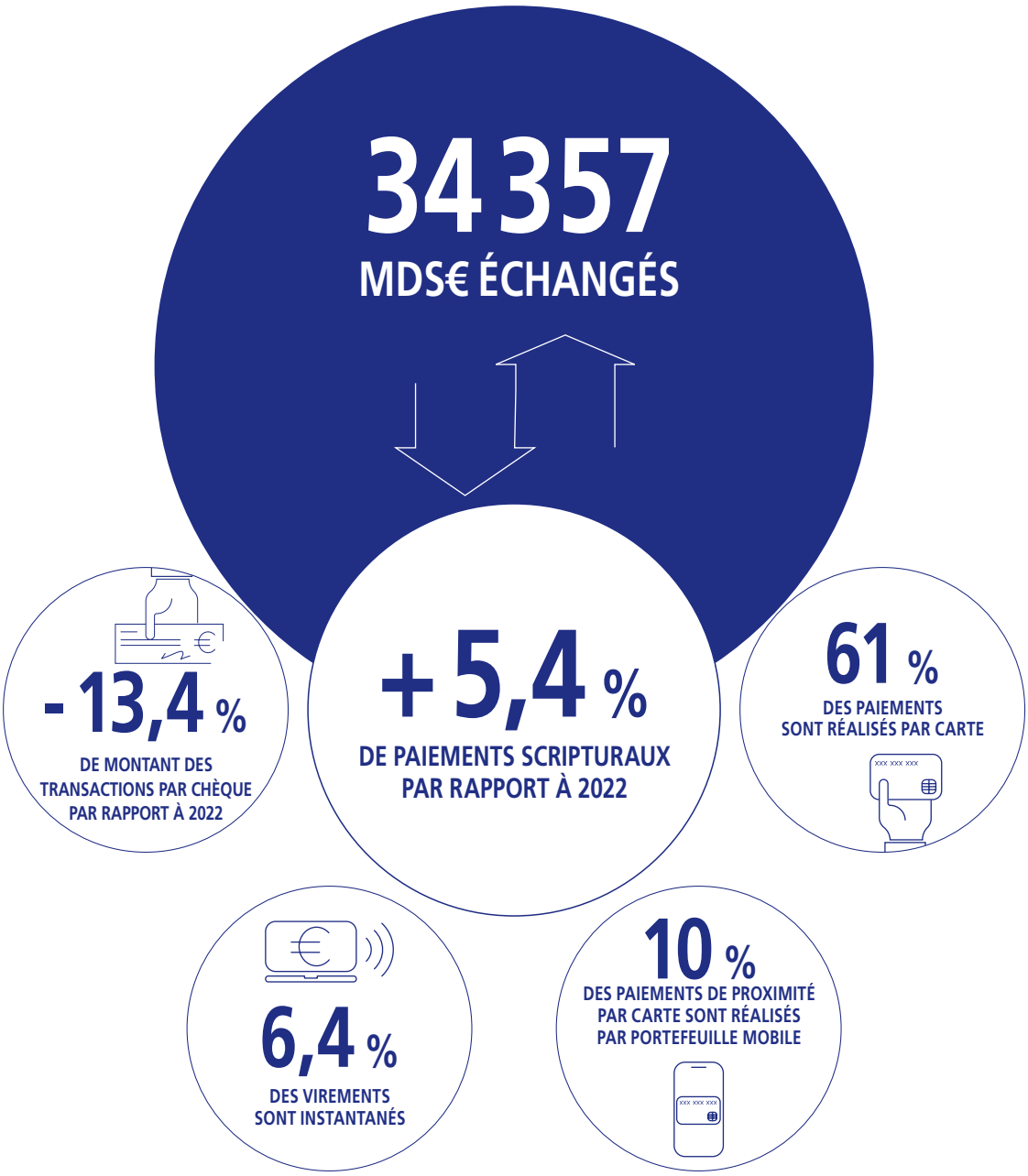
- *Concernant les paiements par carte à distance,* ***l'Observatoire a adopté un plan d'action qui vise à renforcer le niveau de sécurité des paiements non authentifiés émis sans recourir au protocole technique 3-D Secure****, qui restent deux à trois fois plus fraudés que les paiements utilisant ce protocole. Les premières mesures sont entrées en application le 10 juin 2024, avec en particulier la mise en place d'un plafonnement de l'acceptation de ces flux à 500 euros par carte et par commerçant, qui aura vocation à être abaissé à 250 puis 100 euros avant la fin de l'année 2024, sauf pour certains secteurs d'activité ;*

- *Face au développement de schémas de fraude par manipulation recourant à l'usurpation d'identité des banques ou d'entités publiques à travers les réseaux de télécommunications,* ***l'Observatoire a approfondi ses travaux avec le secteur des télécommunications pour suivre la mise en place des mesures de prévention****, dont le programme MAN (mécanisme d'authentification des numéros) qui vise à certifier le numéro présenté lors de la réception d'un appel téléphonique.*

Le chapitre 3 restitue les travaux de l'Observatoire sur l'informatique quantique et la sécurité des systèmes de paiement par carte bancaire*, dans le cadre de ses missions de veille technologique. L'informatique quantique offre des perspectives prometteuses dans de nombreux domaines (finance, logistique, météorologie, chimie, etc.), tout en suscitant de nouveaux défis, notamment en matière de sécurité dans le numérique. Ainsi, le déchiffrement des communications et protocoles électroniques sécurisés selon les standards actuels, dont ceux utilisés dans les paiements, pourrait devenir une réalité à un horizon de dix à vingt ans.* ***Il s'agit d'une menace sérieuse pour la sécurité nationale, déjà prise en compte par les autorités publiques*** *(loi française de programmation militaire, août 2023), et dont le secteur des paiements doit se saisir dès maintenant en raison des cycles de vie des matériels et logiciels de paiement par carte (puces, terminaux de paiement électronique, serveurs, etc.).* ***C'est pourquoi l'Observatoire a adopté un ensemble de recommandations qui visent à assurer sur le long terme la bonne préparation du marché français des paiements face à cette « menace quantique ».***

Dans un contexte d'évolution rapide des moyens de paiement, mais aussi des techniques de fraude, l'Observatoire reste mobilisé pour veiller à la sécurité de l'ensemble des moyens de paiement et ainsi offrir à tous les utilisateurs, des particuliers aux entreprises, une authentique liberté de choix dans leurs usages au quotidien. Dans son programme de travail pour 2024 et 2025, l'Observatoire s'attachera en particulier à étudier les possibilités de partage d'informations en vue de renforcer les moyens de lutte contre la fraude au virement, et à poursuivre les actions engagées avec les acteurs du secteur des télécommunications d'une part et du commerce à distance d'autre part. Enfin, l'Observatoire va orienter ses travaux de veille technologique sur l'utilisation des méthodes de scoring *et de l'intelligence artificielle dans le cadre de la lutte contre la fraude.*

L'USAGE DES MOYENS DE PAIEMENT EN 2023



L'ÉVOLUTION DE LA FRAUDE EN 2023

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

-35 %
DE TAUX DE FRAUDE POUR LES PAIEMENTS PAR CARTE SUR INTERNET DEPUIS 2019

222 M€
DE TRANSACTIONS FRAUDULEUSES NEUTRALISÉES SUR LE CHÈQUE

1,195
MD€ DE PRÉJUDICE

+0,2 %
DE FRAUDE EN VALEUR

0,040 %
DE TAUX DE FRAUDE SUR LES VIREMENTS INSTANTANÉS

379 M€
DE FRAUDE PAR MANIPULATION

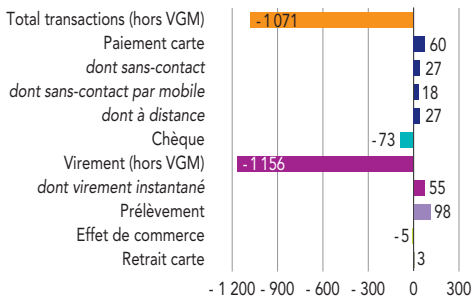
1

ÉTAT DE LA FRAUDE EN 2023

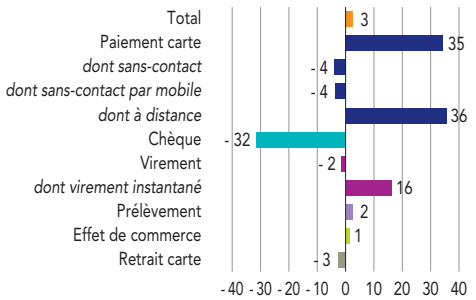
Données clés

G1 Évolution des moyens de paiement entre 2022 et 2023

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



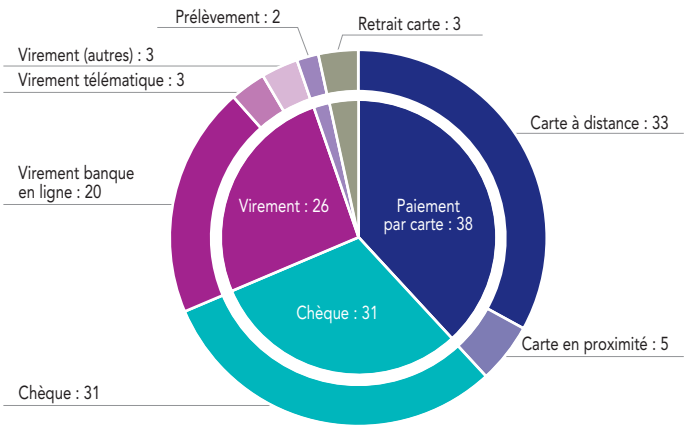
b) Fraude (en millions d'euros)



Note : VGM, virement de gros montant.

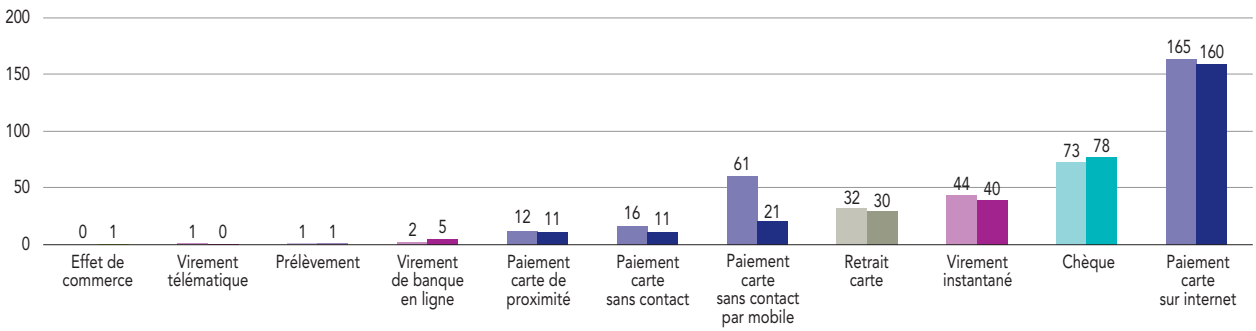
Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

G3 Vulnérabilité des principaux canaux de paiement à la fraude en 2022 et 2023 (en euros de fraude pour 100 000 euros de paiement)



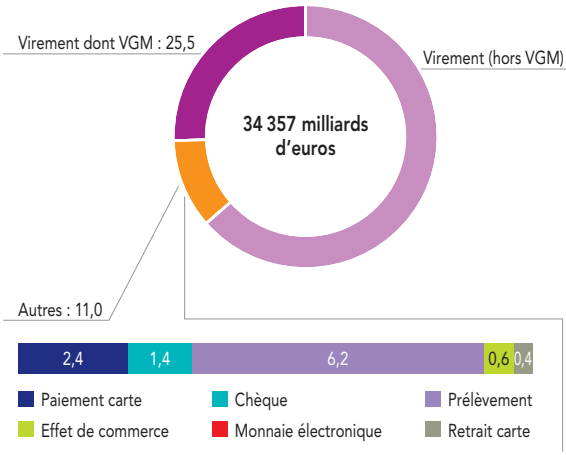
Source : Observatoire de la sécurité des moyens de paiement.

1.1 Vue d'ensemble

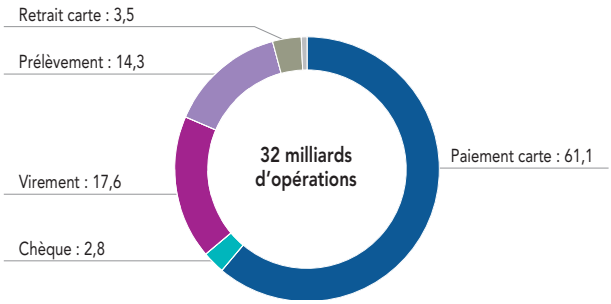
1.1.1 Cartographie des moyens de paiement

G4 Usage des moyens de paiement scripturaux en 2023 (en %)

a) En montant



b) En volume



Note : VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

Les opérations de paiement scripturales réalisées par les particuliers, les entreprises et les administrations ont atteint 32,2 milliards de transactions en 2023 (+ 5,2 % par rapport à 2022), pour un total de 34 357 milliards d'euros (– 19,3 % par rapport à 2022). La baisse importante des montants échangés, de plus de 8 000 milliards d'euros, s'explique principalement par la contraction des virements de gros montant (VGM)[1], en repli de 45 % comparativement à 2022. Cette variation est imputable à la modification des pratiques de gestion de trésorerie de certaines administrations dans un contexte de taux d'intérêt redevenus positifs et, plus marginalement, à l'évolution de l'activité économique. Les opérations de paiement scripturales hors VGM s'inscrivent en légère diminution (– 4 %, soit – 1 071 milliards d'euros).

Les virements restent prépondérants dans le total des flux en montant, avec une part stable à 89 %. En particulier, les VGM atteignent 29 % des montants échangés par virements, pour seulement 1,3 % de leur nombre. Le virement instantané poursuit sa progression rapide (+ 84 % en volume et + 46 % en valeur) pour représenter désormais 6,4 % des virements en volume (contre 3,8 % en 2022).

La carte bancaire demeure le moyen de paiement scriptural préféré des Français. Sa part, hors retraits, dans les volumes de transactions continue de progresser, et passe de 59,6 % en 2022 à 60,7 % en 2023. La croissance des flux en volume se retrouve aussi dans le paiement sans contact (68 % des paiements par carte de proximité, contre 61 % en 2022), dont en particulier par mobile (10 % des paiements par carte de proximité, contre près de 6 % en 2022).

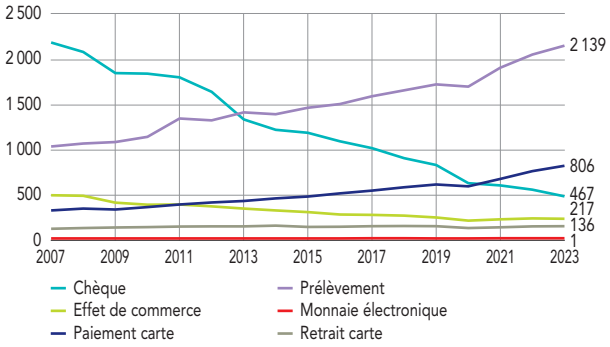
Le montant des transactions par chèque se replie toujours (– 13,4 %), ainsi que le nombre de chèques émis (– 11,6 %). Les chèques représentent désormais moins de 3 % des transactions scripturales.

Les retraits d'espèces par carte restent relativement stables d'une année sur l'autre (– 0,8 % en volume et + 2,0 % en valeur).

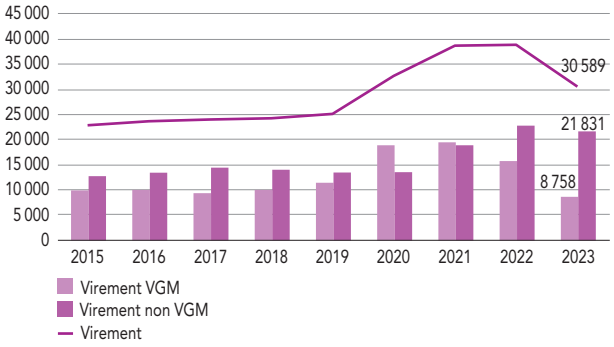
1 Virements de gros montant (VGM) : virements émis au travers de systèmes de règlement de montant élevé (Target2 et Euro1) réservés à des paiements professionnels.

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

a) Par instrument (hors virement)



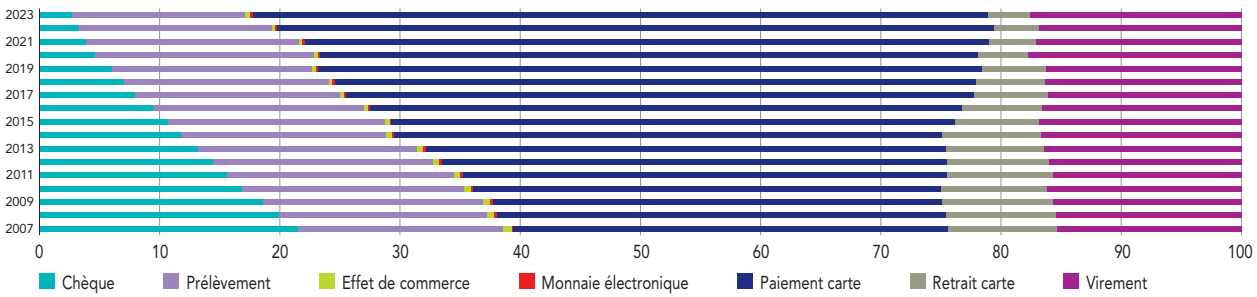
b) Par virement



Note : VGM, virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

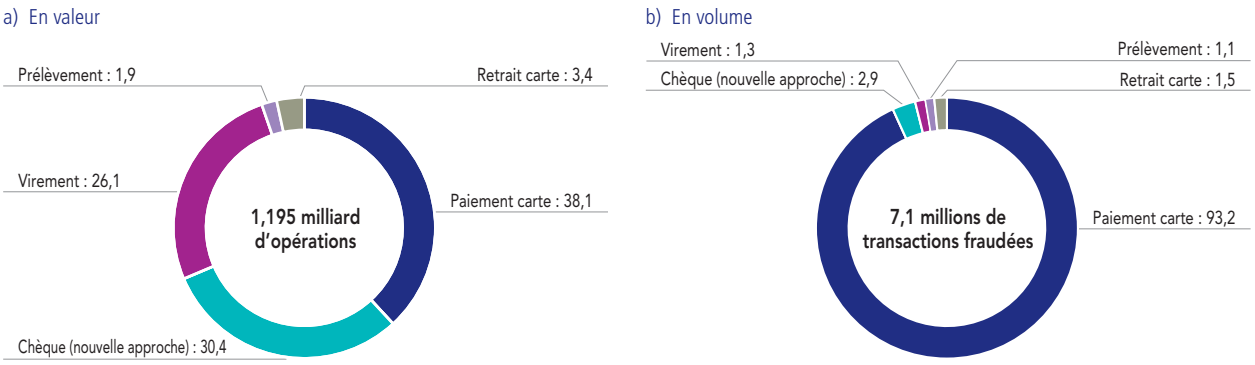
1.1.2 Panorama de la fraude aux moyens de paiement

La fraude aux moyens de paiement scripturaux se stabilise à 7,1 millions d'opérations (– 0,6 % par rapport à 2022), pour un préjudice de 1,195 milliard d'euros (+ 0,2 % par rapport en 2022).

Au regard des principales évolutions observées, cette tendance résulte, d'une part, d'une baisse de la fraude sur le chèque (– 32 millions d'euros), contrebalancée, d'autre part, par une hausse de la fraude sur la carte (+ 35 millions d'euros), en particulier sur le paiement par carte à distance (+ 36 millions d'euros) :

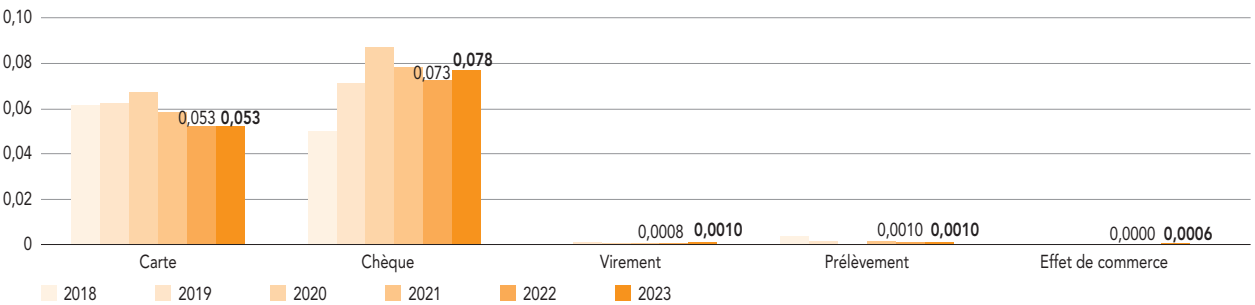
- Bien que le montant de la fraude tend à diminuer sur le chèque, le taux de fraude sur ce moyen de paiement repart à la hausse, dans un contexte où les règlements par chèque baissent plus rapidement que la fraude (– 14 % de montants échangés, contre – 8 % de montants de fraude) ;
- À l'inverse, le taux de fraude global sur la carte se maintient à 0,053 %, son plus bas niveau historique, dans la mesure où la fraude croît à un rythme équivalent à celui des opérations de paiement (+ 8 % par rapport à 2022). La carte représente désormais 38,1 % des montants de fraude en 2023, contre 35,3 % en 2022.

G7 Répartition de la fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

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



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

Source : Observatoire de la sécurité des moyens de paiement.

1.2 État de la fraude sur la carte de paiement

1.2.1 Vue d'ensemble – Cartes émises en France

La carte conforte son statut de moyen de paiement principal du quotidien, avec des flux qui continuent de progresser en 2023, dans les mêmes proportions en volume et en valeur (+ 7 %). Les paiements effectués par mobile poursuivent leur croissance, et se situent désormais à 4 % du montant des opérations par carte émise en France en 2023, contre 2 % en 2022.

Après deux années enchaînant repli puis stabilisation, la valeur de la fraude repart à la hausse pour atteindre 496 millions d'euros (+ 7 % par rapport à 2022). Le canal des paiements par carte sur internet reste le plus exposé, avec 71 % de la valeur de la fraude, contre uniquement 23 % du montant total des opérations. Par ailleurs, la part de la fraude sur les paiements sans contact et par mobile continue de régresser : elle passe respectivement de 3 à 2 % et de 2 à 1 %.

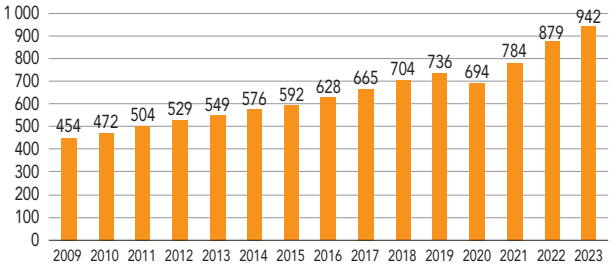
Après avoir confirmé une diminution proche de 10 % sur deux années consécutives grâce à la généralisation de l'authentification forte sur les transactions à distance, le taux de fraude sur les opérations par carte émise en France se stabilise à 0,053 % en 2023, soit son plus bas niveau historique.

Cette tendance s'analyse au travers de deux effets qui se compensent : d'une part, une baisse de 2 points de base liée à la réduction des taux de fraude sur presque tous les canaux d'initiation (hormis les paiements à distance hors internet) ; d'autre part, une hausse de 2 points de base liée à une proportion accrue, dans les flux, des paiements sur internet, relativement plus exposés à la fraude.

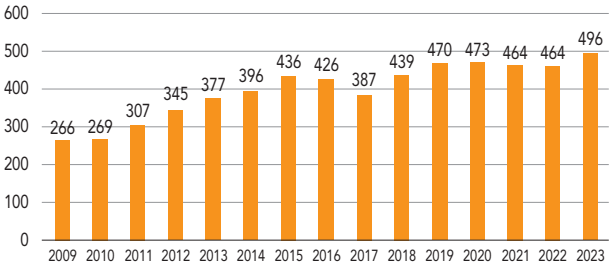
Le taux de fraude sur les paiements sur internet poursuit sa baisse : il passe de 0,165 % en 2022 à 0,160 % en 2023 (– 3 %),

G9 Les cartes émises en France en 2023

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



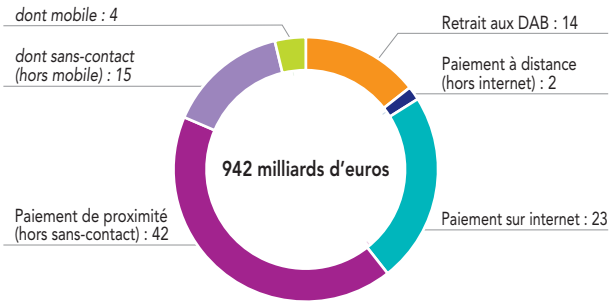
b) Valeur totale de la fraude (en millions d'euros)



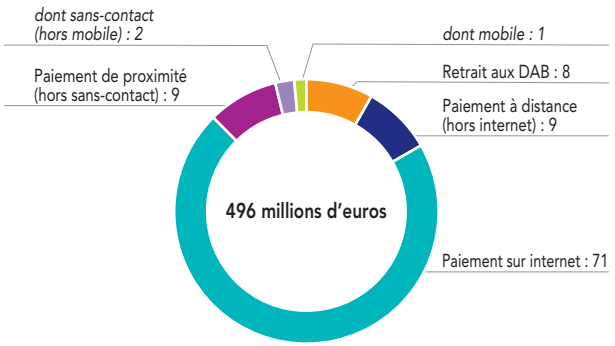
Source : Observatoire de la sécurité des moyens de paiement.

G10 Le canal d'utilisation des cartes émises en France en 2023 (en %)

a) Répartition du montant des opérations



b) Répartition de la valeur de la fraude



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

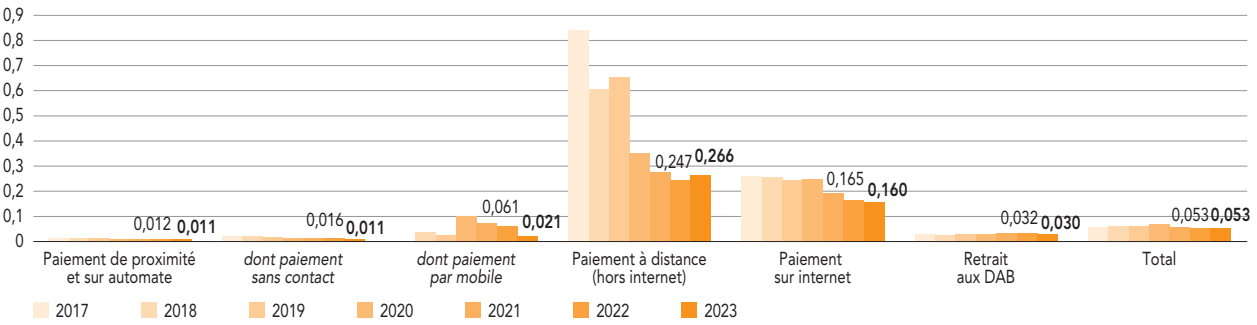
et atteint ainsi un nouveau plus bas niveau historique. Cela confirme l'effet très positif des règles d'authentification forte de la directive sur les services de paiement (DSP 2) et de l'amélioration des outils de mesure du risque développés par les acteurs de la monétique.

Le taux de fraude sur les paiements à distance hors internet repart à la hausse, passant de 0,247 % en 2022 à 0,266 % en 2023, alors qu'il était en constante diminution depuis 2019. Toutefois, ces opérations de paiement où le numéro de carte est communiqué par courrier, téléphone ou courriel représentent moins de 2 % des paiements par carte.

Enfin, le taux de fraude des paiements par mobile a été divisé par trois par rapport à 2022 (0,021 %, contre 0,061 %). Cela découle principalement du renforcement des outils de maîtrise du risque de fraude, notamment au moment de l'enrôlement de la carte dans la solution par le recours systématique à une authentification forte du porteur. Ces progrès sont d'autant plus importants que ce moyen de paiement est en plein essor depuis 2019. En effet, son utilisation a été multipliée, en montant, par un peu plus de 42 entre 2019 et 2023, et représente en 2023 6 % du montant total des paiements par carte de proximité et 20 % des paiements sans contact.

Le paiement sans contact confirme sa position de mode de paiement privilégié en proximité (68 % des transactions pour 31 % des montants). Son taux de fraude fléchit à 0,011 %, plus bas niveau historique. Cette baisse résulte surtout d'une diminution des vols de cartes donnant lieu à quelques transactions inférieures au plafond de 50 euros.

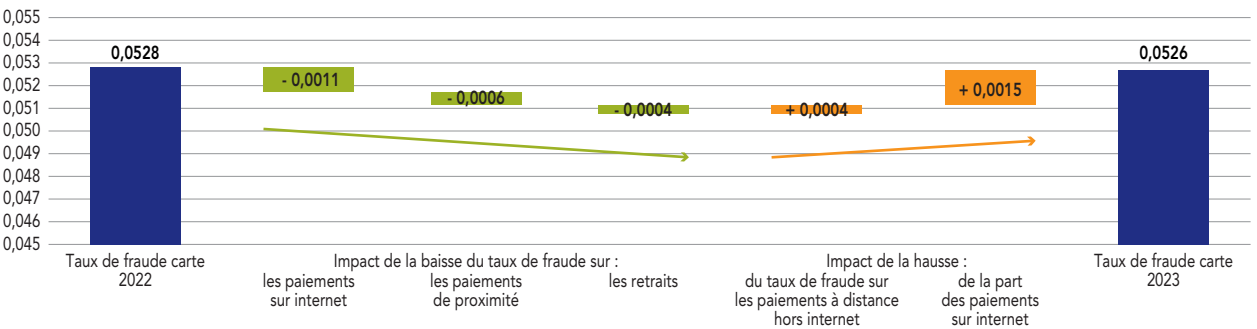
G11 Évolution des taux de fraude en valeur sur les cartes françaises par canal d'initiation (en %)



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

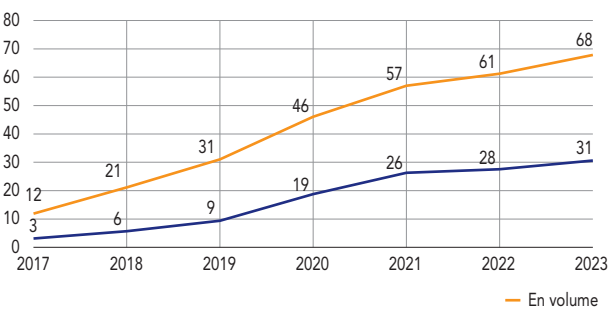
G11 bis Impact de l'évolution des taux de fraude par canal sur le taux de fraude global (en %)



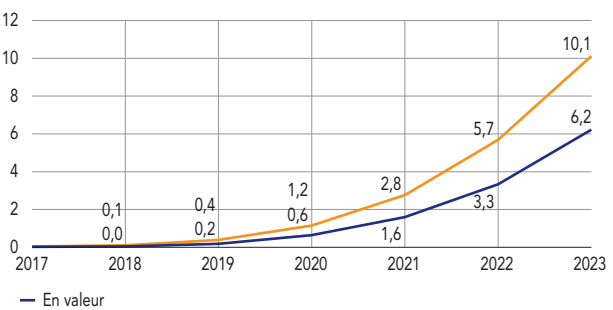
Source : Observatoire de la sécurité des moyens de paiement.

G12 Paiements par carte de proximité (en %)

a) Part des paiements sans contact



b) Part des paiements par mobile

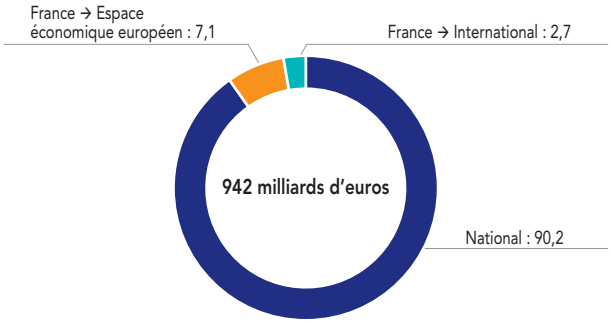


Source : Observatoire de la sécurité des moyens de paiement.

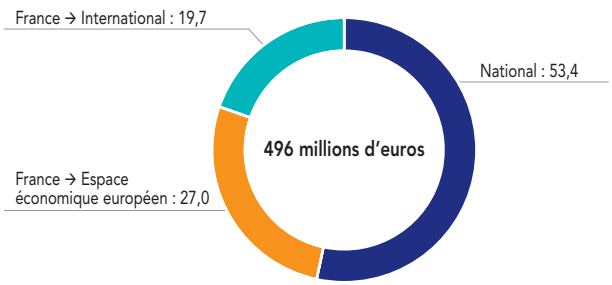
1.2.2 Répartition de la fraude par zone géographique – Cartes émises en France

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

a) Répartition du montant des opérations

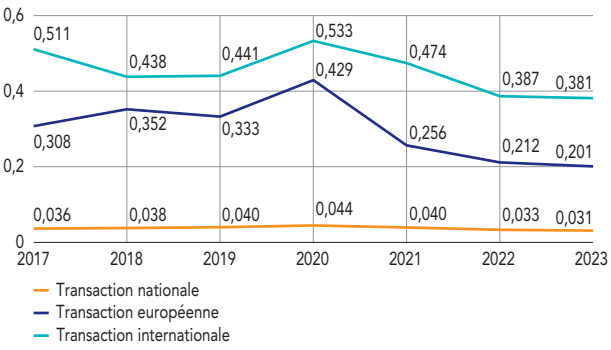


b) Répartition de la valeur de la fraude



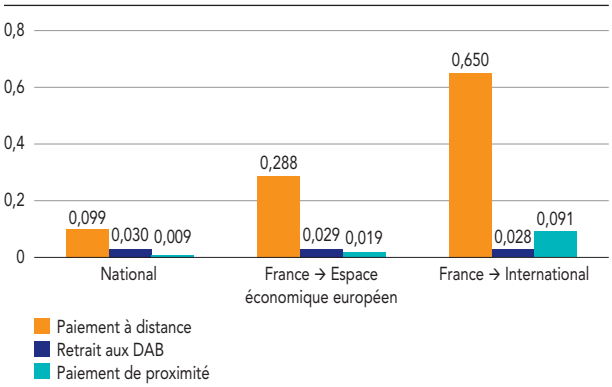
Source : Observatoire de la sécurité des moyens de paiement.

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



Source : Observatoire de la sécurité des moyens de paiement.

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



Note : DAB, distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

En 2023, les transactions internationales (incluant celles vers l'Espace économique européen) représentent en valeur, de manière stable, 10 % des opérations réalisées au moyen de cartes émises en France. Elles concentrent près de 47 % de la fraude (contre 43 % en 2022), pour un préjudice de 231 millions d'euros.

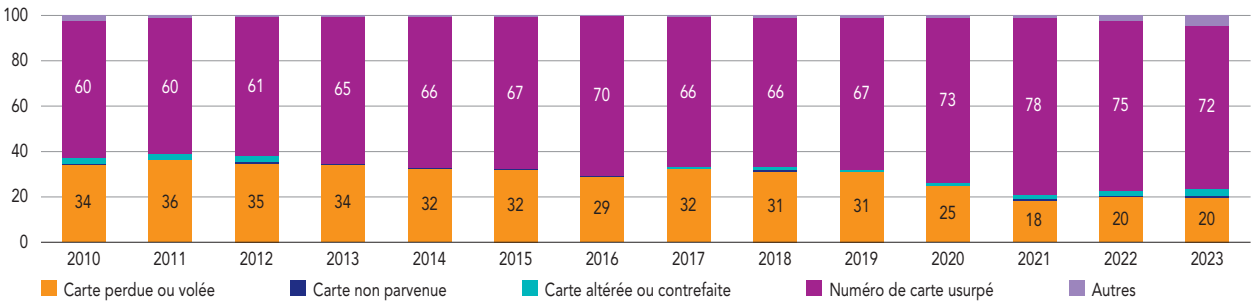
Toutefois, si les transactions par carte à l'international sont structurellement plus sujettes à la fraude, car constituées pour l'essentiel de paiements à distance, leur taux de fraude continue de s'améliorer. Ainsi, le taux pour les transactions européennes (c'est-à-dire réalisées avec des cartes françaises auprès d'accepteurs européens) baisse de 17 %, et celui des transactions internationales de 2 %.

Quelle que soit la zone géographique, le canal des paiements à distance (majoritairement sur internet) affiche les taux de fraude les plus élevés. Dans l'Espace économique européen, le taux de fraude des paiements sur internet recule toutefois de 8 %, grâce aux règles d'authentification forte, mais reste néanmoins trois fois plus élevé que celui observé sur le plan national (0,278 %, contre 0,093 %).

Les paiements de proximité à l'international sont plus exposés à la fraude, en raison de technologies moins robustes et donc plus vulnérables à la contrefaçon, comme la lecture de piste magnétique ou la prise d'empreinte physique de la carte.

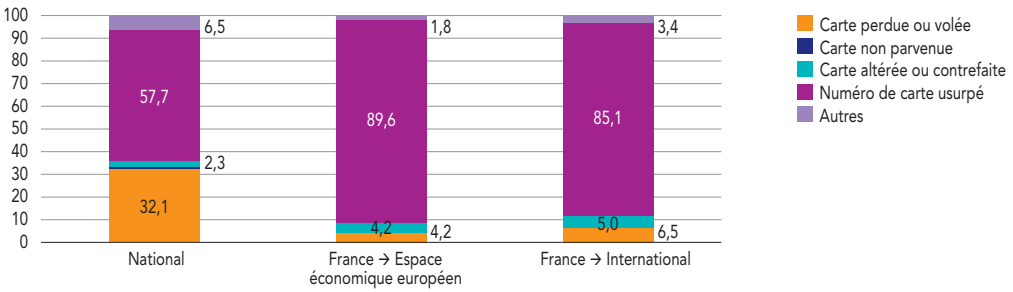
1.2.3 Répartition de la fraude par mode opératoire – Cartes émises en France

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



Source : Observatoire de la sécurité des moyens de paiement.

G17 Typologies dans la valeur de la fraude par zone géographique en 2023 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

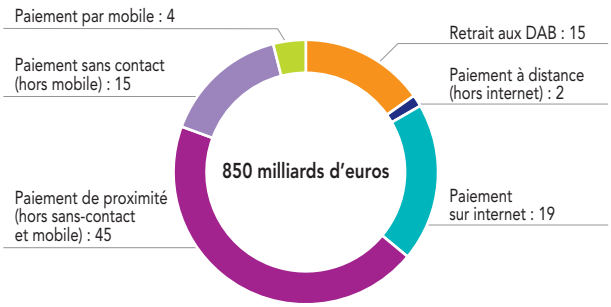
La part de la fraude fondée sur l'usurpation de numéros de carte demeure prépondérante, même si elle continue de décroître légèrement, de 75 % en 2022 à 72 % en 2023. La technique employée reste l'hameçonnage par courriel ou par SMS.

La part de la fraude liée à la perte ou au vol de carte se stabilise, toujours à un niveau modeste (20 %). Très logiquement, l'usage des cartes perdues ou volées se manifeste d'abord sur le territoire national (32 % de la fraude), tandis que la fraude par usurpation du numéro de carte se concrétise d'abord sur internet, constat partagé dans l'ensemble des zones géographiques. L'utilisation des cartes altérées ou contrefaites se produit principalement dans les pays extérieurs à l'Union européenne (5 % seulement de la fraude dans l'UE), où le standard de la carte à puce n'est pas encore généralisé.

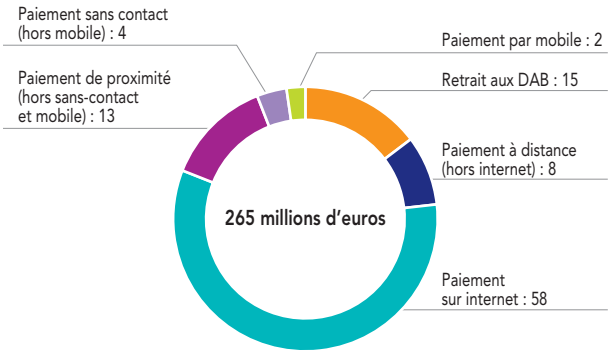
1.2.4 Répartition de la fraude sur les opérations nationales

G18 Transactions nationales par carte en montant (en %)

a) Répartition des transactions

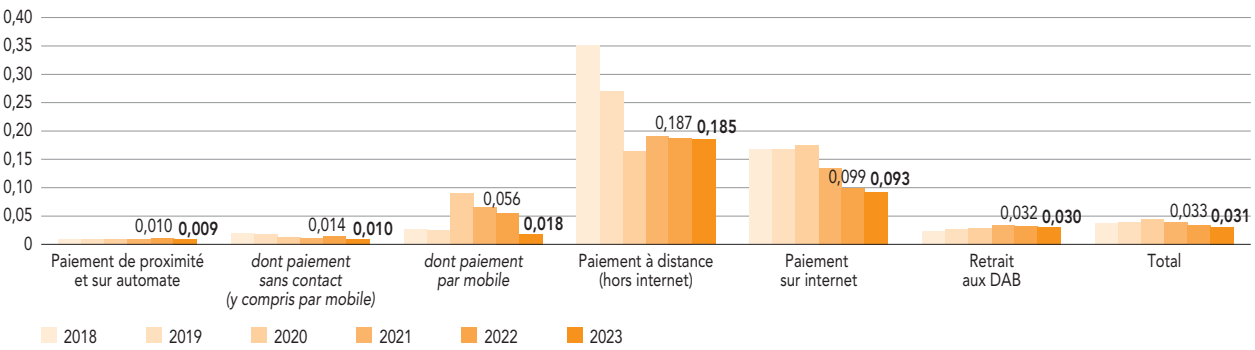


b) Répartition de la fraude



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

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



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

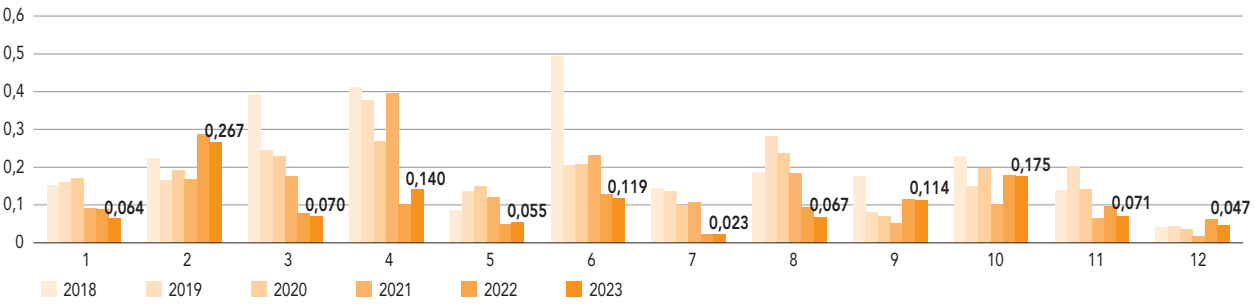
Dans les opérations nationales réalisées par carte, la part des paiements à distance demeure stable en 2023, à 21 %, l'essentiel étant effectué sur internet (93 %). Avec 175 millions d'euros de fraude relevés, ces opérations pèsent pour près de 66 % dans le total de la fraude nationale (58 % pour les paiements sur internet), en augmentation de 3 points par rapport à 2022. Les paiements sur internet continuent toutefois de bénéficier de la généralisation de la mise en place de l'authentification forte (directive DSP 2). En effet, le taux de fraude sur ces paiements recule encore de 6 % par rapport à 2022, à 0,093 %, son plus bas niveau historique. En six ans, depuis 2017 où les règles d'authentification forte n'étaient pas entrées en application, ce taux de fraude a ainsi été divisé par deux.

Les paiements par mobile continuent de croître ; ils représentent désormais 4 % des transactions nationales, pour seulement 2 % de la valeur de la fraude totale. La mise en œuvre de mesures de sécurité, telles que l'authentification forte à l'enrôlement, a fait chuter le taux de fraude de près de 68 % entre 2022 et 2023, à 0,018 %.

Au total, la tendance au repli du taux de fraude sur les transactions nationales par carte se confirme, avec une baisse de 6 % en 2023, qui l'amène à 0,031 %, après une première régression de 16 % en 2022.

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

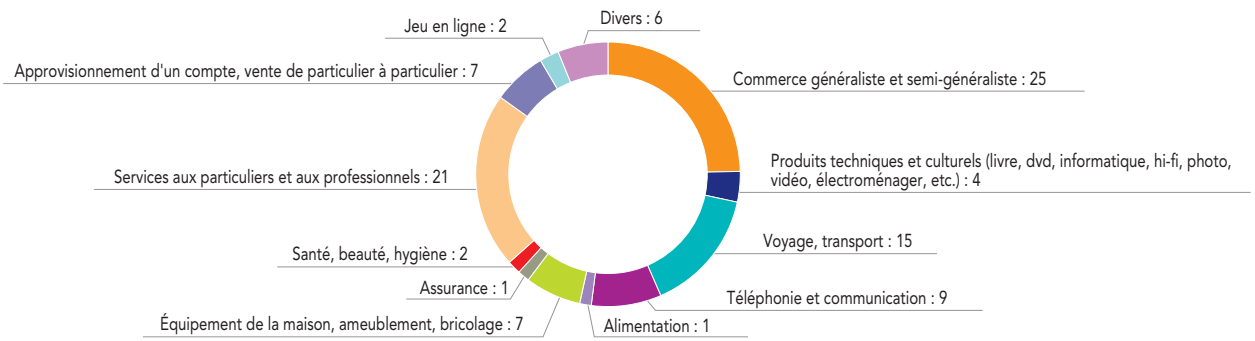
G20 Évolution du taux de fraude sur les paiements nationaux par carte sur internet, par secteur (en %)



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

Source : Observatoire de la sécurité des moyens de paiement.

G21 Répartition de la fraude sur les paiements nationaux par carte sur internet en valeur, par secteur en 2023 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

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

Source : Observatoire de la sécurité des moyens de paiement.

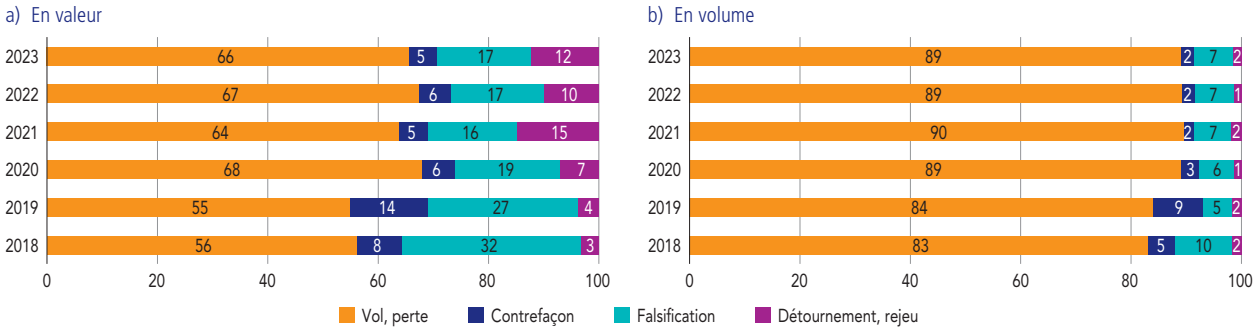
Les paiements nationaux par carte sur internet avec recours au protocole d'échange 3-D Secure (ou protocole privatif équivalent) sont proportionnellement trois fois moins fraudés que ceux réalisés sans cette sécurisation. Parmi les paiements hors 3-D Secure se trouvent principalement des paiements initiés par le commerçant (*merchant initiated transactions*, MIT), qui s'apparentent à des prélèvements avec la carte comme support (abonnements, paiements différés ou réservations par exemple), ainsi que certaines transactions exemptées d'authentification forte.

Les paiements hors 3-D Secure avec authentification forte ont fait l'objet d'une première déclaration en 2023 auprès de la Banque de France par les réseaux de paiement par carte et les établissements bancaires assujettis. Ce sont essentiellement des paiements réalisés à l'aide de portefeuilles mobiles de type X-Pay. Sur le plan national, le taux de fraude correspondant, de 0,12 %, se situe au niveau du taux de fraude sur les paiements sur internet (0,09 %).

Par ailleurs, sur le plan national, les modalités du dispositif d'exemption à l'authentification forte s'avèrent efficaces. En effet, les transactions exemptées qui transitent par 3-D Secure font ressortir un taux de fraude légèrement inférieur aux transactions avec authentification forte (0,06 %, contre 0,07 %), ce qui souligne que les exemptions prévues pointent bien les transactions les moins risquées.

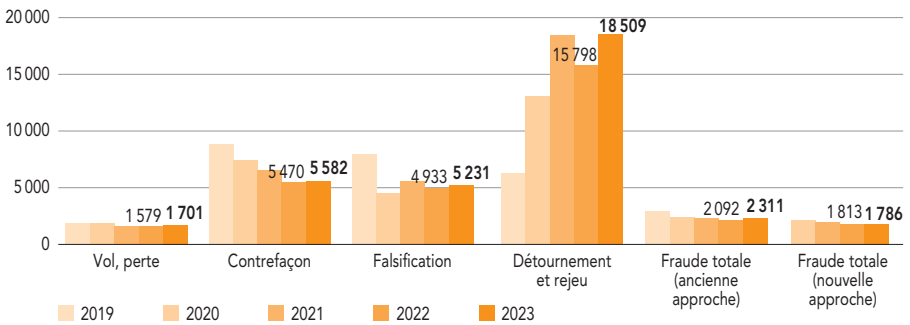
1.3 État de la fraude sur le chèque

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



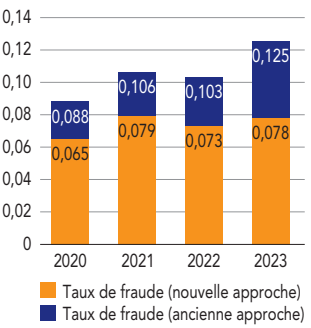
Source : Observatoire de la sécurité des moyens de paiement.

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 2023, le montant des opérations frauduleuses par chèque continue de fléchir pour s'établir à 364 millions d'euros (– 8 % par rapport à 2022). Cette régression tient en grande partie à la mise en place par les banques de mécanismes de prévention contre la fraude, conformément à la feuille de route de l'Observatoire. Elles ont notamment instauré des dispositifs de blocage ou de temporisation des remises de chèques qui ont permis de neutraliser 222 millions d'euros de remises frauduleuses (+ 38 % par rapport à 2022).

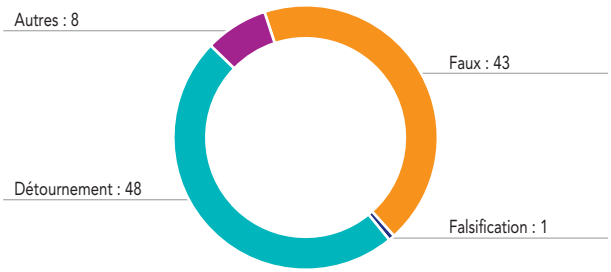
Néanmoins, compte tenu de la baisse encore plus accentuée des montants échangés par chèque (– 13,4 %), le taux de fraude sur le chèque marque un rebond pour atteindre 0,078 % en 2023, contre 0,073 % en 2022, après déduction de la fraude déjouée. Le principal type de fraude reste, de loin, l'utilisation de chèques perdus ou volés, en remise directe à l'encaissement par le fraudeur ou en règlement auprès de commerçants ou de particuliers (66 % des montants et 89 % des transactions frauduleuses).

Le montant moyen de la fraude au chèque augmente pour toute la typologie des fraudes. Il atteint 2 311 euros avant retraitement de la fraude déjouée. En revanche, lorsque les fraudes sont neutralisées après remise de chèques à l'encaissement (du fait d'une détection plus efficace par les banques des fraudes les plus élevées), ce montant moyen chute à 1 786 euros.

Bien que l'Observatoire ait relevé des progrès intéressants en 2023, à la suite des recommandations publiées en 2021, le chèque demeure le moyen de paiement qui affiche le taux de fraude le plus élevé, avec une tendance haussière en 2023 (+ 7 % par rapport à 2022).

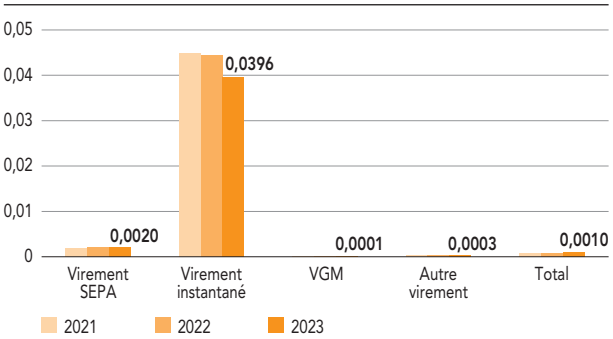
1.4 État de la fraude sur le virement

G26 Répartition de la fraude au virement en valeur par typologie de fraude en 2023 (en %)



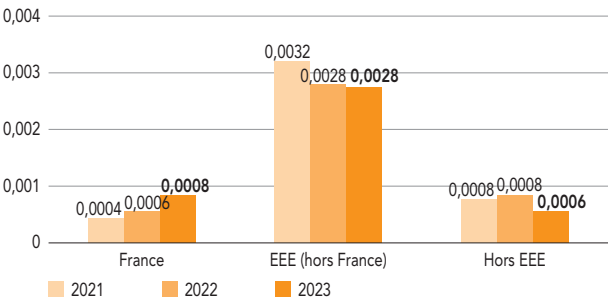
Source : Observatoire de la sécurité des moyens de paiement.

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



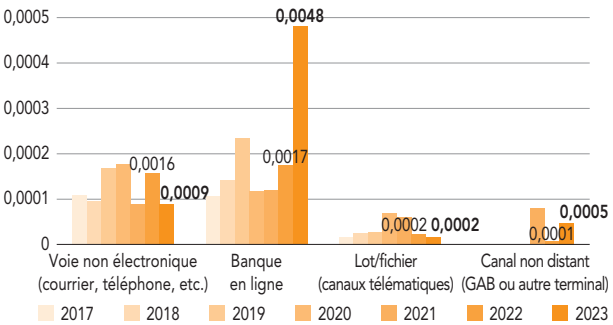
Note : SEPA, *Single Euro Payment Area* ; VGM, virement de gros montant.
Source : Observatoire de la sécurité des moyens de paiement.

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



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

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



Note : GAB, guichet automatique bancaire.
Source : Observatoire de la sécurité des moyens de paiement.

La valeur de la fraude au virement est globalement stable (– 0,5 %), passant de 313 millions d'euros en 2022 à 312 en 2023, alors que le volume des transactions frauduleuses s'accroît de 18 %. Par suite, le montant moyen de virement fraudé fléchit à 3 446 euros (contre 4 075 en 2022).

Le canal proportionnellement le plus fraudé reste celui de la banque en ligne, dont le taux de fraude progresse fortement pour atteindre 0,0048 % en 2023. Cette hausse de plus de 180 % procède de deux facteurs concomitants : d'une part, la forte montée de la fraude (+ 10 % en 2023 ; 237 millions d'euros, contre 216 en 2022, et 166 en 2021) et, d'autre part, une contraction substantielle du montant des virements (près de 60 % ; 5 milliards d'euros, contre 12 en 2022). Le second facteur est à relier à l'évolution des règles de gestion de trésorerie dans certaines grandes administrations.

À l'inverse, la nette amélioration observée en 2022 de la sécurité des virements initiés par les entreprises et les administrations par canaux télématiques se pérennise en 2023 : le taux de fraude est stabilisé à 0,0002 %, après 0,0006 % en 2021.

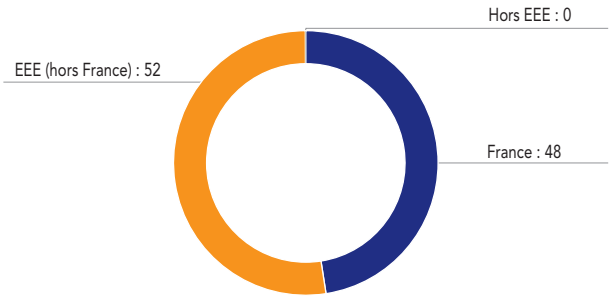
Les méthodes de fraude au virement continuent d'évoluer. Les fraudeurs recourent davantage aux comptes ouverts en France pour récupérer leurs fonds, même si les virements européens sont proportionnellement trois fois plus fraudés que les virements nationaux. Par ailleurs, ils mobilisent à la fois des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

L'évolution de la fraude en valeur sur le virement instantané reste maîtrisée au regard du développement de ce moyen de paiement : 31 % seulement de progression de la fraude en montant par rapport à 2022, pour des transactions en hausse de plus de 46 %. Par suite, le taux de fraude diminue sensiblement (– 11 % par rapport à 2022) et reste par exemple inférieur à celui de la carte (0,040 %, contre 0,053 %). Ces deux moyens de paiement sont pourtant majoritairement utilisés par les consommateurs et s'appuient sur des mécanismes de sécurité semblables (avec en particulier le recours aux mêmes dispositifs d'authentification forte du payeur pour les paiements en ligne).

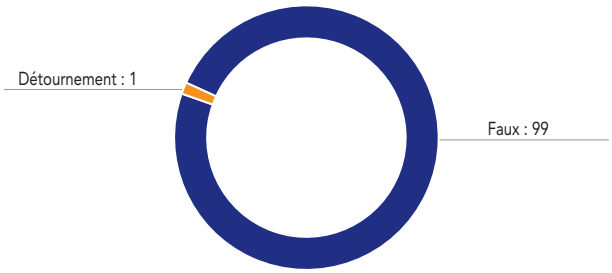
1.5 État de la fraude sur le prélèvement

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

a) Par zone géographique



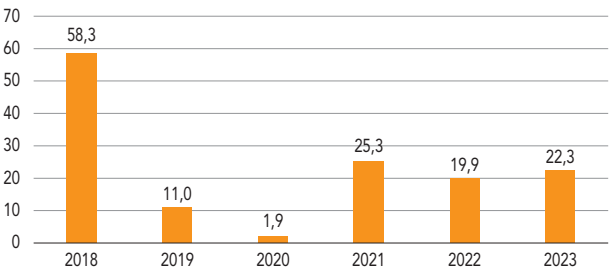
b) Par typologie de fraude



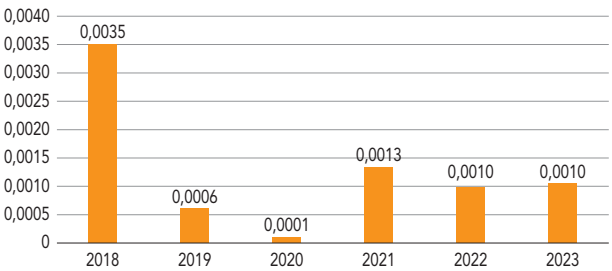
Note : EEE, Espace économique européen.
Source : Observatoire de la sécurité des moyens de paiement.

G31 Fraude au prélèvement

a) En valeur (en millions d'euros)



b) Taux (en %)



Source : Observatoire de la sécurité des moyens de paiement.

La fraude au prélèvement reste très volatile d'une année sur l'autre. En 2023, son montant augmente légèrement et atteint 22,3 millions d'euros (contre 20 en 2022) et son taux se stabilise à 0,0010 %. Elle émane presque exclusivement de créanciers fraudeurs, qui émettent de faux ordres, sans mandat de prélèvement ni relation économique avec la victime.

L'Observatoire relève toutefois deux évolutions notables par rapport à 2022 :

- d'une part, la fraude enregistrée par les établissements des créanciers touche exclusivement des comptes ouverts dans l'Espace économique européen, dont 48 % en France et 52 % hors France, alors qu'en 2022, 94 % de la fraude s'effectuait par l'intermédiaire de comptes ouverts en France ;
- d'autre part, la fraude par détournement, par lequel le fraudeur débiteur usurpe l'identité et le numéro de compte bancaire international (IBAN) d'un tiers pour signer un mandat de prélèvement, a fortement baissé en 2023, à 1 % des montants de fraude, contre 28 % en 2022.

ENCADRÉ

❶

Indicateurs, enseignements et préconisations des services du ministère de l'Intérieur sur la fraude aux moyens de paiement en 2023

Le ministère de l'Intérieur est représenté à l'Observatoire par l'Unité nationale cyber de la Gendarmerie nationale et la Direction nationale de la police judiciaire (DNPJ) de la Police nationale. Comme chaque année, ces deux services ont communiqué à l'Observatoire leurs principales observations sur les fraudes aux moyens de paiement constatées en 2023.

1. Étude statistique du ministère de l'Intérieur sur les escroqueries : un champ d'étude beaucoup plus large que celui de l'OSMP mais des enseignements convergents et complémentaires

En 2023, les publications statistiques du ministère de l'Intérieur ont fait l'objet d'une refonte méthodologique. La nouvelle méthode de suivi des infractions regroupe sans distinction les escroqueries et les fraudes aux moyens de paiement afin de préserver la cohérence des données. En effet, en raison de pratiques de codification différentes entre les services d'enregistrement, il est impossible d'isoler de manière précise les données de fraude aux moyens de paiement, telle qu'elle est définie par l'Observatoire de la sécurité des moyens de paiement (OSMP), parmi les escroqueries.

Le 10 juillet 2024, le Service statistique ministériel de la sécurité intérieure (SSMSI) a publié pour la première fois une étude spécifique sur les escroqueries enregistrées par les services de sécurité [1]. Cette étude, qui concerne la période allant de 2016 à 2023, décrit une augmentation constante des infractions de la famille des escroqueries enregistrées par les services de police et de gendarmerie nationales. Ces infractions incluent certaines fraudes aux moyens de paiement. En 2023, 411 700 victimes d'escroqueries et de fraudes aux moyens de paiement ont été enregistrées par les services de police et de gendarmerie nationales, soit une augmentation de 7,3 % par an depuis 2016 (soit + 64 % en sept ans) pour un préjudice global estimé à 4,5 milliards [2] d'euros en 2023 pour les personnes physiques [3].

La méthodologie d'enregistrement de la fraude aux moyens de paiement du SSMSI – qui est aujourd'hui agrégée systématiquement aux escroqueries – se distingue fortement de celle de l'Observatoire. En effet, en agrégeant les fraudes aux moyens de paiement aux escroqueries, la méthodologie du SSMSI retient un périmètre beaucoup plus large que celui de l'OSMP. En effet, le périmètre du SSMSI inclut toutes les escroqueries liées aux crédits et aux investissements, les fausses ventes sur internet, les escroqueries aux rançongiciels ainsi que les escroqueries à la romance, qui ne sont pas comptabilisées par l'OSMP comme des fraudes aux moyens de paiement. Par ailleurs, le SSMSI évalue le nombre de victimes enregistrées [4] à partir des dépôts de plainte alors que l'OSMP comptabilise les transactions frauduleuses déclarées par les prestataires de services de paiement et les réseaux de paiement par carte. Enfin, l'évaluation par le SSMSI du préjudice subi est issue du croisement des données enregistrées lors du dépôt de plainte et des données provenant des enquêtes de victimation [5]. L'OSMP s'appuie sur le montant précis des transactions frauduleuses déclarées par les établissements concernés. Ainsi, toutes ces différences de méthodologie et de périmètre empêchent le rapprochement direct des données publiées par le SSMSI et de celles publiées par l'Observatoire.

1 Service statistique ministériel de la sécurité intérieure (SSMSI), « Les escroqueries enregistrées par les services de sécurité entre 2016 et 2023 », *Interstats Analyse*, n° 68, juillet 2024.

2 L'estimation du préjudice subi par les personnes physiques victimes d'escroqueries et de fraudes aux moyens de paiement à 4,5 milliards d'euros comprend les infractions déclarées et les infractions non déclarées à la police et à la gendarmerie. Ces infractions non déclarées sont estimées par l'intermédiaire des enquêtes annuelles Cadre de vie et sécurité du ministère de l'Intérieur, appelées aussi enquêtes de « victimation ».

3 Dans son étude publiée le 10 juillet 2024, le SSMSI estime que le préjudice subi déclaré par les personnes morales victimes d'escroqueries et de fraudes aux moyens de paiement oscille entre 600 et 800 millions d'euros sur la période allant de 2016 à 2023.

4 D'après l'enquête Vécu et ressenti en matière de sécurité (VRS) de 2022 du SSMSI, environ une victime d'escroquerie sur dix porte plainte.

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

Toutefois, l'étude publiée par le SSMSI n'est pas contradictoire avec certaines évolutions de la fraude aux moyens de paiement constatées par l'Observatoire. Ainsi, **la fraude aux moyens de paiement repose de plus en plus sur la manipulation des victimes (par exemple, la fraude au faux conseiller bancaire, la fraude au président, ou encore la fraude aux coordonnées bancaires, etc.) et touche en nombre de faits davantage les personnes physiques que les personnes morales**. En effet, d'après l'étude du SSMSI, les personnes morales représentent 8,7 % des victimes en 2023, contre 16,1 % en 2016.

La publication du 10 juillet 2024 permet d'appréhender le profil des victimes personnes physiques. D'après l'étude, l**es jeunes adultes (25-34 ans) sont les victimes les plus représentées lors des dépôts de plainte**. Alors que cette tranche d'âge représente 11 % de l'ensemble de la population, elle constitue 17 % des victimes. Concernant le profil des escrocs mis en cause, il a très peu évolué depuis 2016 : 31 % des mis en cause appartiennent à la tranche d'âge 15-24 ans et 26 % à celles des 25-34 ans.

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

Depuis 2018, la plateforme Perceval de la gendarmerie permet de recueillir auprès des utilisateurs le signalement des usages frauduleux de cartes bancaires sur internet. Les enregistrements effectués sur cette plateforme peuvent être plus facilement rapprochés des tendances constatées par l'Observatoire. Elle fait état de 259 094 signalements en 2023 (contre 304 923 en 2022, soit une baisse de 15 %) pour un préjudice total de 155 millions d'euros (contre 161 millions d'euros en 2022, soit une baisse de 4 %), soit un préjudice moyen par signalement de 598 euros (contre 529 euros en 2022, + 12 %). Il convient de noter qu'un signalement sur la plateforme Perceval peut couvrir plusieurs transactions initiées frauduleusement à partir des mêmes données de carte usurpées.

Le taux de signalement des fraudes, rapproché des statistiques de l'Observatoire, ressort en baisse sur Perceval. En effet, 44 % de la fraude à la carte sur les paiements internet telle que quantifiée par l'Observatoire aurait été signalée sur Perceval en 2023, contre 51 % en 2022. Les victimes ont tendance à ne déclarer que les fraudes les plus importantes : en 2023, le montant moyen par transaction frauduleuse est de 64 euros d'après les statistiques de l'Observatoire contre 150 euros d'après Perceval (598 euros par signalement qui comprend en moyenne près de quatre transactions).

Une autre plateforme, appelée Thésée, ouverte en mars 2022 et gérée par l'Office anti-cybercriminalité (OFAC) de la Police nationale, permet aux particuliers victimes d'escroqueries en ligne de déposer plainte à distance [6]. En 2023, cette plateforme a recensé 59 500 dépôts de plaintes relatifs à une escroquerie ou une fraude aux moyens de paiement. Cela représente 14,5 % du total des victimes d'escroquerie ou de fraude aux moyens de paiement recensées par le SSMSI, taux en augmentation par rapport à 2022 (11,4 %).

L'Observatoire rappelle l'utilité des déclarations de fraude sur les deux plateformes Perceval et Thésée. Les forces de l'ordre peuvent ainsi recouper les informations nécessaires aux démantèlements des réseaux de fraudeurs.

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

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

La fraude par *skimmer* [7] consiste à récupérer, par le biais de terminaux de paiement trafiqués ou usurpés, les données bancaires stockées

6 La démarche en ligne sur la plateforme Thésée se substitue bien à un dépôt de plainte effectué en présentiel au commissariat de police ou en gendarmerie. Les données issues de Thésée sont intégrées au nombre de victimes d'escroquerie ou de fraude aux moyens de paiement publié par le SSMSI le 10 juillet 2024 dans son étude.

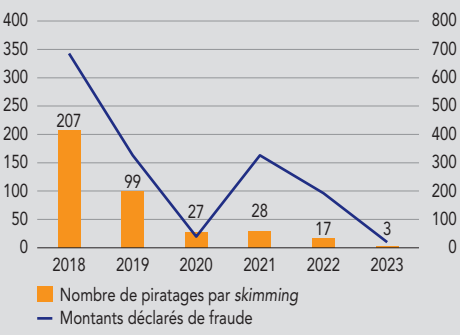
7 Matériel se glissant dans la fente d'un automate tout en laissant de l'espace pour qu'une carte bancaire puisse y être glissée naturellement. Une copie des données de la piste magnétique sera alors réalisée par le matériel sans que cela n'ait une quelconque implication sur le bon fonctionnement de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

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

Les chiffres du Groupement des cartes bancaires mettent en lumière une chute drastique des piratages par *skimming* sur ces dernières années (cf. graphique). Pour l'année 2023, seulement trois attaques ont été recensées pour un préjudice total de 19 563 euros (contre 192 540 euros en 2022, soit une baisse de 90 %). Ces trois attaques ont été commises sur des distributeurs automatiques de carburant (DAC), contre 17 en 2022. Aucune attaque n'a été recensée sur les distributeurs automatiques de billets (DAB), contrairement à 2022 où trois attaques avaient été dénombrées. Ces tendances sont cohérentes avec celles remontées par les acteurs des paiements à l'Observatoire.

Néanmoins, les gestionnaires de stations-essence comme les gestionnaires de DAB doivent rester vigilants pour prévenir les tentatives de substitution d'un terminal de paiement légitime par un terminal compromis ou toute installation par un tiers d'un dispositif externe frauduleux (lecteur, caméra, clavier, etc.).

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



Sources : Groupement des cartes bancaires.

La fraude au ***sh****imming*[8], qui repose sur des procédés similaires au ***sk****imming*, vise à récupérer les données contenues dans la puce de la carte. La complexité technique du dispositif limite encore les attaques. Le préjudice financier lié à ce type d'attaque est estimé à 36 000 euros en 2023, en baisse par rapport à 2022 (50 000 euros).

4. Les faux ordres de virement : globalement stables, mais restent un point de vigilance pour les administrations publiques

Les escroqueries aux « faux ordres de virement » (FOVI) sont caractérisées par les forces de l'ordre comme des arnaques financières consistant à obtenir de la victime un virement qu'elle pense légitime vers un compte bancaire géré par l'escroc. Procédant généralement par téléphone ou par courriel et usant de techniques d'ingénierie sociale, les escrocs exploitent les vulnérabilités humaines et organisationnelles de leurs cibles afin de leur faire réaliser des virements frauduleux. Ces escroqueries concernent en priorité les entreprises et les administrations publiques, mais les particuliers ne sont pas épargnés.

Les deux modes opératoires principaux sont :

- La fraude aux coordonnées bancaires (changement de RIB) : l'escroc usurpe l'identité d'un fournisseur de sa cible et prétexte auprès d'elle un changement de coordonnées bancaires aux fins de détourner le paiement des factures[9].
- La fraude au président : l'escroc usurpe l'identité d'un haut responsable de l'entreprise ou d'un de ses représentants (avocat, consultant, etc.) pour obtenir d'un collaborateur de l'entreprise cible la réalisation d'un virement à destination d'un nouveau compte. L'escroc insiste auprès de sa victime sur le caractère **confidentiel** et **urgent** de ce virement.

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

9 Les professions du chiffre et du droit sont également visées. Par exemple, dans le cas d'une étude notariale, l'escroc peut chercher à se substituer à l'étude devant recevoir d'un particulier le paiement de l'achat d'un bien immobilier, ou se substituer au particulier devant percevoir de la part de l'étude le produit de la vente.

La crise sanitaire de 2020 avait favorisé une forte recrudescence des cas de FOVI, du fait des situations d'urgence créées dans l'exécution d'un certain nombre de paiements et de la généralisation du télétravail. Le développement rapide de nouveaux modes de fonctionnement et d'organisation a permis à des acteurs malveillants l'exploitation de ces vulnérabilités nouvelles.

Depuis la fin de la crise sanitaire, **le nombre de faits commis se maintient à un niveau élevé alors que le préjudice global tend à diminuer**. Cette évolution s'explique par **la hausse du nombre de faits commis au préjudice des administrations publiques**, qui portent généralement sur des montants unitaires plus faibles.

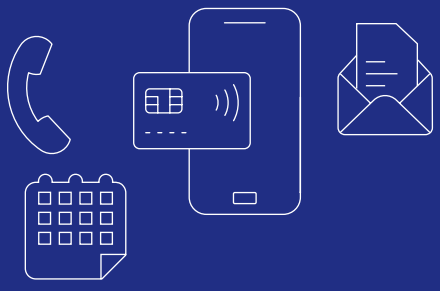
Ainsi, en 2023, pour les seuls FOVI à l'encontre des personnes morales, la direction nationale de la Police judiciaire (DNPJ) a été informée de 635 affaires pour un préjudice total de 48 millions d'euros, contre 537 affaires en 2022 pour un préjudice total de 68 millions d'euros [10].

Ces évolutions sont cohérentes avec les tendances générales remontées par les acteurs des paiements à l'Observatoire : la fraude au virement par détournement se stabilise en valeur (+ 1 %) alors qu'elle a tendance à augmenter en volume (+ 47 %).

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

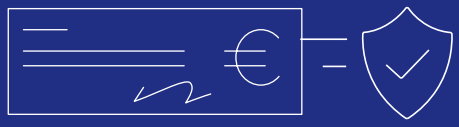
CHAPITRE 2
SYNTHÈSE DES ACTIONS CONDUITES PAR L'OBSERVATOIRE

Des **recommandations pour renforcer la sécurité des virements et des prélèvements,** en particulier de nouvelles actions de sensibilisation des utilisateurs et le développement de mécanismes de partage d'informations entre prestataires de services de paiement



La mise en place d'**un plan de lutte contre la fraude sur les paiements par carte à distance non sécurisés**, avec en particulier une limitation de l'acceptation des paiements par courrier, par téléphone ou des paiements récurrents ou fractionnés sans preuve d'authentification

Des travaux avec les opérateurs de téléphonie pour **lutter contre les usurpations à travers les réseaux de communication,** avec en particulier la préparation d'un mécanisme d'authentification du numéro d'appelant et la protection des identifiants des émetteurs de SMS



Des efforts demandés aux banques pour **renforcer la sécurité des envois de chéquiers et faciliter les mises en opposition**

2

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

2.1 Travaux sur la fraude aux paiements SEPA

2.1.1 Contexte

La lutte contre la fraude au virement et au prélèvement repose sur un ensemble d'actions intervenant à différents niveaux (mise en œuvre de solutions techniques, sensibilisation ou évolutions réglementaires) et à plusieurs étapes du parcours du paiement.

L'Observatoire de la sécurité des moyens de paiement propose, dans ce chapitre, un tour d'horizon des mesures et bonnes pratiques qu'il soutient et qui sont aujourd'hui mises en œuvre par les établissements financiers, les entreprises de tous secteurs, les associations, les administrations, les autorités et le grand public. Cet état des lieux aborde également les difficultés et limites auxquelles ces pratiques se heurtent, ainsi que les initiatives à venir (ou en cours d'étude) visant à compléter les dispositifs actuels, et conduisent l'Observatoire à formuler des recommandations pour renforcer la sécurité des virements et des prélèvements SEPA.

Rappel sur l'identification d'un compte bancaire

L'**IBAN** (*International Bank Account Number*) est un élément structurant des scénarios de fraude et des moyens pour les déjouer.

Il s'agit de l'identifiant international d'un compte bancaire auprès d'une institution financière dans un pays donné, qui est notamment utilisé dans le cadre de la réalisation de virements et prélèvements SEPA (*Single Euro Payment Area*, espace unique de paiement en euros), ou de transferts de fonds à l'international.

Il est constitué au maximum de 34 caractères alphanumériques, qui comprennent le code du pays où est tenu le compte, l'identification nationale du compte et une clé de contrôle.

Si le compte est détenu en France, il possède 27 caractères et commence par « FR ». Il est suivi d'une clé de contrôle, puis du code banque, du code guichet, du numéro de compte et de la clé RIB du compte français, tels qu'inscrits sur le relevé d'identité bancaire (RIB) :

2.1.2 Lutte contre la fraude au virement

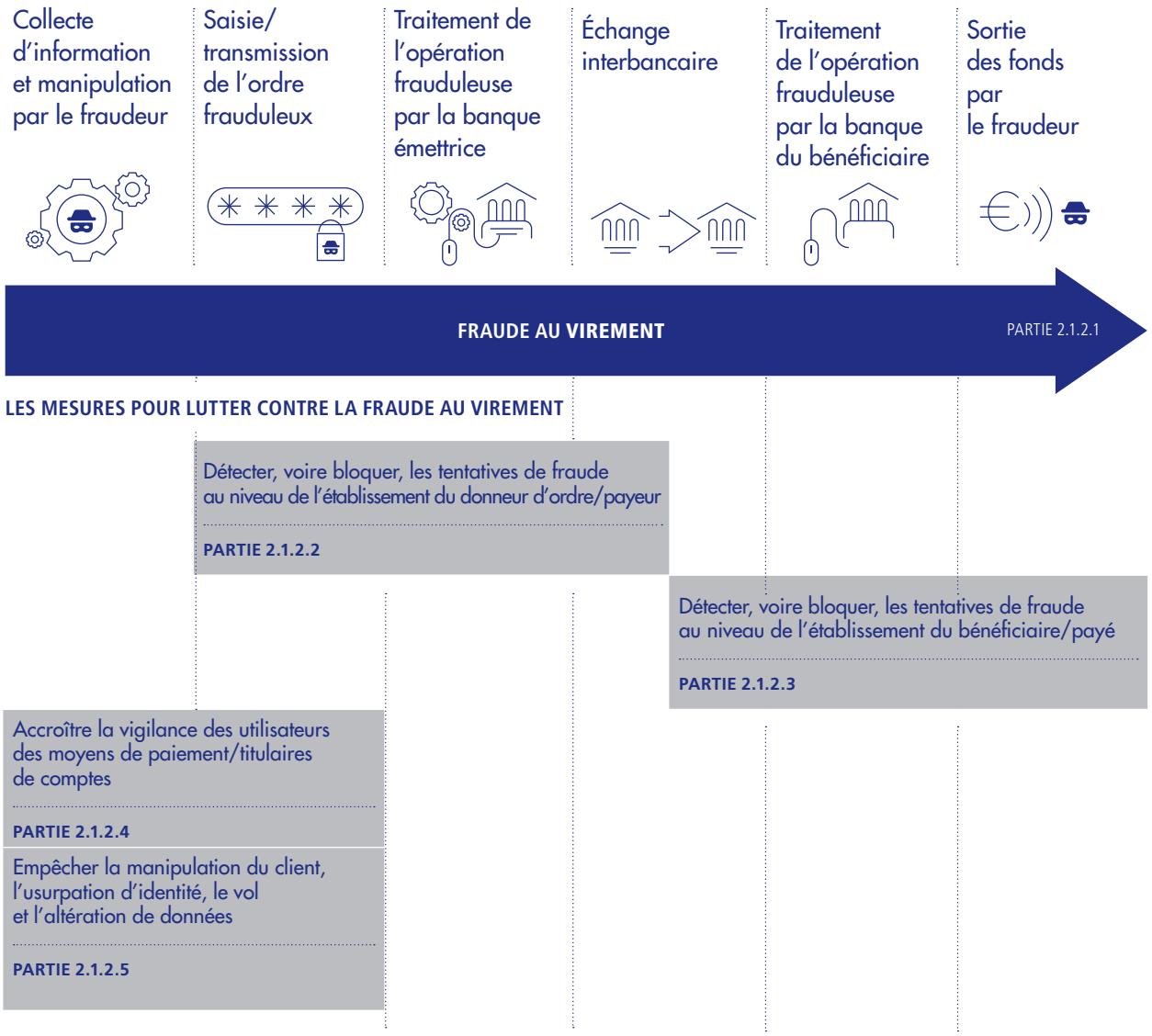
Les nouvelles tendances de fond dans l'évolution de l'usage du virement au sein du grand public, avec le développement du virement instantané soutenu par l'Eurosystème [1], constituent des défis dans le cadre de la lutte contre la fraude.

Le virement instantané, dont l'usage devrait s'accélérer dans le sillage du règlement européen qui lui est consacré [2], réduit le temps d'intervention possible pour l'émetteur. Ce mode de virement ne bénéficie pas, par nature, du délai d'exécution minimum d'un jour ouvré existant dans le cas d'un virement « classique », réduisant d'autant la possibilité de réagir lorsqu'une irrégularité est constatée. Et ce, non seulement pour l'utilisateur, mais aussi pour le prestataire de services de paiement (PSP) pour qui le temps alloué pour détecter une opération suspecte avant transmission vers le système de paiement est drastiquement réduit à quelques millisecondes.

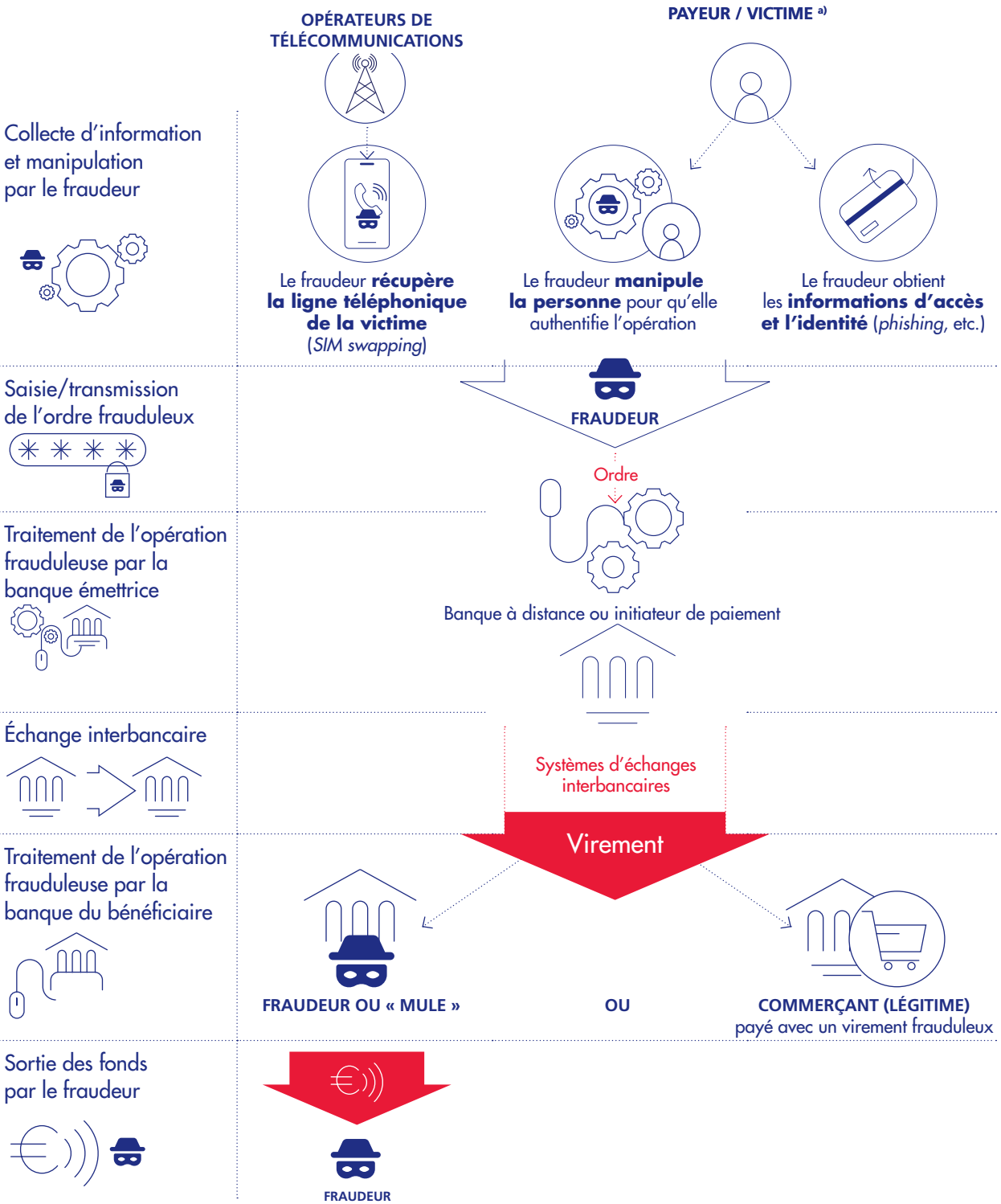
1 Stratégie de la Banque centrale européenne relative aux paiements de détail.

2 Règlement européen visant à rendre accessible à tous le paiement instantané en euros.

FRAUDE AU VIREMENT : COMMENT LUTTER ÉTAPE PAR ÉTAPE



MÉCANISME DE LA FRAUDE AU « FAUX VIREMENT »



a) Payeur/victime : peut être une personne physique ou une personne morale (entreprise, association, administration, etc.).
Note : Cette infographie n'illustre pas de manière exhaustive le déroulement d'une fraude au virement de type « faux ».

Cette problématique sera d'autant plus prégnante lorsque l'utilisation du virement instantané sera davantage répandue, y compris en point de vente (par exemple, avec le flash de QR code statique). Les fraudeurs pourraient ainsi employer des modes opératoires proches de ceux observés dans le cas de la fraude à la carte et au paiement mobile.

Enfin, l'écosystème global du virement est par nature complexe, compte tenu du nombre d'acteurs impliqués dans la chaîne des paiements (PSP teneurs de compte du payeur et du payé, prestataires d'initiation de paiement, sociétés de financement, etc.), et de l'ouverture géographique offerte par SEPA [3], en Europe et bientôt en dehors [4].

2.1.2.1 Les principaux modes opératoires de fraude au virement

■ **Cas de la saisie du virement par le fraudeur lui-même, qui aura réussi à obtenir les accès nécessaires (typologie « faux »)**

Dans cette typologie de fraude au virement, le fraudeur arrive à saisir **lui-même** un faux virement *(cf. infographie ci-contre).*

Le scénario le plus classique est le suivant :

- Le fraudeur usurpe l'accès à la banque à distance de sa victime :
  - en obtenant les identifiants et code secret par du *phishing* (faux site, imitant par exemple celui de la banque, transmis par courriel ou SMS qui permet au fraudeur d'obtenir de la part de la victime les identifiants nécessaires), du *squatting* publicitaire (fausses annonces usurpant les marques des banques poussées en tête des résultats des moteurs de recherche) ou des *malwares* (logiciels malveillants ayant infecté l'ordinateur, la tablette ou le téléphone du payeur afin de récupérer ses données sensibles) ;
  - en contournant l'authentification forte par manipulation de la victime à l'aide de techniques d'ingénierie sociale (par exemple, un appel usurpant le numéro d'un conseiller bancaire [*spoofing*]) afin qu'elle authentifie l'opération ;
  - en contournant l'authentification forte par détournement de la ligne téléphonique de la victime (par manipulation/exploitation des processus organisationnels ou techniques de l'opérateur téléphonique de la victime pour obtenir une copie de sa carte SIM [*SIM swapping*]), voire en arrivant à s'enrôler lui-même dans la solution d'authentification forte de la victime (après l'avoir manipulée).
- Le virement est émis par l'établissement PSP de la victime vers celui du bénéficiaire, à travers les systèmes d'échanges interbancaires.
- Le compte du bénéficiaire peut être domicilié en France ou dans un autre pays de la zone SEPA.
- Le compte peut avoir été ouvert par le fraudeur lui-même, sous une identité usurpée ou fictive, ou avoir été ouvert par une « mule », c'est-à-dire un tiers (individu ou société) rémunéré par le fraudeur pour le laisser utiliser ses coordonnées bancaires. Enfin, le fraudeur peut avoir utilisé le numéro de compte de toute entité commerciale légitime dans le but de payer un bien ou un service avec les fonds de la victime.
- Les fonds, s'ils n'ont pas été directement utilisés auprès d'une entité commerciale légitime, sont ensuite rapidement transférés vers un compte dans un autre établissement (parfois dans un pays hors zone SEPA), dans l'optique d'éviter toute récupération des fonds par le PSP de la victime.

■ **Cas de la saisie du virement par le client lui-même suite à une manipulation par le fraudeur (typologie « détournement »)**

Dans cette typologie de fraude au virement, la victime **initie l'ordre de paiement sous la contrainte ou la manipulation** du fraudeur, sans altération ni modification des attributs du virement par ce dernier *(cf. infographie page suivante).*

Le scénario le plus classique est le suivant :

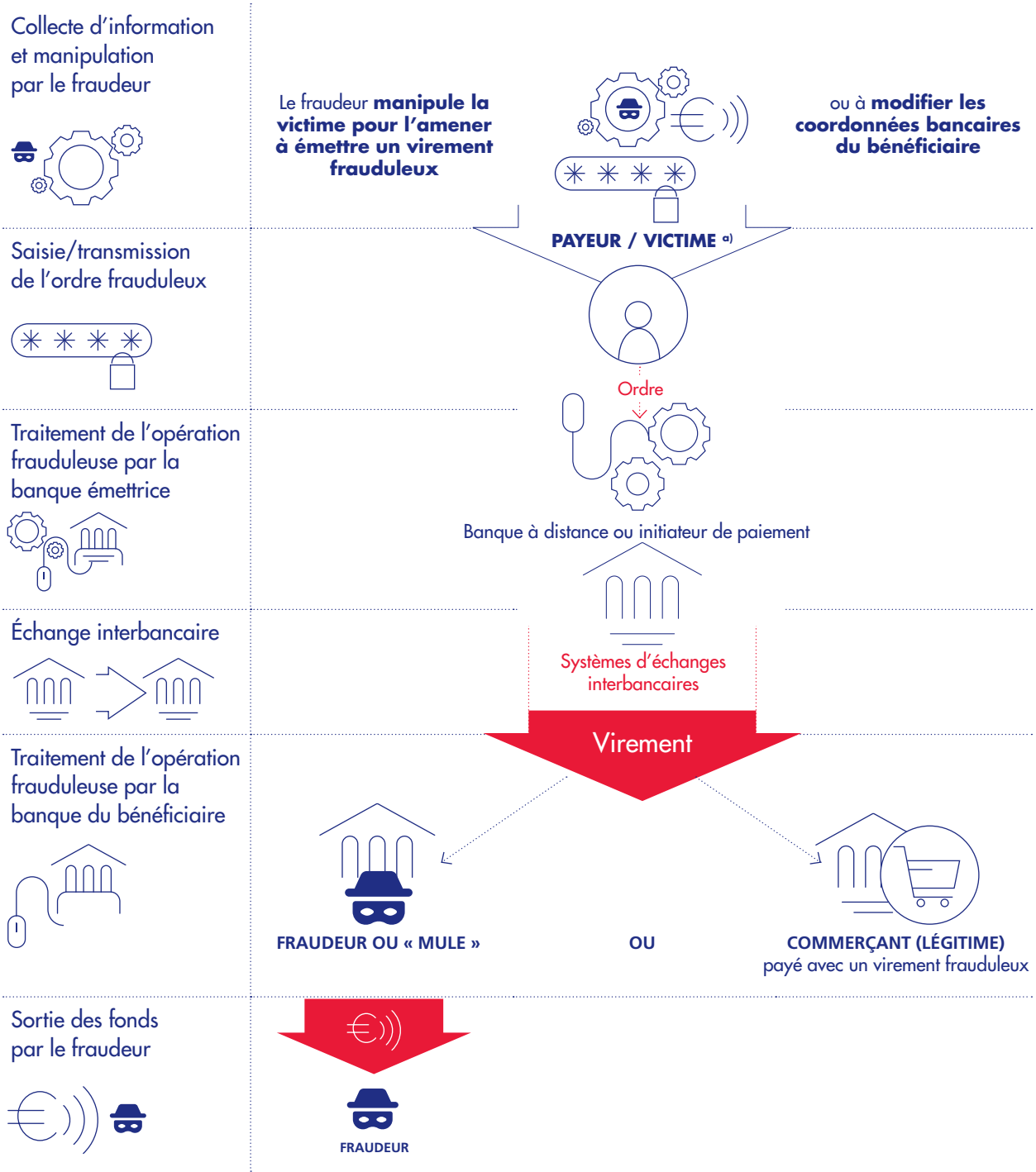
- Le fraudeur utilise des techniques d'ingénierie sociale dans l'optique d'inciter la victime à réaliser un virement en utilisant les coordonnées bancaires qu'il lui aura transmises :
  - en usurpant l'identité d'un artisan ou d'un fournisseur – dans le cas d'une entreprise – en relation avec la victime. Le RIB reçu par le payeur peut également avoir été modifié (par accès du fraudeur au courrier ou boîte mail) ;
  - en usurpant l'identité d'un supérieur hiérarchique (scénario appelé « fraude au président ») ;
  - d'autres scénarios, de plus en plus sophistiqués, font leur apparition (par exemple, QR code statique falsifié pour réaliser un paiement mobile par virement, imitation de la voix par logiciel de *deepvoice*, détournement de vidéo par logiciel de *deepfake* [5], etc.).

3 SEPA – *Single Euro Payment Area*, espace unique de paiement en euros qui vise à harmoniser les moyens de paiement entre ses membres.

4 *Scheme One-Leg Out Credit Transfer* du Conseil européen des paiements (*European Payment Council*) : règles et standards visant à faciliter l'interopérabilité des opérations de virements internationaux dont l'émetteur ou le récepteur est en zone SEPA.

5 Technique de synthèse audio ou vidéo reposant sur l'intelligence artificielle.

MÉCANISME DE LA FRAUDE AU « DÉTOURNEMENT DE VIREMENT »



a) Payeur/victime : peut être une personne physique ou une personne morale (entreprise, association, administration, etc.).
Note : Cette infographie n'illustre pas de manière exhaustive le déroulement d'une fraude au virement de type « faux ».

- Le virement est émis par l'établissement PSP de la victime vers celui du bénéficiaire, à travers les systèmes d'échanges interbancaires.
- Le compte peut avoir été ouvert par le fraudeur lui-même, sous une identité usurpée ou fictive, ou avoir été ouvert par une « mule », pour mémoire un tiers (individu ou société) rémunéré par le fraudeur pour le laisser utiliser ses coordonnées bancaires. Enfin le fraudeur peut avoir utilisé le numéro de compte de toute entité commerciale légitime dans le but de payer un bien ou un service avec les fonds de la victime.
- Les fonds, s'ils n'ont pas été directement utilisés auprès d'une entité commerciale légitime, sont ensuite rapidement transférés vers un compte dans un autre établissement (parfois dans un pays hors zone SEPA), pour éviter toute récupération des fonds par le PSP de la victime.

■ Autres typologies connues

La typologie « falsification » d'un ordre, actuellement minoritaire, qui consiste en l'interception et la modification d'un ordre de virement légitime (par exemple, par intrusion dans la base de données d'émission de virement de l'entreprise).

Le bénéficiaire d'un virement peut également être la cible d'une fraude, par exemple les marchands fraudés suite à un piratage de leur système d'information ayant permis la modification de leur IBAN ou du QR code utilisé par les acheteurs pour effectuer leurs paiements. Les fonds transférés par des acheteurs en paiement de leurs achats ne sont donc pas versés aux marchands légitimes, mais aux fraudeurs.

D'autres scénarios sont à noter compte tenu de leur ampleur actuelle, mais ne sont pas pour autant qualifiés de fraudes au virement à proprement parler :

- Usage du virement dans des scénarios d'escroquerie plus complexes. On peut par exemple citer :
  - La fraude au faux courtier : les consommateurs, titulaires de crédits à la consommation se font démarcher par un soi-disant « courtier spécialisé » qui leur promet d'obtenir une offre de rachat à un taux très attractif. Cette personne est en réalité en quête des données personnelles de l'emprunteur potentiel qu'il réutilisera ensuite pour souscrire un crédit auprès d'un autre établissement en son nom. Le consommateur se retrouve alors redevable d'un crédit supplémentaire alors même que ses anciens crédits ne sont pas remboursés, car le « faux courtier » a détourné les fonds à son profit.
  - L'arnaque aux faux placements : sous prétexte d'un placement financier très lucratif (par exemple, dans des cryptoactifs), la victime est incitée par le fraudeur à réaliser des virements.
- Arnaques au faux vendeur sur des sites de vente d'articles de seconde main avec paiement par virement instantané (en dehors des solutions de paiement embarquée sur le site).

2.1.2.2 Les mesures pour détecter, voire bloquer, les tentatives de fraude au niveau de l'établissement du donneur d'ordre/payeur

■ Panorama des mesures et bonnes pratiques existantes

L'authentification forte

Rendue obligatoire pour les PSP par la deuxième directive européenne sur les services de paiement (DSP 2) [6], l'authentification forte des utilisateurs s'est progressivement généralisée sur les sites et applications mobiles de banque à distance afin de sécuriser les étapes clés de la réalisation d'un virement. La combinaison d'au moins deux éléments d'authentification constitue un « garde-fou » contre l'intervention directe du fraudeur sur le compte du payeur : on peut la retrouver en particulier sur l'accès au compte, l'ajout d'un nouveau bénéficiaire et l'autorisation du virement.

Les éléments constituant l'authentification forte d'une personne sont généralement ses identifiants et code secret (éléments qu'elle est la seule à connaître – facteur de **connaissance**) et son mobile (élément qu'elle est la seule à posséder – facteur de **possession**), ou un facteur d'authentification propre à l'utilisateur (portant des caractéristiques propres à l'individu lorsque la vérification se fait par biométrie – facteur d'**inhérence**). Des procédures spécifiques existent également dans le cas de l'enrôlement d'un nouvel appareil servant lors de l'authentification.

Lorsqu'un virement est émis par le biais d'une solution d'initiation de paiement, celle-ci s'appuie sur le résultat de l'authentification réalisée au niveau du PSP teneur de compte de l'utilisateur. Ces solutions s'accompagnent parfois d'un mécanisme de vérification de son adresse e-mail.

6 Cf. article 97 sur l'authentification.

Bien que l'authentification forte réduise le risque d'usurpation de l'accès à la banque à distance, rendue plus difficile par le biais de l'indépendance des facteurs d'authentification, la persistance de la fraude au virement rappelle qu'elle ne constitue pas un rempart absolu. En effet, le développement des techniques d'ingénierie sociale a permis aux fraudeurs de contourner ces barrières techniques en manipulant directement l'utilisateur afin qu'il saisisse lui-même le virement frauduleux ou qu'il authentifie un virement saisi par le fraudeur. L'ingénierie sociale est également utilisée afin d'obtenir la ligne téléphonique du client par manipulation/exploitation des processus organisationnels et/ou techniques des opérateurs téléphoniques afin de s'approprier *in fine* les facteurs d'authentification du client, à son insu.

En outre, les mécanismes d'authentification les plus efficaces s'appuient sur l'utilisation de l'application mobile de l'établissement, or tous les clients ne sont pas équipés de *smartphones*, d'appareils compatibles avec l'application, voire ne souhaitent pas l'installer. Certains établissements proposent donc à leurs clients des boîtiers physiques, mais à défaut, l'authentification par envoi d'un code à usage unique par l'intermédiaire d'un SMS reste pratiquée, en complément de l'utilisation d'un code secret. Ce mode d'authentification présente malheureusement plusieurs défauts : SMS parfois pauvre en information sur le contexte de l'opération à authentifier, exposition plus forte au risque de vol de ligne téléphonique (*SIM swapping*), etc.

Bloquer ou temporiser l'émission d'un virement sur la base de critères

Afin d'empêcher l'émission d'un virement frauduleux depuis la banque à distance ou d'en limiter l'impact, les PSP s'appuient sur des critères prédéfinis qui permettront soit de bloquer, soit de temporiser l'émission du virement.

Le critère le plus communément utilisé est le plafond du montant fixé par la banque, adapté à la clientèle, en deçà du plafond maximal autorisé par SEPA. Certains critères sont décidés par le client lui-même. Il a en effet, dans certains établissements, la possibilité de désactiver le virement instantané afin d'empêcher l'exploitation de l'immédiateté du règlement dans le cas d'un accès par un fraudeur à son espace de banque à distance. Concernant la clientèle « entreprise », des règles supplémentaires sont parfois mises en place afin de, par exemple, limiter aux horaires d'ouverture des bureaux la plage horaire durant laquelle un virement peut être émis.

L'opportunité de « donner la main » au client sur un plus grand nombre de paramètres (plafonds, désactivation temporaire, horaires admis, etc.) est envisagée par certains établissements. Bien qu'elle ne permettrait pas de bloquer un fraudeur qui aurait réussi à contourner l'authentification forte pour modifier les paramètres à son avantage, cette fonctionnalité constituerait un niveau de protection supplémentaire pour le client, ajusté à ses usages.

Imposer des critères n'est pas non plus sans effet de bord. Par exemple, dans le cadre d'un usage légitime, le client peut chercher à éviter le dépassement du plafond en « découpant » son virement en plusieurs opérations de plus petits montants, ce qui a parfois pour effet de générer des alertes dans les outils de détection d'opérations suspectes *(cf. sous-partie ci-après)*, compte tenu de la similarité avec des techniques de fraude constatées.

Concernant la temporisation, elle existe de fait sur le virement classique, mais est interdite dans le cas des virements instantanés par les exigences réglementaires [7]. Elle est parfois encore appliquée par des PSP entre l'ajout d'un nouveau bénéficiaire et la saisie d'un virement. Mais cette pratique peut être perçue à contre-courant de la tendance du marché qui converge vers des paiements plus rapides et plus fluides.

Les outils de détection des opérations suspectes

Sous l'impulsion des paiements SEPA, les PSP ont tous mis en œuvre des outils permettant de détecter les opérations de virement suspectes et de générer des alertes. Ces outils appliquent un score à chaque opération en se fondant sur des règles basées sur l'expérience métier, l'analyse des données de connexion et de l'appareil utilisé.

C'est également un domaine d'application important pour l'intelligence artificielle (IA). Les établissements implémentent des moteurs de *machine learning* – dits « semi-supervisés » – dont le rôle est de déduire eux-mêmes les critères permettant de détecter une opération suspecte. L'intervention humaine afin de recalibrer les règles de détection et « réentraîner » les modèles d'IA sur la base de nouvelles données reste cependant indispensable et fréquente. Ces traitements devront par ailleurs être revus à travers le prisme de l'IA Act [8], adopté par l'Union européenne en 2024. L'IA n'a néanmoins pas remplacé les outils de *scoring* classiques basés sur des règles métier ; elle est généralement utilisée en complément.

La complexité de maintenance de ces outils réside dans le fait que l'évolution permanente des techniques de fraude est concomitante avec celle des usages légitimes des clients. Il s'agit donc d'un équilibre à trouver entre détecter le maximum de fraudes possible et minimiser la gêne du client en limitant les rejets à tort.

■ Évolutions à l'étude ou en projet

Le partage des données de fraude entre établissements

L'hypothèse a été envisagée par la communauté bancaire que les fraudeurs réutilisaient les mêmes numéros de compte dans leurs attaques envers plusieurs clients de PSP différents. Dans ce cadre, le partage de données entre PSP peut constituer un levier efficace de lutte contre la fraude.

Dans cette perspective, plusieurs initiatives ont été envisagées, voire mises en place. On peut tout d'abord citer le projet MISP [9] du Conseil européen des paiements (*European Payment Council*) – en cours – qui vise à donner la capacité aux PSP de la zone SEPA de collaborer en mettant en commun leurs données : les nouveaux schémas de fraude constatés jusqu'aux données d'identification des fraudeurs, avec parmi elles l'IBAN bénéficiaire utilisé.

Ces initiatives se heurtent toutefois aux droits nationaux qui empêchent le partage des données clients hors des frontières du pays, voire entre des établissements d'un même pays. Dans le cas de la France en particulier, le secret bancaire interdit aujourd'hui aux banques de se communiquer ces données entre elles. Dans d'autres pays européens, des dispositifs de partage uniquement locaux ont été mis en place.

La communauté bancaire française a néanmoins souhaité engager des travaux dans l'optique de mettre en œuvre un dispositif de partage de données, dont la Banque de France serait le tiers de confiance gestionnaire, et de faire évoluer la législation française au préalable.

Si ce dispositif se met en place, plusieurs points d'attention sont à relever pour en évaluer correctement la portée. Tout d'abord, les fraudeurs pourraient utiliser des numéros de compte bénéficiaire différents pour chaque fraude réalisée, rendant inefficace le croisement de ces IBAN avec une liste de comptes connus. L'usage d'IBAN « virtuels » [10] pourrait également faciliter cette pratique en masquant le « vrai » numéro de compte, derrière plusieurs IBAN virtuels créés *ad hoc* au sein de la banque du bénéficiaire fraudeur. Enfin, le référencement à tort de comptes pourrait être préjudiciable à leurs titulaires légitimes, ce qui implique une gestion rigoureuse de la base de comptes par l'ensemble des participants et la nécessité d'un processus de déréférencement efficace.

Détection des opérations suspectes au niveau des systèmes d'échanges interbancaires

Des systèmes interbancaires de paiement par lesquels transitent les virements SEPA sont en train de développer des services de *scoring* centralisés – sans blocage des opérations. Ces services seront utilisables par la communauté des banques participantes afin d'être alertées ou de compléter leur *scoring* interne. Les systèmes interbancaires pourront également être interrogés en amont de l'émission du virement.

2.1.2.3 Les mesures visant à détecter, voire bloquer, les tentatives de fraude au niveau de l'établissement du bénéficiaire/payé

La détection de la fraude du côté de la banque du bénéficiaire du virement est difficile sur la seule base de l'analyse d'une opération entrante. En outre, en l'absence d'indication claire permettant de déterminer l'usurpation d'identité ou le blanchiment de la part du client (du bénéficiaire de l'opération frauduleuse), refuser ou temporiser une imputation sur le compte du client en cas de simple suspicion d'activité frauduleuse est juridiquement risqué à réaliser pour le teneur de compte, qui peut s'exposer à des poursuites de la part de son client. Dans le cas du virement instantané, cela multiplierait les rejets sans certitude qu'il s'agisse de fraude avérée, puisqu'aucune temporisation n'est possible lors de l'arrivée des fonds.

Les établissements peuvent en revanche identifier l'activité frauduleuse d'un client lorsque celui-ci va tenter de sortir les fonds vers un autre compte, rentrant ainsi dans le périmètre des outils de surveillance des opérations émises. Cela passe notamment par l'implémentation de règles repérant les séquences anormales entre arrivée puis sortie de fonds sur un même compte.

7 Règlement européen (UE) 2024/886 du 13 mars 2024 visant à rendre accessible à tous le paiement instantané en euros, exigeant le crédit du compte du payé dans les dix secondes après réception de l'ordre par le PSP émetteur (article 1).

8 Règlement européen encadrant les usages de l'intelligence artificielle.

9 *Malware Information Sharing Platform* (plateforme de partage d'informations sur les logiciels malveillants), terme générique pour désigner les plateformes de partage de données de cybersécurité, ici spécialisées dans la fraude bancaire.

10 IBAN alternatif associé à celui du compte, utilisé pour réorienter les flux, faciliter le suivi et la réconciliation par le client.

Dans le contexte de l'initiation de paiement [11], les prestataires de services d'initiation de paiement (PISP, *Payment Initiation Service Providers*) mettent en œuvre une procédure de contrôle appelée par certains « *penny test* » visant à s'assurer de la validité des coordonnées bancaires du bénéficiaire – par exemple un marchand – avec lequel ils entrent en relation. Pour réaliser ce test, le PISP va émettre un virement d'un euro vers la banque tenant le compte indiqué par le bénéficiaire. Une fois le virement traité, une grande majorité des banques renvoie au PISP dans son message de confirmation le nom du titulaire du compte crédité. Le PISP pourra ainsi s'assurer de la bonne correspondance entre les informations fournies par le bénéficiaire (nom, raison sociale, etc.) et celles associées au numéro de compte fourni, avant de permettre l'initiation de paiements plus importants.

Néanmoins, les fraudeurs savent cibler les établissements offrant des facilités d'ouverture de comptes. Même pour un établissement appliquant des contrôles rigoureux lors de l'entrée en relation avec son client, les risques restent importants. Les moyens de vérification de l'identité de la personne reposent sur les pièces d'identité présentées, qui peuvent être falsifiées. Il est donc important que l'ouverture de comptes jugée risquée par le PSP s'accompagne de diligences complémentaires [12], notamment la justification de l'adresse du domicile, les activités professionnelles, les ressources et la provenance des fonds, et que les établissements s'assurent que les opérations sont cohérentes avec ces éléments. Les risques sont particulièrement élevés pour l'ouverture de comptes au bénéfice de personnes morales : dans ce cas le risque de fraude se rencontre lors de la création même de la personne morale (qui a pu avoir eu lieu à distance) et lors de l'ouverture de compte en son nom. Comparativement à une personne physique, les contrôles réalisés sont différenciés et plus propices à la falsification.

Même si les futurs moyens d'identification numérique basés sur le contrôle d'un certificat eIDAS [13] permettraient de sécuriser grandement ce processus (carte d'identité nationale électronique [14], le cachet électronique visible [15] associé, et leur pendant virtuel, l'identité numérique nationale [16] – en projet), ils ne seront toutefois pas obligatoires pour le client particulier, qui peut, par ailleurs, ouvrir un compte avec des documents d'identité étrangers. Dans le cas des « mules », les documents d'identité ne seront même pas falsifiés.

Le processus des retours de fonds en cas de fraude dans le contexte d'un virement SEPA est précisé dans l'encadré 2 situé en fin de chapitre.

2.1.2.4 Les mesures visant à accroître la vigilance des utilisateurs des moyens de paiement/ titulaires de comptes

Le rôle devenu prépondérant de l'ingénierie sociale dans la fraude remet le client au centre du dispositif de prévention. Sa vigilance est la première ligne de défense face aux attaques des fraudeurs qui le ciblent directement. Mais face à la sophistication des techniques de manipulation, le client doit pouvoir bénéficier d'une information claire et accessible proposée par les acteurs bancaires, voire d'outils concrets pour l'aider à se prémunir contre les tentatives de fraude.

■ **Panorama des mesures et bonnes pratiques existantes**

Les messages d'information à destination des clients lors du parcours de paiement

Lorsque le client s'apprête à finaliser la saisie d'un virement sur sa banque à distance puis à l'autoriser, il est normalement incité par son PSP à vérifier la légitimité de l'opération et la validité de son contenu.

De plus, l'OSMP recommande qu'à chaque étape d'authentification apparaissent de manière claire les informations relatives à l'opération, telles que le montant, le bénéficiaire, le caractère irrévocable de la validation, et la possibilité d'annuler l'opération.

Des messages de mise en garde peuvent également apparaître pour inviter le client à la vigilance avant une action sensible. Pour garder l'attention du client dans la durée et éviter que les messages d'avertissement soient trop rapidement validés par habitude, certains établissements font varier périodiquement le contenu. Ces initiatives n'éliminent hélas pas le risque de banalisation du message.

Les campagnes de sensibilisation du grand public

En relation avec le virement, les campagnes de mise en garde et de sensibilisation sur la fraude bancaire ont une importance cruciale. Elles sont en général axées sur la protection des données personnelles et d'authentification pour les usages de banque à distance, ainsi que sur la vigilance vis-à-vis des techniques de manipulation.

L'efficacité de ces actions, en particulier leur capacité à sensibiliser les populations les plus exposées à la fraude, requiert l'utilisation de tous les canaux de diffusion à disposition, des plus traditionnels (télévision, presse, etc.) aux plus récents (réseaux sociaux), en faisant preuve d'une grande pédagogie *(cf. encadré 3)*.

Comme l'ensemble des moyens de lutte contre la fraude, la communication préventive doit continuellement s'adapter au perfectionnement des attaques par ingénierie sociale qui continuent de déjouer la vigilance du public, et à l'émergence de nouveaux scénarios de fraude exploitant les évolutions technologiques (croissance du paiement mobile, intelligence artificielle pour usurper la voix et l'image, etc.).

La sensibilisation en entreprise

Pour se protéger contre les scénarios de fraude spécifiques aux entreprises (falsification d'ordre, fraude au président ou au faux fournisseur, etc.), les entreprises peuvent mener des actions de communication ou de formation auprès de leurs employés, souvent dans le cadre plus large de la cybersécurité. Ce besoin s'est fait d'autant plus sentir avec les cas d'attaques exploitant les situations d'isolement du personnel à distance depuis la crise de la Covid.

Les actions de communication et de formation s'accompagnent également de tests sur la vigilance du personnel (par exemple, les campagnes de test « *phishing* »).

Les commerçants, en tant que bénéficiaires de paiement, font également l'objet d'actions de communications ciblées par leurs PSP, compte tenu de leur exposition à certains scénarios de fraude (par exemple, préconisation de ne pas envoyer de marchandises avant d'avoir reçu les fonds, qui ont pu être détournés par les fraudeurs suite à un piratage de leur système d'information).

Contrôle de cohérence entre l'IBAN et le nom du bénéficiaire (situation actuelle)

Plusieurs solutions existent sur le marché pour permettre au client de contrôler que l'identifiant d'un compte fourni par un tiers correspond bien à son nom ou à son immatriculation dans le cas d'une personne morale. Ces outils sont actuellement utilisés dans le monde de l'entreprise. Ils contribuent notamment à lutter contre les fraudes au faux fournisseur (le fraudeur usurpe l'identité d'un fournisseur et transmet ses propres coordonnées bancaires), en incitant l'utilisateur à vérifier par contre-appel l'identifiant du compte fourni, en cas de résultat négatif du contrôle de cohérence.

Le principe de fonctionnement varie selon l'offre : un réseau de banques participantes qui contribuent aux vérifications par l'intermédiaire de leurs propres bases de données clients, une communauté d'entreprises qui partagent ses informations fournisseurs, l'analyse d'un historique d'opérations pour détecter une incohérence entre un IBAN et un nom de bénéficiaire déjà connu. Le périmètre de comptes couvert est principalement le territoire français, bien que des partenariats permettent dans de rares cas de l'étendre à d'autres pays.

Concernant les opérations de virement réalisées par le grand public, ce contrôle est aujourd'hui très rarement effectué par le PSP. L'OSMP recommande donc que cette absence de contrôle soit explicitement mentionnée lors de l'ajout d'un nouveau bénéficiaire ou l'autorisation d'un virement.

■ Évolutions à l'étude ou en projet

Généralisation du contrôle de cohérence entre l'IBAN et le nom du bénéficiaire

Le règlement européen sur le virement instantané va exiger des PSP la mise à disposition systématique pour le client de ce contrôle de cohérence lors de l'ajout d'un bénéficiaire ou lors de la saisie du virement (instantané ou classique). Le service aura par ailleurs une portée européenne puisqu'un « *scheme* » [17] va définir les règles d'harmonisation et de mise en relation des différents systèmes domestiques, et ainsi tenter de limiter les tentatives de fraude utilisant des comptes domiciliés dans un pays de la zone SEPA.

L'efficacité du dispositif dépendra néanmoins du choix du client de l'utiliser avant de réaliser un virement, puis de la décision qu'il prendra de confirmer ou non son ordre de virement en cas de réponse défavorable.

11 Service qui permet à toute personne (particulier ou entreprise) d'ordonner un virement direct de compte à compte à partir d'un site internet, d'une application mobile ou d'un logiciel de gestion. Les prestataires de service d'initiation de paiement (PISP) sont les acteurs intermédiaires offrant ce service, par exemple, à des commerçants souhaitant offrir cette possibilité aux acheteurs.

12 Arrêté du 2 septembre 2009 pris en application de l'article R. 561-12 du Code monétaire et financier et définissant des éléments d'information liés à la connaissance du client et de la relation d'affaires aux fins d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme.

13 eIDAS est le règlement de l'Union européenne sur l'identification électronique et les services de confiance pour les transactions électroniques, qui définit notamment les normes européennes pour les certificats électroniques utilisés dans les mécanismes d'authentification ou les signatures électroniques.

14 Format de carte d'identité équipée d'une puce contenant un certificat électronique eIDAS.

15 Code en deux dimensions, non falsifiable, apposé sur un document contenant les informations permettant de garantir son origine et son intégrité (par exemple, l'état civil d'une personne).

16 Solution d'identification numérique mise en œuvre par l'État français, s'appuyant sur le téléphone mobile, pour faciliter l'identification dans le cadre de services en ligne.

17 Ensemble de règles sur lesquelles s'accordent les participants d'un système (de paiement, de messagerie, etc.).

2.1.2.5 Les mesures pour empêcher la manipulation du client, l'usurpation d'identité, le vol et l'altération de données

Les moyens de télécommunication et internet sont les outils de prédilection du fraudeur, pour obtenir les données personnelles ou d'authentification de la victime, ou entrer directement en contact avec elle.

■ **Panorama des mesures et bonnes pratiques existantes**

La fermeture de sites et le filtrage des e-mails et SMS de *phishing*

Une première méthode afin d'empêcher le fraudeur d'atteindre le client est de supprimer ses moyens d'accroche dès qu'ils sont identifiés.

Les courriers électroniques indésirables contenant de faux sites web, copiant ou non des sites légitimes, peuvent être déclarés sur des plateformes telles que Signal Spam. De même, le service Phishing Initiative mis à disposition par un opérateur de téléphonie permet de vérifier si un site a déjà fait l'objet d'un signalement pour *phishing*, et à défaut de le signaler.

Une veille est par ailleurs réalisée par les entreprises ou entités publiques dont les sites sont souvent falsifiés pour tromper leurs clients ou usagers. Une fois la déclaration instruite, des démarches sont faites auprès des fournisseurs de service internet concernés pour tenter de faire fermer les sites en question.

Les faux SMS affichant des noms d'entités légitimes ou des numéros d'apparence régulière peuvent être retransmis au numéro de téléphone 33700 pour traitement par les opérateurs concernés. Des outils de filtrage existent chez ces derniers, basés sur des listes de noms d'émetteurs à bloquer, mais ils ne peuvent cependant pas analyser le contenu du SMS lui-même pour des raisons de protection de la vie privée, sauf s'il est déclaré comme suspect par un abonné.

Par ailleurs, pour répondre à la multiplicité des plateformes de déclaration permettant au grand public de déclarer un site, un e-mail ou un SMS suspect, le site Cybermalveillance.gouv.fr aide l'utilisateur à se diriger vers le bon service, par l'intermédiaire d'un diagnostic en ligne *(cf. encadré 4)*.

Malgré les actions mises en œuvre par les acteurs publics et privés dans cette course permanente pour éliminer sites et SMS malveillants, l'efficacité de l'identification dépend beaucoup de la diligence des personnes ciblées, face au très grand nombre d'attaques qu'elles sont incitées à déclarer.

Les services de vérification des cartes SIM ou des données sur l'abonné au service de téléphonie

Pour identifier l'usurpation de ligne téléphonique par le fraudeur lorsque celui-ci tente de réaliser son opération avec son propre mobile, des opérateurs de téléphonie proposent désormais deux services de contrôle, interrogeables par les PSP ou les commerçants.

Le service SIM Verify permet de vérifier, lors d'une authentification, l'ancienneté de la carte SIM utilisée. On peut ainsi détecter les suspicions de cartes issues d'attaques par *SIM swapping*, généralement activées de manière récente.

Le service matchID fournit quant à lui le moyen d'interroger la base de données de l'opérateur afin de croiser les données de l'abonné téléphonique avec celles du client de la banque, et ainsi repérer les éventuelles incohérences.

La sécurisation des environnements informatiques du particulier et de l'entreprise

Outre l'usage du *phishing* pour collecter les informations dont ils ont besoin, les fraudeurs bénéficient également des fuites de données issues des *malwares* installés sur les ordinateurs individuels, ou du piratage des systèmes d'information des entreprises auxquelles les personnes ont pu confier leurs données (par exemple, les sites de e-commerce ou de fournisseurs de services).

Pour bloquer à la source ces fuites de données, les postes de travail doivent être suffisamment sécurisés (antivirus, accès internet utilisé, etc.).

Il en est de même pour les entreprises et administrations stockant les données personnelles ou de paiements de leurs clients/usagers : les sites accessibles depuis internet doivent être correctement sécurisés (authentification, chiffrement des flux, etc.), et le système d'information interne doit se prémunir contre le piratage externe et la fraude interne (robustesse de la gestion de l'accès et des droits, chiffrement des bases de données, outils de filtrage réseau et de détection, procédures de contrôle, etc.). Dans le cas des entreprises amenées à transmettre des ordres de virement à leurs PSP, il s'agit également de se protéger contre les risques d'une altération des ordres dans leur système d'information (par exemple, modification de l'IBAN bénéficiaire d'un paiement à émettre).

La signature électronique pour empêcher la falsification de document

La signature électronique, normalisée par le règlement eIDAS de l'Union européenne, accompagne progressivement la

dématérialisation des échanges entre entreprises ou entre entreprises et particuliers. La norme eIDAS doit permettre à la fois de s'assurer de l'identité du signataire et de l'intégrité du document depuis sa signature. Plusieurs niveaux de sécurisation de la signature existent, donnant une garantie plus ou moins forte de l'identité du signataire. Pour les actes les plus courants et comportant le moins de risque, l'acte de signature peut prendre la forme d'une fonctionnalité de site web interagissant avec le signataire renforcée par un code à saisir transmis par SMS ou e-mail.

Le niveau supérieur de signature électronique s'appuie, lui, sur des certificats électroniques, délivrés par un tiers de confiance, garantissant l'identité du signataire à travers un processus d'enrôlement. Dans le cadre de la lutte contre la fraude, ce type de signature peut, par exemple, confirmer l'identité de la personne qui transmet ses coordonnées bancaires dans le cadre du paiement d'une facture.

La signature électronique avec certificat est de plus en plus fréquente dans le domaine professionnel. Elle est pour le moment beaucoup moins répandue au sein du grand public, mais cela devrait évoluer avec la généralisation de la carte d'identité nationale électronique, dont la puce contient justement un certificat.

■ Évolutions à l'étude ou en projet

Lutte contre l'usurpation de numéro dans le cadre des fraudes par téléphone (*spoofing*)

La loi Naegelen [18], entrée en vigueur en 2023, prévoit la mise en place d'un dispositif d'authentification à destination des opérateurs qui permettra d'empêcher la réutilisation illicite d'un numéro légitime dans le but de l'afficher à l'utilisateur. Cette technique est en effet exploitée par les fraudeurs afin de se faire passer pour un interlocuteur de confiance auprès de la victime (par exemple, faux conseiller bancaire).

2.1.3 Lutte contre la fraude au prélèvement

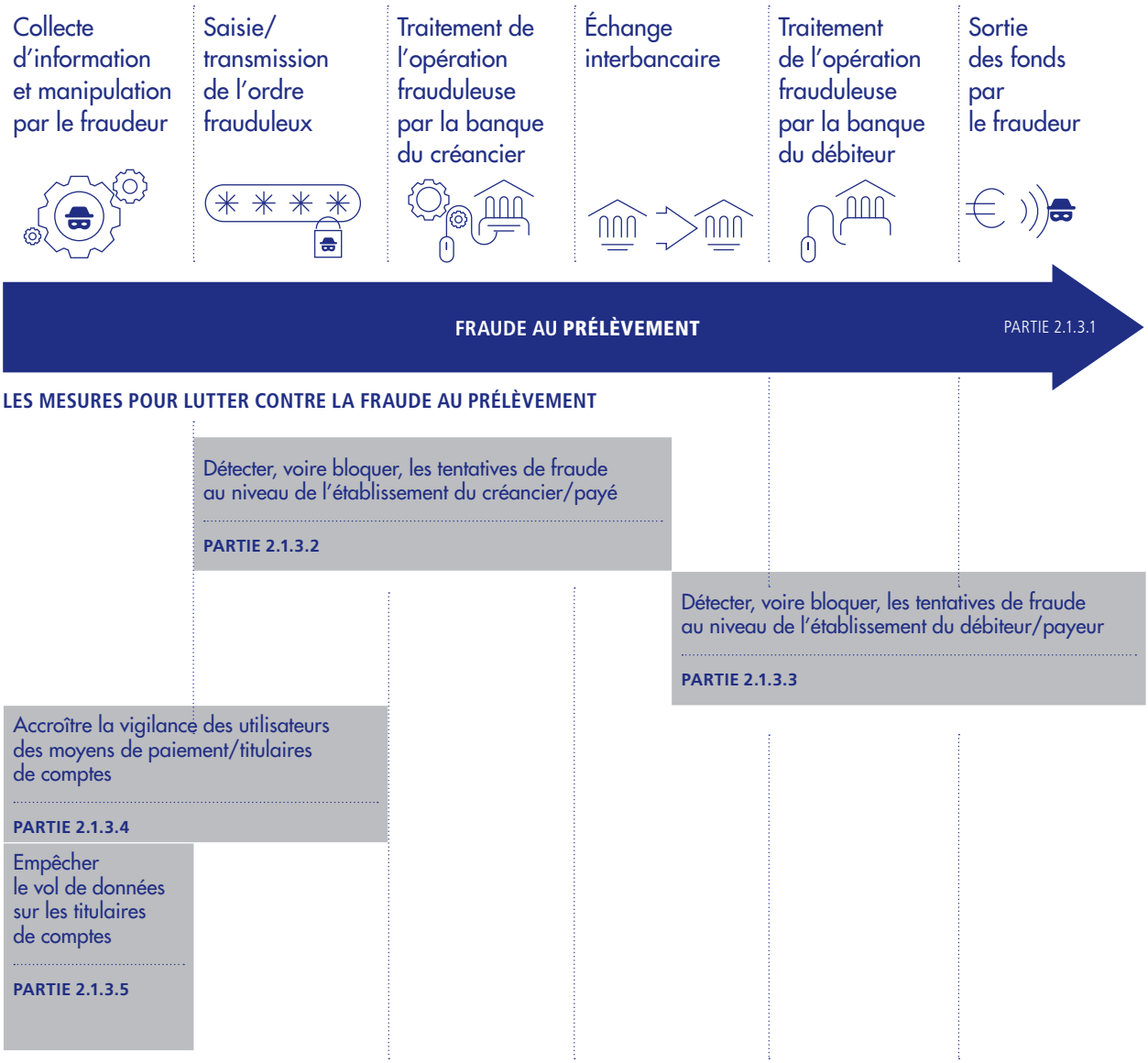
À propos du fonctionnement du prélèvement SEPA [1]

- Le prélèvement est une opération de paiement par laquelle un créancier (le payé) ordonne, à travers le système bancaire, le transfert direct d'une somme depuis le compte bancaire d'un débiteur (le payeur) qui lui aura au préalable donné son consentement, matérialisé par la signature d'un mandat.
- Afin de s'assurer qu'un créancier est habilité à réaliser un prélèvement, il doit demander via son établissement teneur de compte un identifiant appelé ICS (identifiant créancier SEPA), utilisable dans l'ensemble des pays de la zone SEPA. Dans de nombreux pays, cet identifiant est émis et géré par un tiers gestionnaire au niveau national : en France, c'est le rôle de la Banque de France. Un créancier peut en outre être radié en cas de non-respect grave de la réglementation en matière de prélèvements SEPA (*SEPA direct debit* – SDD), notamment en cas de fraude.
- Il y a deux types de prélèvements SEPA (SDD) : le prélèvement standard (*SDD Core*) et le prélèvement interentreprises (*SDD business to business* – B2B). Dans le cas du SDD B2B où le débiteur est en principe une personne morale, le mandat est obligatoirement fourni à la banque du débiteur et systématiquement contrôlé, il est donc peu exposé à la fraude. Dans le cas du *SDD Core*, le mandat n'est en revanche pas connu de la banque du débiteur, qui n'a pas l'obligation de contrôler le mandat signé par son client ni de le transmettre à celle du créancier. Les scénarios de fraude et mesures décrites dans cette section portent donc essentiellement sur les *SDD Core*.
- Dans le cas du *SDD Core*, le débiteur dispose d'un délai de huit semaines pour contester un prélèvement, quel que soit le motif, puis treize mois pour un prélèvement pour lequel il n'a pas donné son consentement (mandat inexistant, révoqué ou caduc) ou dont l'un des principaux éléments est erroné.

1 Cf. règles (*Rulebook*) du *scheme SEPA direct debit* du Conseil européen des paiements (*European Payment Council*).

18 Loi n° 2020-901 du 24 juillet 2020 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux. Précisément, l'article L44-IV du Code des Postes et Communications électroniques.

FRAUDE AU PRÉLÈVEMENT : COMMENT LUTTER ÉTAPE PAR ÉTAPE



2.1.3.1 Les principaux modes opératoires de fraude au prélèvement

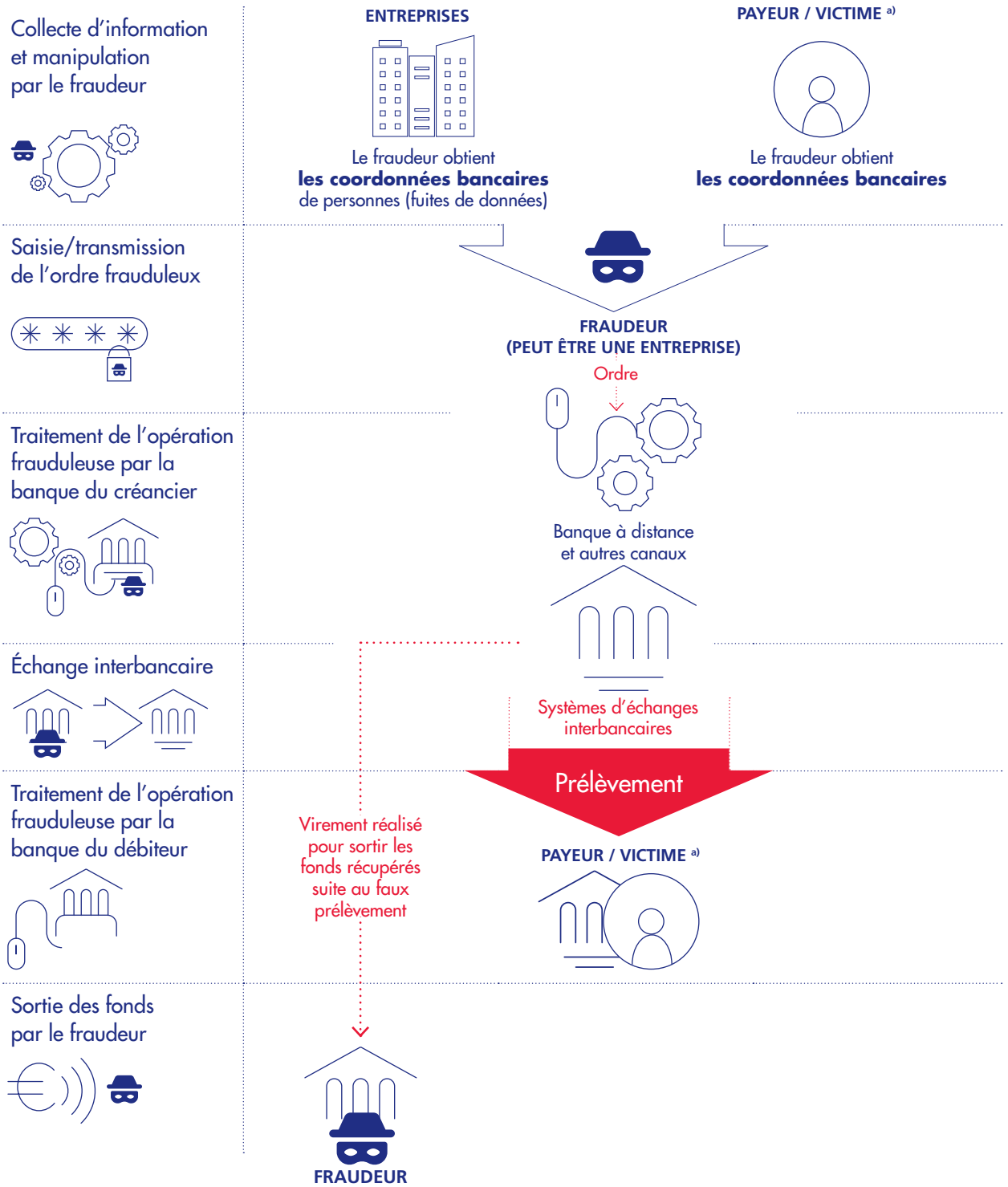
■ Cas de l'émission d'un prélèvement par un créancier fraudeur (typologie « faux »)

Dans cette typologie de fraude au prélèvement, le fraudeur créancier émet des prélèvements vers **des numéros de compte qu'il a obtenus illégalement et sans aucune autorisation**.

Le scénario classique est le suivant *(cf. infographie ci-contre)* :

- Le fraudeur obtient les coordonnées bancaires de la victime (personne physique ou morale) pour saisir un ordre de prélèvement :
  – en achetant une liste d'IBAN ayant, par exemple, été volée dans le système d'information d'une entreprise lors d'un piratage (comptes de salariés, clients ou fournisseurs) ;

MÉCANISME DE LA FRAUDE AU « FAUX PRÉLÈVEMENT »



a) Payeur/victime : peut être une personne physique ou une personne morale (entreprise, association, administration, etc.).
Note : Cette infographie n'illustre pas de manière exhaustive le déroulement d'une fraude au prélèvement de type « faux ».

– en prenant le contrôle d'une société ayant une base de données clients débiteurs préexistants.

- Le prélèvement est émis par le PSP du créancier vers celui du débiteur, à travers les systèmes d'échanges interbancaires. Une référence unique du mandat (RUM) est renseignée dans l'ordre, mais aucune copie du mandat ne transite avec l'ordre.
- Le compte bénéficiaire peut avoir été ouvert par le fraudeur lui-même, sous une identité usurpée ou fictive, ou avoir été ouvert par une « mule », c'est-à-dire un tiers (individu ou société sans réel objet et détenue par un individu « prête-nom ») rémunéré par le fraudeur pour le laisser utiliser ses coordonnées bancaires.
- Une fois les sommes prélevées et imputées sur le compte frauduleux, les fonds sont ensuite rapidement transférés vers un compte dans un autre établissement (parfois dans un pays hors zone SEPA) pour faire obstacle, après remboursement des débiteurs, aux tentatives de récupération des fonds par les PSP du créancier et, le cas échéant, par celui du débiteur.

■ Cas de souscription d'un mandat de prélèvement avec le compte d'un tiers (typologie « détournement »)

Dans cette typologie de fraude, le fraudeur souscrit à un service auprès d'un créancier légitime, mais **renseigne les coordonnées bancaires du compte de la victime à la place des siennes** pour qu'y soient prélevées les sommes facturées *(cf. infographie ci-contre)*.

■ Autres typologies connues

- L'entente frauduleuse entre créancier et débiteur :
  – Dans ce scénario, un créancier fraudeur émet des prélèvements sur un compte détenu par un débiteur complice de façon régulière et en augmentant progressivement les montants.
  – Un peu avant la fin de la période de rétraction légale (de treize mois après le paiement du prélèvement), le débiteur conteste les prélèvements qui ont été débités sur son compte, au motif qu'il n'a pas signé de mandat de prélèvement correspondant.
  – Au moment des rejets des prélèvements, le solde du compte du créancier fraudeur ne permet plus le remboursement des opérations contestées, car les fonds ont été transférés vers un compte tenu à l'étranger.
- Cas d'arnaque, non considérés comme fraude au paiement à proprement parler, dans lesquels des prélèvements sont réalisés sans respect des conditions prévues par le mandat, ou lorsqu'un mandat a été révoqué ou caduc.

2.1.3.2 Les mesures visant à détecter, voire bloquer, les tentatives de fraude au niveau de l'établissement du créancier/payé

■ Panorama des mesures et bonnes pratiques existantes

Surveillance des opérations

Malgré les moyens mis en œuvre, les PSP des créanciers éprouvent des difficultés à détecter la fraude lors de l'émission de l'opération par leur client.

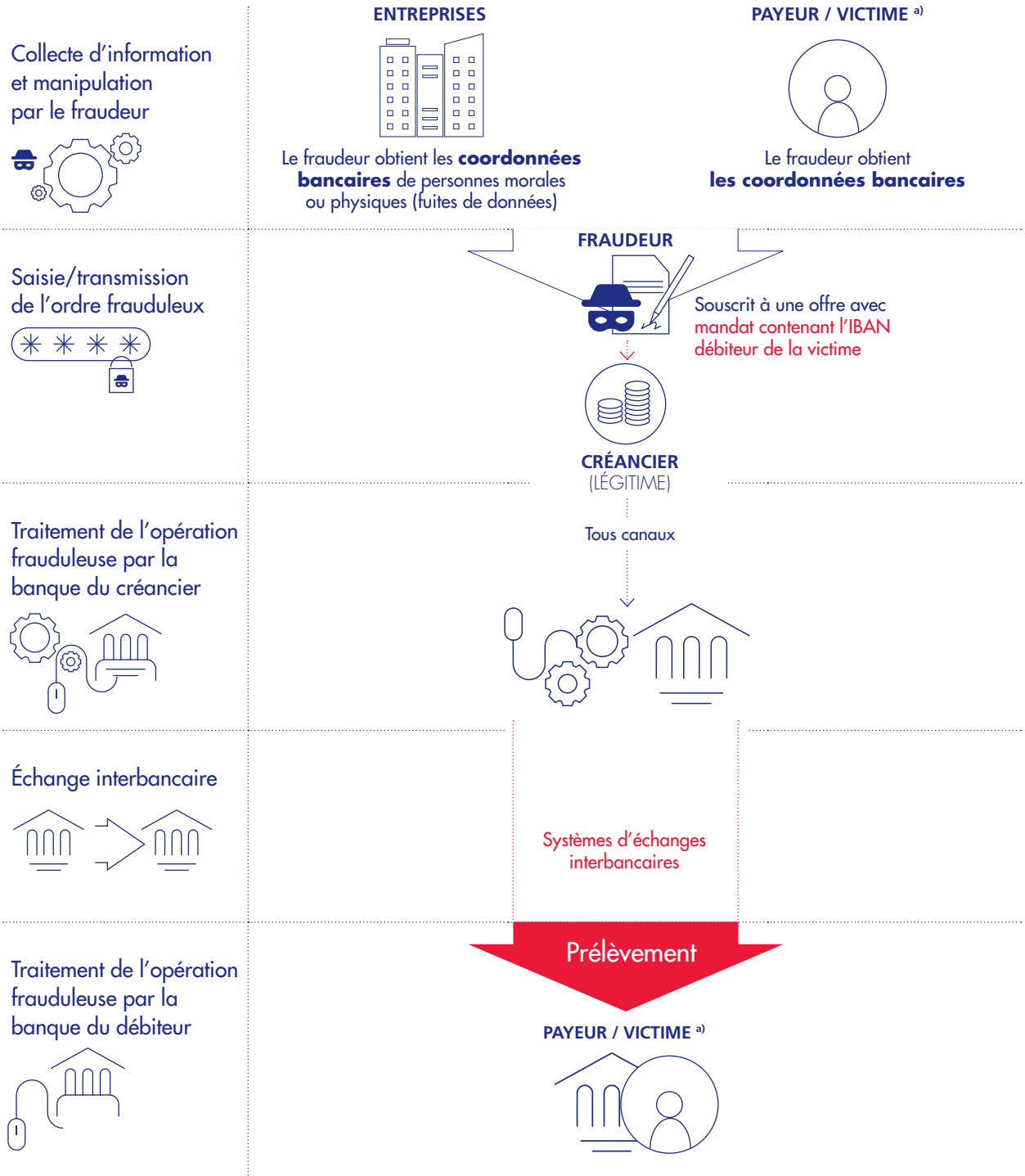
Tout d'abord, les plateformes de surveillance, accompagnées ou non d'intelligence artificielle, ont du mal à identifier les prélèvements frauduleux. En effet, les faibles volumes de fraude constatés jusqu'à récemment sur ce moyen de paiement n'ont pas permis de dégager des modèles types d'opération permettant de bien calibrer les règles de détection.

Ensuite, il existe peu de critères permettant de détecter *a priori* la malveillance d'un créancier. Le mandat n'est pas un prérequis à la validation d'un prélèvement par le PSP émetteur, et il pourrait de toute façon avoir été falsifié par le fraudeur. Les possibilités d'échapper à un contrôle strict de l'ICS fourni, que le créancier fraudeur aura fait créer auprès d'un établissement tiers, sont également nombreuses *(cf. section 2.1.3.3, partie « Panorama des mesures et bonnes pratiques existantes », sous-partie « Contrôle de l'ICS »* infra*)*.

Enfin, le créancier fraudeur peut avoir utilisé un compte ouvert dans un établissement étranger pour émettre son prélèvement, donc hors de portée des autorités de régulation françaises, ou avoir repéré les établissements ayant les procédures de contrôle les moins contraignantes.

De la même manière que pour les virements, les établissements peuvent en revanche identifier l'activité frauduleuse d'un client lorsque celui-ci va tenter de sortir les fonds vers un autre compte, rentrant ainsi dans le périmètre des outils de surveillance des opérations émises. Cela passe notamment par l'implémentation de règles repérant les séquences anormales entre arrivée puis sortie de fonds sur un même compte.

MÉCANISME DE LA FRAUDE AU « DÉTOURNEMENT DE PRÉLÈVEMENT »



a) Payeur/victime : peut être une personne physique ou une personne morale (entreprise, association, administration, etc.).
Note : Cette infographie n'illustre pas de manière exhaustive le déroulement d'une fraude au prélèvement de type « détournement ».

2.1.3.3 Les mesures visant à détecter, voire bloquer, les tentatives de fraude au niveau de l'établissement du débiteur/payeur

■ **Panorama des mesures et bonnes pratiques existantes**

Contrôle de l'ICS

Le PSP qui reçoit un prélèvement à débiter sur le compte de son client a la possibilité de vérifier l'existence et la validité (y compris la non-radiation) de l'ICS présent dans l'opération. Mais il ne peut effectivement le faire que si l'ICS a été émis en France, en interrogeant le référentiel géré par la Banque de France.

Si l'opération est émise par un créancier ayant obtenu son identifiant ICS à l'étranger, il est impossible pour le PSP d'effectuer un contrôle sur la base du référentiel ICS du pays concerné. Les référentiels ICS locaux, lorsqu'ils existent, n'étant pas partagés entre autorités nationales, les fraudeurs savent exploiter cette gestion en silo des ICS au niveau européen.

Les contrôles des PSP sont également limités par l'usage fait de prestataires de services mutualisant les émissions de prélèvement, l'ICS, voire le numéro de compte, pour un ensemble de créanciers. Bloquer un ICS sur cette base n'est pas souhaitable puisqu'il peut regrouper à la fois des créanciers fraudeurs et légitimes, sans possibilité de les distinguer.

De la même manière, un créancier ayant eu une activité légitime jusqu'ici peut être désormais sous le contrôle d'un fraudeur et donc passer au travers de la vérification de l'ICS par le PSP, tant que la fraude n'a pu être détectée sur la base des contestations des débiteurs.

Contrôle du créancier au moyen des listes établies par le client

Le PSP du débiteur peut être amené à contrôler l'opération de prélèvement sur la base de listes de créanciers fournies et mises à jour par le client.

Pour plus de détails, se référer à la section « 2.1.3.4 Les mesures visant à accroître la vigilance de l'utilisateur des moyens de paiement/titulaires de comptes ».

Surveillance des opérations

Les prélèvements sont surveillés par des plateformes de détection de la fraude. Cependant, le blocage d'une opération suspecte sans contestation du client débiteur au préalable est rare.

Cela s'explique notamment par les différentes possibilités de contournement du contrôle des ICS décrites précédemment, qui peuvent également s'appliquer à l'IBAN : par exemple, le créancier fraudeur qui peut être masqué derrière le compte du prestataire de services de mutualisation d'émission de prélèvement, ou le créancier initialement légitime désormais contrôlé par le fraudeur. L'IBAN utilisé par le fraudeur peut aussi être différent à chaque fraude, comme pour le virement.

Si le PSP du débiteur décide d'effectuer un rejet qui s'avère non justifié, la procédure de régularisation par les deux établissements est considérée comme complexe et coûteuse par la communauté bancaire, d'autant que la probabilité de « faux positifs » sur les prélèvements est élevée en l'état actuel des outils de détection. L'établissement peut néanmoins prévenir le client en cas de suspicion, mais la décision de blocage d'une fraude revient principalement au client lui-même.

2.1.3.4 Les mesures visant à accroître la vigilance de l'utilisateur des moyens de paiement/ titulaires de comptes

Compte tenu des limites constatées par les PSP concernant leur capacité à pouvoir détecter et bloquer des prélèvements frauduleux, la vigilance et la réactivité des titulaires de comptes sont primordiales pour espérer déjouer une fraude avant débit du compte ou la détecter rapidement après débit.

■ **Panorama des mesures et bonnes pratiques existantes**

Information et notification d'un nouveau prélèvement à venir

Les sites et applications de banque à distance permettent au client d'être informé, parfois par notification (application sur *smartphone*, SMS, e-mail), de l'arrivée imminente d'un nouveau prélèvement sur son compte. L'information visible peut contenir le montant, le nom de la société, son ICS et la référence du mandat utilisé. La possibilité lui est aussi donnée de contester cette opération.

Cela n'exclut hélas pas les possibilités de contournement par le fraudeur pour tromper ses victimes : prise de contrôle d'un créancier connu et de son ICS, utilisation d'un nom de société proche ou usurpation de l'ICS d'un créancier légitime.

Listes noires et blanches de créanciers

Le client a la possibilité de spécifier auprès de son PSP des listes noires (exclusion de créanciers présents dans la liste) et blanches (autorisation limitée aux créanciers présents dans la liste) conformément aux règles du SEPA [19]. Cet outil est, sur le principe, efficace puisqu'il donne au PSP un critère explicite de filtrage des prélèvements sans mandat avant

débit sur le compte, et permettrait donc en théorie de contenir une partie importante des fraudes sur ce moyen de paiement.

Mais cette possibilité semble peu utilisée par la clientèle des banques et peu mise en avant par les banques elles-mêmes. Son utilisation suppose en effet une rigueur de gestion des listes de la part du client vis-à-vis des mandats qu'il signe, puisqu'aucun mécanisme de synchronisation n'existe entre ces données. En cas d'erreur dans la gestion des listes (par exemple, omission d'un créancier sur une liste blanche ou ajout d'un créancier à tort sur une liste noire), les rejets à tort léseraient les créanciers de bonne foi, ainsi que les débiteurs eux-mêmes, qui pourraient se retrouver dans une situation délicate d'impayés de factures (téléphonie, assurances, mutuelle, etc.) et de rupture d'une prestation de services importante.

2.1.3.5 Les mesures visant à empêcher le vol de données sur les titulaires de comptes

■ Panorama des mesures et bonnes pratiques existantes

Sécurisation des données de paiement dans le système d'information des entreprises

Les PSP sont réglementairement dans l'obligation de protéger les données sensibles de paiement [20] – c'est-à-dire pouvant être exploitées dans une fraude. Cette protection s'effectue à l'aide de mécanismes robustes tels que le chiffrement des données en mouvement (flux) et au repos (stockage), l'authentification forte pour l'accès aux données par le personnel interne, et autres mesures aidant à garantir la confidentialité et l'intégrité des données. En outre, l'OSMP recommande que l'identifiant du compte soit masqué sur les écrans de banque à distance [21].

Les entreprises non soumises à cette directive sont également amenées à manipuler ce type de données, par exemple les identifiants de compte bancaire de salariés, clients ou fournisseurs. Ces données sont considérées comme « hautement personnelles » selon la Commission nationale de l'informatique et des libertés (CNIL) [22], lorsqu'il s'agit des comptes bancaires de personnes physiques. Toutefois, le règlement général de protection des données (RGPD) [23] exige des entreprises qu'elles mettent en œuvre des mesures de sécurisation correspondant au niveau de risque évalué dans le cadre de leurs activités, sans néanmoins imposer de mesures techniques particulières.

Malheureusement, les nombreuses fuites de données de compte relevées ces dernières années montrent que les bases de données d'IBAN sont insuffisamment protégées dans les entreprises ou par leurs prestataires.

2.1.4 Recommandations relatives aux paiements SEPA

Recommandation n° 1 :

Permettre le partage des données de fraude entre établissements

L'Observatoire encourage l'évolution du cadre réglementaire dans le but de permettre un partage entre établissements des données relatives aux fraudes détectées sur les virements et prélèvements.

Recommandation n° 2 :

Poursuivre et renforcer la mise en garde du public vis-à-vis des techniques d'ingénierie sociale

L'Observatoire appelle l'ensemble des parties prenantes des secteurs public et privé à poursuivre leurs efforts de communication pour alerter et sensibiliser le public aux risques liés aux techniques de manipulation directe de l'utilisateur de services de paiement. Dans un contexte de sophistication des techniques d'ingénierie sociale par les fraudeurs, l'utilisateur de services de paiement est devenu une cible privilégiée. Afin d'atteindre l'audience la plus large possible, ces actions de sensibilisation devraient être récurrentes, employer tous les canaux d'information disponibles, et faire preuve de la plus grande pédagogie dans leur contenu.

19 Règlement SEPA article 5-3 d.

20 DSP 2, article 5, paragraphe 1 g.

21 *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement*, 2017.

22 Lignes directrices du groupe « Article 29 » sur l'analyse d'impact relative à la protection des données.

23 Règlement général sur la protection des données – article 32.

Recommandation n° 3 :

Prendre toutes les précautions nécessaires dans l'usage du virement

L'Observatoire rappelle aux utilisateurs de services de paiement plusieurs bonnes pratiques à mettre en œuvre lorsqu'ils souhaitent réaliser un virement, d'autant plus s'il s'agit d'un virement instantané :

- n'effectuez un virement que lorsque vous êtes certain de l'identité du bénéficiaire et de son IBAN ;
- en cas de doute, réalisez un contre-appel vers le bénéficiaire pour confirmer l'exactitude de ses coordonnées bancaires, en particulier s'il est supposé vous avoir communiqué un changement récent ;
- ne réalisez jamais d'opération sous la pression et dans la précipitation, notamment lorsque l'opération est réalisée à la demande d'une personne se faisant passer pour votre conseiller ou pour un collaborateur du service des fraudes ;
- pour réaliser un virement, privilégiez l'usage de l'espace de banque à distance, les solutions d'initiation de paiement ou les déplacements en agence bancaire ;
- tout au long du processus de paiement, prêtez attention aux informations et avertissements relatifs à l'opération qui sont affichés par votre prestataire de services de paiement.

Recommandation n° 4 :

Sensibiliser le public au risque de fraude au prélèvement et rappeler les mesures de protection du débiteur

L'Observatoire encourage les prestataires de services de paiement et les services publics à rappeler les principes de fonctionnement du prélèvement bancaire et les risques associés. Ces actions de sensibilisation devraient en particulier décrire le rôle du créancier, du débiteur et de leurs prestataires de services de paiement respectifs dans la gestion du mandat de prélèvement, ainsi que les mesures de protection dont bénéficie le débiteur et les règles de vigilance qu'il doit appliquer. Notamment :

- la vérification régulière des extraits de compte et la consultation des messages transmis par sa banque ;
- la nécessité de réagir au plus tôt en cas d'anomalie constatée ;
- la mise à disposition par la banque du débiteur de moyens de consultation des créanciers actifs prélevant son compte ;
- la possibilité d'indiquer les créanciers non autorisés à prélever son compte, ou à l'inverse, de limiter les créanciers autorisés à le faire, sous réserve d'une gestion rigoureuse de ces listes ;
- les délais réglementaires durant lesquels il peut obtenir un remboursement auprès de sa banque : huit semaines de façon inconditionnelle, treize mois pour un prélèvement réalisé sans consentement (non autorisé).

2.2 Mesures de prévention de la fraude sur les paiements par carte à distance hors 3-D Secure

2.2.1 Contexte des travaux

La directive UE n° 2015/2366 du 25 novembre 2015 sur les services de paiement, dite DSP 2 [24], transposée en droit français dans le Code monétaire et financier [25], prévoit le recours à un dispositif d'authentification forte du payeur pour les paiements électroniques ainsi que pour les opérations exécutées par le biais d'un moyen de communication à distance susceptibles de comporter un risque de fraude [26]. Le règlement délégué UE n° 2018/389 du 27 novembre 2017 (ou RTS, *regulatory technical standard*) prévoit toutefois des exemptions [27] concernant notamment les opérations effectuées en faveur d'un bénéficiaire de confiance, les opérations récurrentes, les opérations de faible montant ou encore les opérations qui présentent un faible niveau de risque.

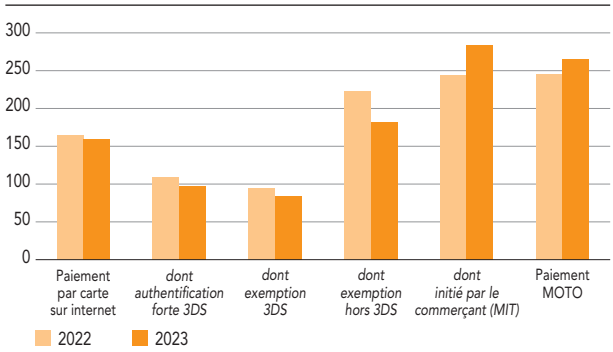
En France, la mise en œuvre progressive de l'authentification forte pour les paiements à distance effectués par carte bancaire s'est effectuée dans le cadre du plan de migration adopté par l'Observatoire [28].

Cette mise en œuvre a été rendue possible par le déploiement de la deuxième version du protocole 3-D Secure destiné à la gestion des échanges entre le commerçant, le porteur de la carte et leurs prestataires de services de paiement (PSP), en vue de l'authentification des paiements par internet. La version 2.0 du protocole permet la gestion de l'authentification forte des paiements à distance à l'aide des différentes solutions actuellement proposées aux porteurs de cartes par les PSP émetteurs, et prend également en charge les demandes d'exemption à l'authentification forte.

La mise en œuvre de l'authentification forte a permis la réduction du taux de fraude sur les paiements à distance effectués via 3-D Secure. Le taux de fraude apparaît aujourd'hui maîtrisé sur l'ensemble de ces paiements, y compris sur ceux bénéficiant d'une exemption à l'authentification forte *(cf. graphique)*.

À l'inverse, le taux de fraude reste aujourd'hui structurellement plus élevé sur les paiements effectués à distance hors 3-D Secure, parmi lesquels les paiements de type MIT (*Merchant Initiated Transaction*) ainsi que les paiements MOTO (*Mail Order, Telephone Order*).

Taux de fraude sur la carte, 2022-2023 (en %)



3DS, *3-D Secure* ; MIT, *Merchant Initiated Transaction* ; MOTO, *Mail Order, Telephone Order*.
Notes : Le taux de fraude correspond au montant de la fraude en euros pour 100 000 euros de paiement.
Le paiement MOTO est un paiement à distance hors internet (réalisé par courrier, postal ou électronique [courriel], ou par téléphone/télécopie).
Source : Observatoire de la sécurité des moyens de paiement.

Par nature, ces paiements, qui ne donnent lieu à aucune authentification au moment de leur émission, sont beaucoup plus exposés à la fraude que les paiements transitant par le protocole 3-D Secure :

- de tels paiements peuvent être initiés par toute personne ayant pu prendre connaissance des données inscrites sur la carte bancaire (numéro et date d'expiration pour les paiements MOTO, et cryptogramme visuel en sus pour les paiements MIT), sans même que cette personne ait besoin d'être en possession de la carte ou d'avoir accès au dispositif d'authentification forte des paiements à distance ;
- en particulier, un commerçant peut transmettre à son PSP des paiements qui ne correspondent en réalité à aucun produit ou service délivré au porteur de la carte, par exemple en réutilisant les données de cartes de paiement précédemment utilisées dans le cadre de transactions légitimes ;
- s'agissant en particulier des paiements MOTO, ceux-ci reposent sur la communication par le client payeur du numéro de sa carte bancaire et de sa date d'expiration par un canal non sécurisé (conversation téléphonique, courriel, envoi postal, télécopie, etc.), puis sur leur manipulation par un opérateur qui assure la saisie sur le terminal de paiement du commerçant. Cette situation favorise la fraude interne ou externe par détournement des données de paiement.

Si les standards techniques en vigueur incluent théoriquement la possibilité de mettre en place une solution d'authentification des paiements MOTO, cette possibilité est en pratique inutilisée et aucune solution uniforme pour l'authentification de ces paiements n'a été identifiée à ce jour.

De plus, les paiements MOTO et les paiements internet hors 3-D Secure sont parfois détournés de leur finalité originelle pour permettre à un commerçant d'accepter des paiements par internet initiés par le client (CIT, *Customer Initiated Transaction*) en contournant l'obligation d'authentification forte pourtant imposée par la DSP 2.

Ces constats conduisent l'Observatoire à formuler des recommandations qui visent à prévenir la fraude sur les paiements à distance effectués hors 3-D Secure.

2.2.2 Périmètre des recommandations

Les présentes recommandations s'appliquent à l'ensemble des paiements à distance sans authentification forte effectués hors 3-D Secure, à savoir :

- d'une part, les paiements MOTO ;
- d'autre part, les paiements internet hors 3-D Secure, au nombre desquels les paiements de type MIT (pour lesquels seule l'authentification forte effectuée lors de la validation du mandat utilise le canal 3-D Secure), ainsi que les paiements CIT demandant le bénéfice d'une exemption sans transiter par le protocole 3-D Secure (on parle alors de paiement DTA, *direct to authorisation*).

Par exception, ces recommandations ne s'appliquent pas :

- aux paiements internet hors 3-D Secure reconnus comme authentifiés fortement par le PSP émetteur, tels que les paiements effectués à l'aide d'une solution mobile de type *wallet* [29] intégrant une solution d'authentification forte reconnue comme conforme à la DSP 2 par le PSP émetteur de la carte ;
- aux paiements électroniques initiés par des personnes morales au moyen de procédures ou de protocoles de paiement dédiés qui sont uniquement mis à la disposition de payeurs qui ne sont pas des consommateurs, lorsque les autorités compétentes ont acquis la certitude que lesdits procédures et protocoles garantissent des niveaux de sécurité au moins équivalents à ceux prévus par la DSP 2 [30] ;

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

25 Article L. 133-1 et suivants.

26 Article L. 133-4 I du Code monétaire et financier.

27 Articles 11 à 18 du règlement UE n° 2018/389.

28 Chapitre 1 du *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement*, 2018.

29 Le *wallet* est un outil de paiement en ligne qui stocke de manière sécurisée les versions numériques des cartes de paiement du propriétaire du *wallet*.

30 Ces paiements sont exemptés de l'obligation d'authentification forte en application de l'article 17 du règlement UE n° 2018/389.

- aux paiements pour lesquels le PSP acquéreur est situé dans un État qui n'est pas partie à l'accord sur l'Espace économique européen.

Les présentes recommandations ont vocation à être mises en œuvre par les commerçants qui acceptent de tels paiements, par leurs prestataires d'acceptation technique, par les différents schémas de cartes ainsi que par l'ensemble des PSP, qu'ils soient émetteurs ou acquéreurs.

2.2.3 Recommandations applicables aux paiements à distance hors 3-D Secure

2.2.3.1 Utilisation des paiements MOTO et des paiements par internet hors 3-D Secure seulement lorsque le recours à un autre mode de paiement n'est pas possible

Le taux élevé de fraude sur ces paiements impose de limiter les paiements MOTO, ainsi que les paiements par internet hors 3-D Secure (autres que ceux reconnus comme authentifiés par le PSP émetteur, par exemple lors de l'utilisation d'un *wallet*), aux seuls cas d'usage auxquels ces modes de paiement sont destinés.

En particulier, les paiements par internet pouvant bénéficier d'une exemption à l'authentification forte ont vocation à être présentés via 3-D Secure. En effet, ce protocole permet la gestion des demandes d'exemption, et la demande d'authentification forte du client lorsque la demande d'exemption est rejetée par *soft decline*.

Recommandation n° 1 :

Limitation des paiements MOTO et MIT aux seuls cas d'usage où le recours à un autre mode de paiement n'est pas possible

Les commerçants veillent :

- à n'accepter des paiements par carte de type MOTO (*Mail Order, Telephone Order*) que pour les contrats souscrits à distance par un canal autre qu'internet (téléphone, courrier, etc.). Ils veillent à recourir à un paiement de proximité ou à un paiement sécurisé par internet chaque fois que la nature d'un contrat et les modalités de sa souscription ainsi que de la livraison des biens ou services commandés sont compatibles avec un tel paiement (par exemple, paiement de proximité lors de la livraison, effectuée directement par le commerçant, de biens commandés par téléphone) ;

…/ …

- à n'accepter des paiements par internet que via le canal sécurisé 3-D Secure, en dehors des cas où le paiement est reconnu comme authentifié par l'émetteur (par exemple, lors de l'utilisation d'un *wallet* intégrant l'authentification forte) et des cas d'usage qui ne permettent pas le recours à 3-D Secure, tels que les paiements de type MIT (*Merchant Initiated Transactions*).

En particulier, les commerçants ne doivent jamais recourir à des paiements par internet hors 3-D Secure et des paiements de type MOTO lorsque le paiement s'effectue par internet et a été initié par le client (CIT, *Customer Initiated Transaction*).

Les prestataires d'acceptation technique et les prestataires de services de paiement acquéreurs veillent au respect de cette recommandation par les commerçants avec lesquels ils ont conclu un contrat d'acceptation.

2.2.3.2 Chaînage valide des paiements MIT

Le recours au protocole 3-D Secure pour l'ensemble des paiements par internet initiés par le client (CIT) devrait conduire à réserver les paiements par internet hors 3-D Secure autres que ceux reconnus comme authentifiés par le PSP émetteur (par exemple lors de l'usage d'un *wallet* intégrant une solution d'authentification forte) aux seuls paiements initiés par le commerçant (MIT).

Chaque paiement MIT doit être associé à une référence de chaînage valide permettant à l'émetteur de la carte de s'assurer du consentement de son porteur au paiement présenté ou, lors du traitement d'une contestation formulée par le porteur, de procéder au rapprochement entre le paiement et le mandat préalablement validé par authentification forte.

Si l'absence de chaînage peut être détectée lors de l'acceptation du paiement par le PSP émetteur, l'analyse de la validité du chaînage (c'est-à-dire s'assurer que le chaînage présenté correspond à une authentification préalable) ne peut être réalisée en temps réel par celui-ci. De ce fait, les chaînages invalides, c'est-à-dire ne correspondant pas à un mandat de paiement dûment validé par le porteur au moyen d'une authentification forte, ne pourront être détectés qu'en réalisant un rapprochement *a posteriori* que les PSP émetteurs sont invités à mettre progressivement en œuvre.

Recommandation n° 2 :

Chaînage valide des MIT

Lors de toute émission d'un paiement MIT, les commerçants communiquent à leur PSP la référence de chaînage issue de la validation par authentification forte du mandat de paiement autorisant le paiement.

Les PSP émetteurs sont invités :

- à mettre en œuvre progressivement un mécanisme de rapprochement entre le chaînage des paiements MIT et les mandats de paiement validés par authentification forte ;
- à notifier aux commerçants et aux prestataires d'acceptation technique les anomalies relevées dans les chaînages présentés dans les transactions MIT qu'ils émettent afin que ces derniers mettent en place un plan d'action visant à y remédier ;
- à défaut de remédiation, à appliquer la limite de vélocité définie par la recommandation n° 7 aux paiements MIT présentés par les commerçants et/ou les prestataires d'acceptation technique concernés par le recours à des références de chaînage invalides.

2.2.3.3 Limitation de la vélocité des paiements MOTO et des paiements par internet hors 3-D Secure

La prévention de la fraude sur les paiements MOTO et sur les paiements par internet hors 3-D Secure (en dehors des cas, tels que l'usage d'un *wallet* intégrant une solution d'authentification forte, où l'opération est considérée comme authentifiée par le PSP émetteur) impose de limiter la vélocité, c'est-à-dire le montant cumulé des achats effectués avec une même carte auprès d'un même commerçant durant une période de 24 heures (glissante).

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

La vélocité est mesurée de manière indépendante pour les paiements MOTO d'une part, et pour les paiements par internet hors 3-D Secure d'autre part.

L'Observatoire invite les PSP émetteurs à rejeter toute opération conduisant au dépassement de cette limite, par *soft decline* lorsque les caractéristiques de l'opération permettent ce mode de rejet.

Cette limite de vélocité ne concerne pas :

- les secteurs d'activité pour lesquels le recours au mode de paiement considéré (MOTO ou MIT) apparaît justifié et pour lesquels le taux de fraude est maîtrisé. Ces secteurs sont intégrés à la « liste d'exclusions » définie en encadré 6 ;
- les paiements MIT associés à une référence de chaînage techniquement valide et pour lesquels le commerçant et le prestataire d'acceptation technique n'ont pas été identifiés comme émettant des paiements associés à des références de chaînage présentant des anomalies.

En outre, des exemptions individuelles pourront être accordées, en fonction du taux de fraude observé pour chaque commerçant [31].

À l'inverse, l'exclusion pourra être levée, sur décision du PSP émetteur et pour la durée de son choix, pour un commerçant dont le code de catégorie de marchand (MCC, *Merchant Category Code*) bénéficie d'une exclusion, mais qui réalise un usage inapproprié des paiements MOTO ou des paiements par internet hors 3-D Secure, ou encore dont le taux de fraude sur ces paiements apparaît insuffisamment maîtrisé au regard des critères définis par le PSP émetteur.

Recommandation n° 3 :

Limite de vélocité et mise en place d'un mécanisme de *soft decline*

Les PSP émetteurs rejettent, par *soft decline* lorsque cela est possible, les paiements MOTO et les paiements par internet hors 3-D Secure reconnus comme non authentifiés par l'émetteur, dès lors que le montant du paiement conduirait au dépassement de la limite de vélocité définie par la présente recommandation.

La limite de vélocité, appréciée sur une période de 24 heures glissantes, est fixée à :

- 500 euros pour la période du 10 juin au 8 septembre 2024 inclus ;
- 250 euros pour la période du 9 septembre au 13 octobre 2024 inclus ;
- 100 euros à compter du 14 octobre 2024.

L'abaissement aux seuils de 250 euros et 100 euros sera soumis à l'examen préalable de la capacité du marché à s'y adapter par le groupe de travail dédié de l'Observatoire.

…/ …

31 Un commerçant est identifié, lors de l'émission d'un paiement par carte, par la valeur renseignée dans le champ *Merchant ID* inclus dans les données de ce paiement.

La vélocité est mesurée de manière distincte :

- d'une part, pour les paiements MOTO ;
- d'autre part, pour les paiements internet hors 3-D Secure. Pour cette catégorie de paiement, la mesure de la vélocité ne prend en compte ni les paiements CIT authentifiés par l'émetteur (notamment par *wallet* mobile) ni les paiements MIT associés à une référence de chaînage valide.

Sont exclus de l'application de cette recommandation :

- les paiements acceptés par des commerçants qui bénéficient d'une exemption (pour le type de paiement concerné) accordée dans les conditions définies en encadré 6, sauf si le PSP émetteur a levé cette exemption pour le commerçant concerné ;
- les paiements MIT qui sont associés à une référence de chaînage valide ;
- les paiements MOTO qui ont fait l'objet d'une authentification forte.

La mise en œuvre des limites de vélocité sera supervisée par un comité de pilotage placé sous l'égide du groupe de travail « authentification forte » de l'Observatoire.

Ce comité de pilotage aura la charge :

- de vérifier que l'ensemble des cas d'usage légitimes des paiements MOTO et des paiements par internet hors 3-D Secure ont été pris en compte et que la mise en œuvre des limites de vélocité ne conduit pas au rejet d'opérations légitimes ;
- de proposer tout ajustement nécessaire des modalités de mise en œuvre de la présente recommandation et en particulier de modifier la liste des activités exclues de son champ d'application ou de différer les dates et conditions d'entrée en application des deuxième et troisième paliers.

2.2.3.4 Sécurité des données de paiement transmises par le payeur lors d'un paiement MOTO

Les commerçants qui acceptent des paiements MOTO doivent apporter une attention particulière à la sécurité des données de paiements qu'ils manipulent, afin de prévenir leur détournement.

S'agissant des paiements par téléphone (*telephone order*), le recours à un système informatisé permet d'éviter la manipulation des données par un opérateur : le client payeur saisit ses données de paiement directement sur le clavier de son téléphone à fréquences vocales (qu'il s'agisse d'un téléphone fixe, d'un téléphone mobile ou d'un *smartphone*) et le système transmet automatiquement ces données vers le terminal de paiement, pour permettre l'acceptation du paiement.

Selon le cas d'usage, le client peut soit être en relation directement avec un serveur vocal (par exemple pour le paiement d'une facture : le client saisira alors la référence de la facture avant de saisir ses données de paiement), soit être en relation avec un opérateur auquel il indique les caractéristiques des biens ou services qu'il souhaite commander, avant d'être mis en relation avec un serveur vocal au moment de procéder au paiement, soit saisir ses données de paiement sur le clavier du téléphone pendant l'échange avec l'opérateur.

Recommandation n° 4 :

Sécurisation des données de paiement

Les commerçants qui acceptent des paiements MOTO veillent à garantir la sécurité des données de paiement communiquées par les clients. Les commerçants qui acceptent des paiements par téléphone (*telephone order*) veillent, dans la mesure du possible, à ce que les clients communiquent leurs données de paiement à un automate ou par saisie directe sur le clavier du téléphone plutôt qu'oralement à un opérateur.

Les prestataires de services de paiement acquéreurs veillent au respect de cette recommandation par les commerçants avec lesquels ils ont conclu un contrat d'acceptation.

2.2.3.5 Expérimentation de l'authentification des paiements MOTO

La mise en œuvre d'un mécanisme d'authentification, même simple (un seul facteur d'authentification), pour les paiements MOTO permettrait l'amélioration du niveau de sécurité puisque ces paiements ne font pour l'instant l'objet d'aucune authentification.

Dans certains cas, cette authentification pourrait s'effectuer à l'aide des dispositifs déjà existants, tels que l'authentification par application mobile des paiements effectués par téléphone, pour les porteurs de cartes enrôlés à la solution d'authentification forte par application mobile proposée par leur PSP, ou par la saisie d'un mot de passe à usage unique reçu par SMS.

Certaines solutions d'authentification forte conçues pour les paiements par internet apparaissent à l'inverse incompatibles avec les paiements par téléphone, qui ne permettent pas la saisie d'un mot de passe alphanumérique. La typologie particulière de la clientèle qui recourt aux paiements par téléphone (par exemple, clients ne disposant pas d'un accès à internet ou d'une ligne de téléphone mobile) devrait par ailleurs être prise en compte.

Recommandation n° 5 :

Expérimentation de l'authentification des paiements MOTO

Les commerçants et les prestataires de services de paiement (PSP) sont encouragés à proposer pour les paiements de type MOTO des solutions d'authentification adaptées à chaque canal de paiement et à la typologie de clientèle concernée.

2.3 Les travaux avec les opérateurs de télécommunications

2.3.1 Contexte

À la suite de la mise en place de l'authentification forte et des mécanismes de mesure du risque (*scoring*) des transactions, impulsée par la deuxième directive européenne sur les services de paiement (DSP 2), **les fraudeurs se sont adaptés. Ils ont développé des techniques d'attaque par manipulation**. En particulier, la fraude au faux conseiller bancaire consiste soit à faire valider les opérations frauduleuses par les victimes elles-mêmes, soit à ce que les fraudeurs s'approprient les outils d'authentification forte pour réaliser directement des opérations frauduleuses.

Ces fraudes s'appuient sur différentes techniques de détournement des outils et infrastructures de télécommunications, notamment :

- l'envoi de messages électroniques ou de SMS usurpant l'identité de l'expéditeur (*phishing* ou *smishing*, c'est-à-dire hameçonnage) et la création de sites miroirs dupliquant des sites légitimes, afin de collecter les données personnelles des clients ;
- l'usurpation de numéros d'appelants (*spoofing*) permettant de tromper le destinataire sur l'origine des appels reçus (par exemple, en affichant le numéro du conseiller bancaire, du standard de la banque ou de son service de mise en opposition des cartes) ;
- la duplication de la carte SIM de la victime (ou *SIM swapping*) qui permet au fraudeur de recevoir à la place de la victime les SMS comportant des informations d'authentification.

Fort de son élargissement au secteur des télécoms, l'Observatoire s'attache à identifier les pistes permettant d'endiguer le recours à ces techniques par les fraudeurs. L'approche concertée a été privilégiée par la constitution d'un groupe de travail réunissant les représentants des prestataires de services de paiement (PSP) et les principaux opérateurs de téléphonie, ainsi que les différentes autorités concernées : Banque de France, Autorité de contrôle prudentiel et de résolution (ACPR), Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), Direction générale du Trésor.

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

La lutte contre le *spoofing* repose principalement sur la mise en œuvre du programme MAN (mécanisme d'authentification des numéros). Celui-ci est conduit par l'Association des plateformes de normalisation des flux interopérateurs (APNF), qui réunit la totalité des opérateurs attributaires de numéros provenant du plan de numérotation national. Ce programme [32], qui vise à appliquer les dispositions du IV de l'article L. 44 du Code des postes et des communications électroniques issues de la loi dite « Naegelen » [33], comporte deux étapes :

- En premier lieu, le déploiement d'une infrastructure technique commune permettant aux opérateurs d'authentifier les appels téléphoniques. La mise en place de l'infrastructure et le raccordement de l'ensemble des opérateurs ont été achevés le 1er juin 2024. L'authentification consiste à garantir, à l'aide d'un certificat électronique, que l'appel provient bien de la ligne associée au numéro présenté comme numéro appelant.
- En second lieu, l'interruption de l'acheminement (c'est-à-dire la coupure) des appels qui ne sont pas authentifiés aura lieu le 1er octobre 2024. En raison des impératifs de continuité liés aux Jeux olympiques, les opérateurs ont fait le choix de ne pas procéder aux coupures des appels non authentifiés durant l'été 2024.

Si le contrôle du respect de la loi Naegelen relève de la mission de l'Arcep, les conséquences du *spoofing* sur la fraude aux moyens de paiement conduisent l'Observatoire à porter une attention particulière au calendrier de mise en œuvre du programme MAN. L'Observatoire veillera également à identifier les scénarios de fraude qui seront susceptibles d'émerger lors de la mise en œuvre effective du programme MAN, du fait d'une éventuelle adaptation des fraudeurs.

32 Cf. *https://www.fftelecoms.org/nos-travaux-et-champs-dactions/calendrier-de-mise-en-oeuvre-du-mecanisme-dauthentification-des-numeros/*

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

Il s'assurera aussi de la réactivité de l'ensemble des acteurs pour endiguer d'éventuels phénomènes de report de la fraude ou de non-conformité d'opérateurs.

Parallèlement au suivi de la mise en œuvre du programme MAN, l'Observatoire a engagé, à la demande des PSP, une réflexion sur les mesures de nature à compléter la lutte contre le *spoofing*. Celles-ci porteraient sur la protection des numéros particulièrement exposés, tels que les numéros des centres d'opposition aux cartes bancaires perdues ou volées.

Ces mesures pourraient reposer sur un mécanisme dit *Do Not Originate* (DNO), qui consiste, pour les opérateurs, à bloquer les appels émis depuis un numéro identifié comme exclusivement destiné à recevoir des appels. Chaque PSP aurait la charge d'identifier les numéros qu'il utilise uniquement en réception, et d'en communiquer la liste aux opérateurs de téléphonie.

L'étude actuellement menée consiste à identifier ces numéros auprès de l'ensemble des PSP intéressés et à mesurer le volume d'appels émis depuis ces numéros, afin de quantifier les usages présumés frauduleux actuellement observés.

2.3.3 La lutte contre le *smishing* : la protection des OAdC (*Originator Address Codes*)

Le *smishing* (ou hameçonnage par SMS, contraction de « SMS » et « *phishing* »), utilisé pour rediriger les clients vers de faux sites ou faux numéros d'appel, est rendu d'autant plus efficace lorsque i) le SMS frauduleux mentionne comme expéditeur un OAdC, c'est-à-dire un libellé comportant 11 caractères alphanumériques plutôt qu'un numéro débutant par 06 ou 07, et que ii) cet OAdC laisse entendre au destinataire du SMS que ce dernier provient d'un expéditeur légitime (banque, service public, etc.), à l'instar du *spoofing*.

L'AF2M [34] a mis en place, en lien avec les prestataires assurant l'acheminement des SMS, un mécanisme de protection des OAdC :

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

La liste des OAdC sensibles et des OAdC interdits est mise à jour de manière régulière, notamment sur la base des signalements envoyés par les particuliers au 33700 (plateforme nationale de déclaration des SMS non sollicités mise en place par l'AF2M).

Le mécanisme de protection des OAdC étant déjà opérationnel, les travaux de l'Observatoire portent sur d'éventuelles pistes de renforcement de la coordination entre le secteur des paiements et l'AF2M. Ces travaux concernent essentiellement la gestion des listes d'OAdC liés au secteur des paiements et les modalités de déclaration des SMS frauduleux identifiés (par exemple, l'amélioration de l'ergonomie et le renforcement de la notoriété du 33700, ou encore la mise en place d'un canal de signalement adapté à un usage professionnel).

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

Afin de prévenir les impacts du *SIM swapping* sur les titulaires des lignes, les opérateurs proposent une interface de programmation d'application (API, *application programming interface*) appelée « *SIM verify* ». Elle permet de savoir si un renouvellement de carte SIM est récemment intervenu sur une ligne téléphonique donnée. Cette API est multi-opérateurs et couvre désormais la quasi-totalité des lignes mobiles françaises.

La consultation de cette API peut ainsi être intégrée dans les outils de détection et de prévention de la fraude des PSP quand ils recourent à une authentification des opérations par « SMS renforcé » (association d'un code à usage unique transmis par SMS et d'un mot de passe statique). Cette démarche est particulièrement pertinente en cas de transaction identifiée comme à risque et pour laquelle une réémission récente de carte SIM est un facteur aggravant qui peut justifier un rejet de l'opération par le PSP.

Les échanges intervenus dans le cadre de l'Observatoire ont permis le partage avec les opérateurs et l'AF2M d'un retour d'expérience très positif de plusieurs PSP sur l'efficacité de cet outil pour la prévention en temps réel de la fraude. Des pistes d'enrichissement de l'API ont été soumises pour examen à l'AF2M (par exemple, communication du lieu ou de l'horodatage de réémission de la carte SIM, ou encore prise en compte des portabilités interopérateurs).

2.3.5 Nouveaux axes de réflexion

Les échanges organisés sous l'égide de l'Observatoire ont permis d'identifier des pistes supplémentaires d'amélioration qui permettraient de renforcer l'action conjointe entre le secteur des paiements et celui des télécommunications dans la perspective d'une lutte plus efficace contre la fraude :

- **Définir une procédure de référence permettant d'assurer de manière optimale la fermeture des numéros des faux centres d'appels** déployés par les fraudeurs, quel que soit l'acteur à l'origine de leur détection (particuliers, banques, opérateurs, etc.) ;
- **Conduire une étude d'opportunité sur le développement d'une API de type « *scam signal* »** permettant à un PSP de savoir si son client est en communication téléphonique au moment où il valide un paiement, afin de déceler un éventuel scénario de fraude par manipulation. Si une solution existe aujourd'hui grâce aux systèmes d'exploitation pour terminaux mobiles (l'application bancaire pouvant accéder à cette information), elle est dépendante des droits que l'utilisateur du terminal accorde à l'application bancaire. Or le PSP ne maîtrise pas ce paramètre. Une API multi-opérateurs de ce type, ainsi qu'il en existe notamment au Royaume-Uni, aurait le mérite d'assurer une couverture complète des porteurs.

Sur ces nouveaux sujets, l'Observatoire agit comme catalyseur en assurant l'implication des parties prenantes concernées. Ainsi, sur l'opportunité d'une API *scam signal*, les participants ont été invités à se rapprocher de leurs homologues britanniques pour disposer de retours d'expérience. Sur le blocage des faux centres d'appels, les travaux devraient notamment impliquer la police et la gendarmerie nationales.

2.4 Suivi des actions de l'Observatoire

2.4.1 Suivi des recommandations de l'Observatoire en matière d'authentification forte des paiements par carte

En matière d'authentification forte des paiements par carte, l'Observatoire a publié ses recommandations dans son rapport annuel 2022. L'authentification forte des paiements sur internet a été introduite par la deuxième directive européenne sur les services de paiement (DSP 2). Son déploiement est terminé en France depuis 2021. Au-delà d'assurer le suivi des effets de l'authentification forte sur la fraude *(cf. chapitre 1)*, l'Observatoire reste mobilisé depuis 2022 pour veiller à l'amélioration durable de la sécurité des paiements sur internet. Ainsi, il contribue activement aux travaux réglementaires européens pour garantir l'harmonisation des règles et des pratiques en matière d'authentification forte des paiements, notamment dans la perspective de la révision DSP 2. L'Observatoire intensifie par ailleurs le dialogue et la coopération avec le secteur des télécommunications afin de concourir utilement à une meilleure sécurité des opérations et procédures téléphoniques *(cf. chapitre 2, section 3)*.

2.4.1.1 Aperçu de l'équipement de solutions d'authentification forte des porteurs

Les porteurs de cartes furent essentiellement équipés de solutions d'authentification forte entre 2019 et 2021. À fin 2023, l'Observatoire note que ces solutions n'évoluent qu'à la marge :

- **L'application mobile sécurisée** reste la principale solution d'authentification forte en France : 74 % des porteurs de cartes en sont équipés (contre 72 % en 2022), et elle représente 82 % des paiements authentifiés. Cette solution permet au porteur de s'authentifier avec un code confidentiel ou un facteur biométrique, par l'intermédiaire de l'application bancaire installée sur son téléphone mobile.
- **L'OTP renforcé** combine un code à usage unique (*one-time password*, OTP) reçu par SMS ou par message vocal (serveur vocal interactif, SVI) avec un mot de passe statique connu par le porteur. Depuis sa mise en place, la proportion de porteurs utilisant ce dispositif a décru de deux points pour atteindre 21 % à fin 2023.
- **L'appareil physique** est mis à disposition du porteur par son prestataire de services de paiement. Il peut s'agir d'un générateur de codes doté d'un clavier de saisie, d'une clé USB ou d'un lecteur de QR code. Ce dispositif s'adresse en particulier aux clients qui effectuent leurs achats en ligne systématiquement depuis l'ordinateur de leur domicile. Seulement 3 % des porteurs en étaient équipés à fin 2023. Cette proportion reste stable par rapport à 2022.

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

Si tous ces dispositifs répondent aux exigences réglementaires pour être reconnus comme des solutions d'authentification forte, l'application mobile sécurisée et le boîtier sécurisé sont jugés les plus sûrs. En effet, ces deux équipements reposent respectivement sur un dispositif de jeton d'identification et un dispositif physique, qui ne peuvent pas être récupérés par un fraudeur agissant à distance.

L'Observatoire rappelle toutefois la liberté de choix des utilisateurs dans leur solution d'authentification, l'établissement de paiement devant offrir au moins une méthode alternative et gratuite à l'application mobile sécurisée.

Cette vue d'ensemble ne couvre pas les solutions d'authentification forte déléguées à un tiers, telles que les portefeuilles mobiles ou portefeuilles électroniques [35]. Dans ces situations, comme le rappelle l'Autorité bancaire européenne (ABE) dans un communiqué du 31 janvier 2023, si l'authentification forte est techniquement mise en œuvre par le fournisseur tiers, l'émetteur reste responsable de la conformité réglementaire de la solution. La prestation de services entre l'émetteur et le fournisseur de la solution doit être conforme aux orientations de l'ABE du 25 février 2019 (EBA/GL/2019/02) relatives à l'externalisation. Par ailleurs, l'enregistrement de la carte dans le portefeuille mobile doit faire l'objet d'une authentification forte préalable et systématique sous la responsabilité directe de l'émetteur (*Questions and Answers* – Q&A – n° 5622 de l'ABE).

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

La deuxième directive européenne sur les services de paiement (DSP 2) [36] fixe comme règle générale le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique. Il existe toutefois des exceptions. Il s'agit de certains cas particuliers définis sous forme d'exemptions dans les normes techniques de réglementation (ci-après évoquées par le sigle RTS pour *regulatory technical standards*) [37] relatives à l'authentification forte et aux interfaces d'accès aux comptes.

Toutes les exemptions s'appuient sur des conditions d'application strictement définies, à l'exception de celle visée à l'article 18 des RTS. Celle-ci porte sur les transactions à faible niveau de risque (communément désignée sous le sigle TRA pour *transaction risk analysis*). Elle repose presque entièrement sur l'appréciation de l'éligibilité de la transaction par les prestataires de services de paiement (PSP). Ce processus est donc susceptible d'induire des distorsions dans son application.

Afin d'apporter davantage de lisibilité au bénéfice de l'ensemble des parties prenantes (prestataires de services de paiement, mais aussi prestataires techniques, systèmes de paiement par carte, commerçants et consommateurs), l'Observatoire s'est attaché à formaliser les principes applicables pour la mise en œuvre des exemptions. Il s'est particulièrement focalisé sur l'exemption TRA, en s'appuyant notamment sur les textes réglementaires et les précisions apportées par l'Autorité bancaire européenne dans ses avis [38] et réponses d'interprétation réglementaire (processus de Q&A) [39].

T1 Principes généraux applicables à toutes les exemptions à l'authentification forte hors TRA

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

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

Source : Observatoire de la sécurité des moyens de paiement.

T2 Principes spécifiques applicables à l'exemption TRA

Recommandations	Destinataires
Respect du taux de fraude de référence par le PSP requérant l'exemption Les RTS prévoient qu'un prestataire de services de paiement (PSP) ne peut recourir à l'exemption TRA que si les deux conditions suivantes sont remplies : • il a déployé un mécanisme de contrôle des opérations en temps réel, intégrant les facteurs d'analyse spécifiés dans la réglementation dans une note de risque attribuée à chaque opération individuelle (article 18 des RTS, *Questions and Answers – Q&A – n° 4127*) ; • et si son taux de fraude pour le type d'opération concernée est suffisamment maîtrisé. Les taux de fraude de référence pour accéder à l'exemption TRA sont définis en annexe des RTS.	Prestataires de services de paiement
Taux de fraude à prendre en compte dans le cas des paiements par carte sur internet Dans le cas des transactions par carte sur internet, l'exemption TRA peut être requise par le PSP émetteur (TRA émetteur) ou par le PSP acquéreur (TRA acquéreur). Seul le taux de fraude de référence du PSP demandant le recours à l'exemption TRA doit être pris en considération (Q&A n° 4034 de l'ABE).	Prestataires de services de paiement
Responsabilité en cas de fraude En cas de fraude sur une transaction ayant bénéficié de l'exemption TRA, la réglementation dispose que la responsabilité financière est supportée par le PSP à l'origine de la demande de TRA [a].	Prestataires de services de paiement
Calcul des taux de fraude pour les paiements par carte L'Observatoire invite les PSP fournissant des services d'émission et d'acquisition à calculer des taux de fraude dissociés pour ces deux activités, et à considérer uniquement le taux de fraude relatif à leur rôle dans une transaction donnée.	Prestataires de services de paiement
Suspension du droit d'usage de l'exemption TRA et notification à la Banque de France Conformément à l'article 20 des RTS, les PSP doivent informer immédiatement la Banque de France si : • leur taux de fraude, calculé pour les besoins de la TRA, dépasse l'un des taux de référence fixés par la réglementation, limitant ainsi leur capacité d'usage de l'exemption TRA ; • leur taux de fraude est au contraire redevenu conforme à l'un des taux de référence, libérant de nouveau leur capacité d'usage de l'exemption TRA.	Prestataires de services de paiement

a) Références : articles 73 et 74 de la deuxième directive européenne sur les services de paiement (DSP 2), complétés par Q&A 4042 de l'Autorité bancaire européenne (ABE).
Note : TRA (*transaction risk analysis*), transactions à faible niveau de risque visées à l'article 18 des RTS (*regulatory technical standards*), normes techniques de réglementation émises par l'ABE.
Source : Observatoire de la sécurité des moyens de paiement.

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

Dans un contexte de baisse continue et 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 tirés de cette étude ont été publiés en juillet 2021 dans le rapport annuel de l'Observatoire relatif à l'exercice 2020 [40]. 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.

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

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

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

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

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

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

T3 Vue synthétique de la mise en œuvre des dix recommandations de l'Observatoire sur la fraude au chèque

Recommandations	Niveau de réalisation
Recommandation n° 1 Révision de la collecte statistique de la Banque de France pour améliorer la connaissance des phénomènes de fraude au chèque	Réalisée
Recommandation n° 2 Améliorer les contrôles de la banque du remettant contre les remises frauduleuses	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 3 Soutenir le développement des contrôles du côté de l'établissement tiré	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 4 Protéger les chèques du vol lors de leur acheminement et chez le client	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 5 Simplifier les procédures de mise en opposition pour perte ou vol	Mise en œuvre sous la responsabilité de chaque établissement et sous la supervision de la Banque de France
Recommandation n° 6 Offrir à un plus grand nombre de bénéficiaires de chèques des outils de consultation du Fichier national des chèques irréguliers (FNCI)	En cours de déploiement : nouvelle offre dite « de mandataire spécifique » mise en place par le service Vérifiance-FNCI-Banque de France
Recommandation n° 7 Renforcer la surveillance par la Banque de France de la résistance physique des formules contre la falsification et la contrefaçon	Réalisée
Recommandation n° 8 Assurer l'efficacité du service Vérifiance-FNCI-Banque de France 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

Source : Observatoire de la sécurité des moyens de paiement.

En tenant compte des contrôles déjà effectués et de la politique de risques de chaque établissement, la Banque de France s'assure, dans le cadre de ses actions de surveillance[41], que les établissements bancaires mettent bien en œuvre ces recommandations. Des progrès intéressants ont été relevés par l'Observatoire en 2023, mais des efforts restent néanmoins attendus. Ces efforts doivent porter sur la sécurisation de l'envoi des chéquiers par voie postale ainsi que sur la simplification des procédures de mise en opposition. Ces deux thèmes constitueront les priorités du groupe de travail « chèque » de l'Observatoire au cours de l'année 2024 *(cf. tableau 3)*.

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

Pour lutter plus efficacement contre le vol de chéquiers pendant la phase d'acheminement chez le client, l'Observatoire a appelé les établissements bancaires à i) privilégier le retrait en agence, ii) sécuriser par tout moyen l'acheminement des chéquiers par voie postale et iii) adopter en ce domaine un dispositif de vigilance permanente assurant une réaction rapide. En effet, l'Observatoire estime qu'environ deux tiers des chéquiers sont acheminés par voie postale sous différentes formes d'envoi (lettre simple, lettre suivie et très peu en lettre recommandée avec accusé de réception). C'est pourquoi, à ce stade, l'Observatoire a émis cette recommandation : **les clients doivent garder à tout moment la possibilité de retirer leur chéquier en agence, au moins pour les clients d'un établissement bancaire disposant d'un réseau d'agences. Cette possibilité doit être explicitement proposée aux clients, et il doit être précisé que ce service est gratuit**[42].

En 2023, le groupe de travail « chèque » de l'Observatoire a conduit des travaux plus approfondis sur les pratiques des banques en matière de transmission des chéquiers. La pratique dominante est l'envoi du chéquier par voie postale. Dans certains établissements bancaires, la possibilité pour les clients de retirer leur chéquier en agence bancaire n'est pas mentionnée dans les conditions générales associées aux moyens de paiement, ni parmi

les modalités de remise de chéquier énumérées dans les plaquettes tarifaires.

Afin de sécuriser ces envois par voie postale, quelques établissements bancaires ont toutefois mis en place un mécanisme d'alerte par l'envoi systématique d'un SMS à l'attention de leurs clients afin d'une part, de les prévenir de l'arrivée prochaine de leur chéquier et d'autre part, d'appeler leur vigilance en leur demandant de se manifester s'ils ne l'ont pas reçu dans un délai déterminé. Certaines banques ont annoncé la généralisation d'un tel service d'alerte par SMS au cours de l'année 2024, mais le groupe de travail constate néanmoins que ces dispositifs sont encore insuffisamment déployés. Or un suivi rapproché des envois de chéquiers permettrait d'inscrire sans tarder au Fichier national des chèques irréguliers (FNCI) [43] les chèques perdus ou volés lors de leur acheminement.

Dans ce contexte, **l'Observatoire sera attentif à ce que les banques mettent à jour de manière effective les modalités de délivrance de chéquier. Celles-ci doivent être complétées de la mention « une remise du chéquier en agence » et doivent préciser la gratuité de ce service**.

De même, pour éviter les envois automatiques de chéquiers par voie postale sans avis préalable au destinataire, **l'Observatoire sera également attentif à ce que les banques mettent en œuvre de manière effective un mécanisme d'alerte par l'envoi systématique d'un SMS à leurs clients**.

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

L'Observatoire a rappelé la nécessité d'agir sans tarder pour inscrire au FNCI un chèque perdu ou volé lors de l'acheminement postal ou chez le client (cambriolage par exemple). Une inscription rapide permet à un créancier ayant accès au FNCI d'identifier un chèque volé avant de l'accepter comme moyen de paiement. Mais pour cela, le porteur légitime doit avoir préalablement mis en opposition le chèque volé ou perdu.

Les procédures d'opposition sont encadrées par des dispositions législatives qui se sont traduites, au sein des établissements bancaires, par un formalisme contraignant. Dans la plupart des cas, une démarche d'opposition sur chèque se fait auprès d'un conseiller en agence bancaire ou par téléphone avec confirmation par écrit. Par ailleurs, il est apparu que certaines pratiques tarifaires peuvent être de nature à décourager le client de procéder à une opposition. Conformément à l'article L. 131-35 [44] du Code monétaire et financier, « *le tireur doit immédiatement confirmer son opposition par écrit, quel que soit le support de cet écrit* ». L'Observatoire souligne que lorsque le client fait le choix de faire une opposition par téléphone, la confirmation écrite de l'opposition ne suppose pas nécessairement un courrier. Elle peut se faire par voie électronique, notamment via les espaces de banque en ligne, ce qui permet de raccourcir les délais de mise en opposition et de conserver la trace de la confirmation.

À ce stade, peu de projets de simplification des procédures d'opposition demandée par l'Observatoire à travers les espaces de banques en ligne ou les applications bancaires ont été présentés.

Dans le cadre d'une mise en opposition de chèque ou de chéquier, l'Observatoire sera attentif à la mise en œuvre effective de la simplification des procédures consistant à permettre au client de faire sa démarche à travers les espaces de banques en ligne ou les applications bancaires. Une mise en opposition faite par téléphone devra pouvoir être confirmée par écrit électronique par l'intermédiaire de ces mêmes espaces.

De même, l'Observatoire rappelle que les établissements bancaires doivent prendre en charge la mise en opposition des chéquiers non réceptionnés par les clients, c'est-à-dire que ce service ne doit pas être facturé au client *(cf. recommandation n° 5)*. Sur ce point, l'Observatoire sera attentif à la mise à jour des conditions générales des banques ou des plaquettes tarifaires.

41 Article L. 141-4 du Code monétaire et financier, paragraphe 4 : « *La Banque de France s'assure de la sécurité des moyens de paiement tels que définis à l'article L. 311-3, autres que la monnaie fiduciaire et de la pertinence des normes applicables en la matière. Si elle estime qu'un de ces moyens de paiement présente des garanties insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier. Si ces recommandations n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au* Journal officiel. »

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

43 Le FNCI, tenu par la Banque de France, centralise les coordonnées bancaires de tous les comptes ouverts par des interdits d'émettre des chèques, ainsi que les numéros des chèques mis en opposition (perte, vol, utilisation frauduleuse) ou associés à des comptes clos.

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

En outre, l'Observatoire rappelle que la Banque de France n'exige des établissements bancaires aucun renouvellement périodique des déclarations au FNCI pour des chèques mis en opposition. **Par conséquent, la pratique de certains établissements consistant à limiter l'opposition à un temps réduit (à un ou deux ans), obligeant ainsi les clients à renouveler régulièrement leur procédure d'opposition, et demander le paiement associé, doit être proscrite. Une attention particulière sera portée par l'Observatoire sur ce dernier point.**

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

Pour lutter contre la fraude, l'Observatoire a exprimé la nécessité de promouvoir plus largement la consultation du FNCI. En effet, cette dernière permet au créancier d'identifier un chèque frauduleux avant de l'accepter comme moyen de règlement. Au-delà des chèques rattachés à des comptes clos ou dont le titulaire fait l'objet d'une interdiction d'émettre des chèques, le FNCI recense tous les chèques mis en opposition signalés par le porteur pour perte, vol ou utilisation frauduleuse [45] et tous les faux chèques, correspondant à des cas de contrefaçon, signalés par les établissements bancaires (arrêté du 24 juillet 1992 relatif au traitement automatisé des informations sur la régularité des chèques mis en œuvre par la Banque de France).

Or, la contribution du FNCI, par son utilisation préventive, dans la lutte contre la fraude est encore très insuffisante. En effet, les consultations du FNCI ont permis de déjouer 7,7 % des cas de fraude au chèque en 2022, certes en amélioration par rapport à 2021 (5,7 %), mais ce taux est bien inférieur à celui de 2018 où il était de 17,2 % [46].

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

- D'une part, tout chèque volé doit faire l'objet d'une mise en opposition et celle-ci doit intervenir le plus rapidement possible après le vol. La mise en œuvre de cette recommandation est fondamentale et doit faire l'objet de plans d'action de la part de chacun des acteurs. L'Observatoire constate en effet une nouvelle baisse du volume de mises en opposition des chèques volés, à raison de 2,3 millions en 2023, contre 2,4 en 2022 et 2,6 millions en 2021.
- D'autre part, les personnes acceptant le chèque comme moyen de paiement devraient consulter plus largement le fichier. Même si le nombre de consultations reste toujours très faible en comparaison de l'usage du chèque, l'Observatoire note que le nombre de consultations du FNCI tourne depuis 2020 autour de 4 % du volume de chèques émis (3,18 % en 2023, contre 3,9 % en 2022) [47].

Le FNCI peut être directement consulté à l'aide du service Vérifiance, le service officiel de consultation de la Banque de France. Aux côtés des modalités traditionnelles de consultation par voie informatique ou par téléphone, une offre dite « agile » a été déployée par Vérifiance. Celle-ci est spécialement destinée aux petits accepteurs de chèques, tels que les professionnels, commerçants et artisans. Elle offre notamment la possibilité de disposer du service par une application mobile. D'autres sociétés spécialisées dans la prévention des impayés sur chèques intègrent aussi la consultation du FNCI dans leur offre à destination des accepteurs de chèques.

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

L'Observatoire constate que le déploiement de cette offre, qui répondrait à sa recommandation n° 6, peine à démarrer. Il soutient donc un projet de modification législative élargissant la consultation du FNCI aux présentateurs de chèques que sont les banques. Il précise que cette consultation ne doit pas être obligatoire et ne doit pas engager la responsabilité du présentateur, dans la mesure où c'est le bénéficiaire

45 Articles L. 131-35 du Code monétaire et financier (cf. note de bas de page n° 5) et L. 131-84 « *Le tiré qui a refusé le paiement d'un chèque pour défaut de provision suffisante ou qui a clôturé un compte sur lequel des formules de chèque ont été délivrées ou qui a enregistré une opposition pour perte ou vol de chèque ou de formules de chèque en avise la Banque de France* ».

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

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

du chèque qui prend la décision d'accepter ce moyen de paiement. En effet, à ce jour, la consultation du FNCI n'est ouverte qu'aux seuls bénéficiaires de chèques. Cette évolution, qui répondrait à la recommandation n° 2 de l'Observatoire, permettrait aux banques remettantes de connaître les chèques mis en opposition au moment de la remise ou lors des traitements. Elle répondrait également à la recommandation n° 6 de l'Observatoire puisqu'elle permettrait aux banques de développer et d'offrir à leurs différents clients un outil de vérification des chèques avant acceptation (entreprises, personnes publiques, associations et particuliers).

2.4.2.4 Perspectives pour 2024

En 2024, l'action de ce groupe de travail portera notamment sur :

- la sécurisation des envois de chéquiers par voie postale (par exemple avec des alertes par SMS) ;
- la possibilité de retirer le chéquier en agence sans frais ;
- la simplification des procédures de mise en opposition pour perte ou vol par le biais des espaces de banques en ligne ou des applications bancaires, tout en limitant les pratiques tarifaires excessives qui découragent les mises en opposition de chèques ou de chéquiers ;
- la suppression de la pratique de renouvellement des procédures d'opposition ainsi que la prise en charge par la banque, sans facturation au client, de la mise en opposition d'un chéquier non reçu par le client.

Il sera également procédé au suivi des recommandations n^{os} 3 et 4 relatives au contrôle effectué par les banques.

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

Dans le cadre de ses travaux de veille annuels, l'Observatoire adresse des recommandations à l'attention des acteurs de marché et des utilisateurs. Les principales recommandations émises au cours des dernières années sont récapitulées dans cette section.

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

T4 Recommandations de l'Observatoire relatives aux solutions d'acceptation de paiement sur *smartphone* ou tablette

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

Source : Observatoire de la sécurité des moyens de paiement.

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

Dans son rapport annuel 2016, l'Observatoire avait réalisé une étude sur l'acceptation des paiements par carte en situation de mobilité. Cette étude s'était principalement intéressée à deux solutions d'acceptation : le terminal autonome et le terminal m-POS (*mobile Point of Sale*). Le développement des terminaux m-POS est toutefois resté marginal puisqu'ils ne représentent en 2022 que moins de 1 % du parc de terminaux déployés en France. Les travaux de normalisation, le regain d'intérêt pour ces solutions d'acceptation de la part des acteurs historiques et technologiques issus du secteur mobile, et les évolutions rapides du marché ont incité l'Observatoire à étudier de nouveau en 2022 la sécurité des solutions de paiement en mobilité. Celle-ci a porté plus précisément sur les solutions d'acceptation de paiement sur *smartphone* ou tablette, dite SoftPOS (*Software Point of Sale*). Il s'agit d'une application installée sur un appareil mobile non conçu pour l'acceptation des paiements par carte, de type *smartphone* ou tablette, pourvu de la technologie NFC (*near field communication*, communication en champ proche). L'Observatoire la perçoit en effet comme une alternative aux terminaux de paiement électroniques (TPE) traditionnels pour l'acceptation des paiements par carte, mais aussi comme une solution foncièrement différente puisqu'elle repose entièrement sur du logiciel.

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

Les recommandations relatives à l'identité numérique et la sécurité des paiements ont été publiées dans le rapport annuel 2021. Les phénomènes d'usurpation d'identité, associés parfois à des techniques de fraude documentaire, peuvent mettre à mal la sécurité générale des moyens de paiement. En particulier, l'Observatoire relève et distingue trois phénomènes de fraude : i) les usurpations d'identité au moment de l'entrée en relation, ii) les usurpations de l'identité du payeur au moment de l'acte d'achat et iii) les usurpations de l'identité du bénéficiaire d'un paiement. Certains schémas de fraude reposent toujours sur l'usurpation d'identité de personnes morales. Toutefois, les risques d'usurpation d'identité portent principalement sur l'identité de personnes physiques.

En cherchant à lutter contre les risques d'usurpation d'identité dans la sphère numérique, les solutions d'identité numérique et les services de confiance sécurisés, comme la signature et le cachet électroniques, peuvent aider à améliorer la sécurité générale des moyens de paiement. Avec la publication en 2021 du référentiel d'exigences destiné aux prestataires de vérification d'identité à distance (PVID) et le processus de révision en cours de la réglementation européenne eIDAS sur l'identification électronique et les services de confiance [48], l'Observatoire invite les acteurs du paiement à lutter contre les usurpations d'identité en recourant aux services d'identité numérique conformes aux exigences PVID ou eIDAS.

T5 Recommandations de l'Observatoire relatives à l'identité numérique et la sécurité des paiements

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

Source : Observatoire de la sécurité des moyens de paiement.

2.4.3.3 Recommandations relatives à la sécurité des paiements en temps réel

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

Dans un contexte de développement rapide du virement instantané, qui pourrait progressivement se substituer au virement classique, voire à d'autres moyens de paiement, l'Observatoire reste particulièrement attentif à la sécurité des paiements en temps réel. En 2023, le virement instantané représentait 6,4 % du nombre total de virements et 0,6 % des montants échangés par virement (hors virements de gros montant traités par les systèmes de paiement de montant élevé). Le nombre de virements instantanés a encore progressé de 84 % par rapport à 2022. L'augmentation devrait se poursuivre dans les prochaines années, soutenue par les stratégies nationales et européennes pour les moyens de paiement et par les initiatives législatives des pouvoirs publics européens. En matière de sécurité, l'Observatoire note que la fraude sur les paiements en temps réel augmente moins vite que les flux, si bien que le taux de fraude sur les virements instantanés a baissé depuis 2021 pour atteindre 0,04 % en 2023. Avec 69 millions d'euros de fraude sur le virement instantané en 2023, soit près de 22 % du total de la fraude recensée sur les virements, l'Observatoire renouvelle son appel vers les industriels des paiements à poursuivre leurs efforts et leurs investissements pour renforcer la sécurité des virements instantanés. De plus, l'Observatoire réitère ses recommandations visant à assurer un développement rapide et sécurisé de ce nouveau moyen de paiement.

48 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS – *Electronic IDentification Authentication and trust Services*).

T6 Recommandations de l'Observatoire relatives à la sécurité des paiements en temps réel

Recommandations	Destinataires
Mettre en œuvre, dans les conditions fixées par la DSP 2, l'authentification forte des utilisateurs pour l'autorisation des paiements en temps réel et pour toute opération sensible périphérique (ajout d'un bénéficiaire, changement de coordonnées, etc.).	Prestataires de services de paiement (émetteurs)
Améliorer en continu les outils de prévention de la fraude en temps réel, notamment au moyen de technologies fondées sur l'apprentissage automatique, pour améliorer la performance des systèmes d'analyse de risques déployés.	Prestataires de services de paiement (émetteurs et receveurs)
Faire usage si nécessaire des mesures de paramétrage des droits, de types plafonds et limitations, pour limiter les préjudices d'un développement incontrôlé de la fraude.	Prestataires de services de paiement (émetteurs)
Identifier les opérations atypiques en réception, notamment quand celles-ci précèdent d'autres opérations en sortie.	Prestataires de services de paiement (receveurs)
Prêter une attention particulière, avant de valider l'ordre de paiement, à l'origine de la demande et l'identité de l'interlocuteur, et vérifier les coordonnées bancaires du bénéficiaire.	Utilisateurs
Saisir des données bancaires exclusivement sur des sites internet ou des applications mobiles réputés fiables et de confiance ; privilégier les sites et applications référencés et s'y connecter directement en considérant avec la plus grande prudence les liens reçus par des moyens de communication peu sécurisés, tels que les SMS et courriels.	Utilisateurs
Avertir, aussi rapidement que possible après l'exécution du paiement, son établissement bancaire de toute opération suspecte non autorisée ou frauduleuse.	Utilisateurs
Soutenir la vigilance des utilisateurs par la mise à disposition d'outils de confirmation du bénéficiaire et d'information active et en temps réel des opérations réalisées sur leur compte.	Prestataires de services de paiement

Source : Observatoire de la sécurité des moyens de paiement.

2.4.3.4 Recommandations relatives à la sécurité des données de paiement

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

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

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

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

T7 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 son fournisseur de services de paiement ou dont le fournisseur est dûment autorisé en France pour la prestation de services de paiement (c'est-à-dire présent dans l'annuaire Regafi ou dans le registre de l'Autorité bancaire européenne).	Utilisateurs
S'informer régulièrement sur les risques numériques et leurs évolutions au moyen, par exemple, du site du gouvernement *www.cybermalveillance.gouv.fr*	Utilisateurs

Note : DSP 2, deuxième directive européenne sur les services de paiement.

Source : Observatoire de la sécurité des moyens de paiement.

2.4.3.5 Recommandations relatives à la sécurité des paiements par mobile

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

Le paiement par carte au point de vente par l'intermédiaire d'une solution mobile a connu un net développement ces trois dernières années, porté par la crise sanitaire et la possibilité de payer sans contact dans la limite de cinquante euros. Le nombre de paiements de ce type a ainsi plus que doublé chaque année entre 2019 et 2023 (+ 141 % par an en moyenne), pour représenter, en 2023, 10 % du nombre de paiements par carte de proximité et 15 % 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 s'établissait à 0,061 % en 2022, s'est fortement contracté en 2023 pour atteindre 0,021 %. Cela traduit un renforcement des outils de maîtrise du risque de fraude, notamment au moment de l'enrôlement de l'utilisateur dans la solution, que l'Observatoire appelle à poursuivre. Pour éviter les risques d'enrôlement de numéros de carte usurpés par les fraudeurs dans ce type de solution, la mise en œuvre d'une authentification forte du porteur, comme prévu par la DSP 2 au titre des opérations sensibles, est impérative.

T8 Recommandations de l'Observatoire relatives à la sécurité des paiements par mobile

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

Source : Observatoire de la sécurité des moyens de paiement.

2.4.4 Rappel des recommandations de l'Observatoire sur les modalités de remboursement des opérations de paiement frauduleuses

L'utilisation de mécanismes d'authentification forte du payeur, qui s'est généralisée depuis 2019 en application de la deuxième directive européenne sur les services de paiement (DSP 2 [49]), a permis de réduire significativement la fraude aux paiements sur internet. La veille assurée par l'Observatoire montre ainsi que le taux de fraude sur les paiements par carte sur internet a baissé de 35 % entre 2019 et 2023. L'Observatoire constate néanmoins que les fraudeurs cherchent à contourner l'authentification forte en développant de nouvelles techniques de fraude, qui s'appuient notamment sur la manipulation des victimes.

Face au développement de ces nouveaux procédés frauduleux qui touchent tous les profils de clients, l'Observatoire a souhaité apporter des précisions sur le droit à remboursement prévu par la DSP 2 en cas de fraude. L'Observatoire a publié à cette fin – le 16 mai 2023 – un ensemble de treize recommandations qui visent à améliorer les démarches de remboursement des victimes de fraude, tout en rappelant la responsabilité des utilisateurs dans la sécurité de leurs moyens de paiement.

Un an après la publication de ces recommandations, les engagements pris par les prestataires de services de paiement doivent avoir été suivis d'une mise en œuvre effective. L'Observatoire s'est engagé à procéder à un bilan de ces recommandations dont les conclusions seront rendues fin 2024. Cette démarche va s'appuyer sur des enquêtes réalisées par l'Autorité de contrôle prudentiel et de résolution (ACPR) afin d'évaluer le niveau de mise en œuvre des recommandations.

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

T9 Recommandations générales de l'Observatoire applicables au traitement des contestations d'opérations de paiement

Recommandations	Destinataires
Recommandation n° 1 : délai maximum des investigations Les prestataires de services de paiement sont invités à mettre en œuvre les investigations dès la réception de la contestation, en prenant en compte les éventuels éléments de description fournis par l'utilisateur (tels que précisés par la recommandation n° 8), et à en limiter la durée à 30 jours, sauf situation exceptionnelle.	Prestataires de services de paiement
Recommandation n° 2 : information du client en cas de reprise des fonds En cas de remboursement susceptible de donner lieu à une reprise de fonds ultérieure en fonction du résultat des investigations engagées, le prestataire de services de paiement informe son client de cette éventualité au moment du remboursement, et veille à ne pas procéder à la reprise des fonds dans un délai excédant 30 jours à compter de la date à laquelle le remboursement a été effectué, sauf situation exceptionnelle.	Prestataires de services de paiement
Recommandation n° 3 : justification du refus de remboursement Lorsque le prestataire de services de paiement refuse le remboursement ou procède à la reprise des fonds, il veille à informer le client de cette décision et lui en communique le motif, en prenant soin le cas échéant de joindre les éléments qui la justifient (par exemple, mandat de prélèvement, éléments transmis par le commerçant ou preuve de négligence grave). En outre, il détaille dans cette même communication les modalités suivant lesquelles une réclamation peut être déposée.	Prestataires de services de paiement

Source : Observatoire de la sécurité des moyens de paiement.

2.4.4.2 Recommandations applicables au traitement de cas spécifiques

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

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

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

T9 *bis* Recommandations de l'Observatoire applicables au traitement de cas spécifiques

Recommandations	Destinataires
Recommandation n° 4 : principes applicables aux opérations sans authentification forte Lorsqu'un utilisateur du service de paiement conteste une ou plusieurs opérations qu'il nie avoir autorisées et que ces opérations n'ont pas été authentifiées de manière forte, le prestataire de services de paiement du payeur rembourse sans délai [a] le montant de ces opérations, sauf lorsqu'il a de bonnes raisons de soupçonner une fraude de l'utilisateur lui-même. Ce soupçon de fraude ne peut résulter de la seule utilisation de l'instrument de paiement. Ce remboursement immédiat ne fait pas obstacle à la reprise ultérieure des fonds lorsque le prestataire de services de paiement réunit des éléments prouvant soit que l'opération a été autorisée (par exemple, par l'existence d'un mandat de prélèvement SEPA [b], soit qu'une fraude a été commise par l'utilisateur lui-même. En revanche, la négligence, même grave, commise par le payeur ne peut fonder le refus de remboursement d'une opération qui n'a pas été authentifiée de manière forte. Dans le cas particulier des paiements initiés par le bénéficiaire (prélèvement ou paiement par carte de type MIT – *Merchant Initiated Transaction*), le payeur bénéficie en outre d'un droit à remboursement immédiat dans un délai de huit semaines qui suit le débit en compte : • pour le prélèvement, ce remboursement est sans condition, indépendamment de l'existence ou non d'un mandat de prélèvement ; • pour le paiement par carte ordonné par le bénéficiaire, si l'autorisation donnée n'indiquait pas le montant exact de l'opération de paiement et si le montant de l'opération dépassait le montant auquel le payeur pouvait raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances propres à l'opération. *Références : articles L. 133-19, L. 133-18, L. 133-25 et L. 133-25-1 du Code monétaire et financier (CMF) et SEPA Direct Debit Core Scheme Rulebook V1.1 section 4.3.4.*	Prestataires de services de paiement
Recommandation n° 5 : principes applicables aux opérations réalisées avec une application mobile se substituant à l'instrument de paiement Lorsque l'utilisateur du service de paiement conteste une opération de paiement qu'il nie avoir autorisée et qui a été réalisée au moyen d'une solution mobile pour laquelle l'enrôlement de l'instrument de paiement n'a pas donné lieu à authentification forte, le prestataire de services de paiement du payeur procède sans délai [c] au remboursement du montant de cette opération. *Références : article L. 133-18 du CMF et Autorité bancaire européenne (ABE), Question and Answer – Q&A – 2021_6141.*	Prestataires de services de paiement

a) La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la réclamation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteur, etc.).
b) Sauf pour les prélèvements contestés dans les huit semaines suivant le débit du compte, pour lesquels le payeur dispose d'un droit au remboursement inconditionnel. SEPA – *Single Euro Payment Area*, espace unique de paiement en euros.
c) La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la réclamation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteur, etc.).

…/…

T9 *bis* Recommandations de l'Observatoire applicables au traitement de cas spécifiques (suite)

Recommandations	Destinataires
Recommandation n° 6 : principes applicables aux opérations authentifiées de manière forte Lorsqu'un client conteste une opération de paiement qu'il nie avoir autorisée et que cette opération a été authentifiée de manière forte, le prestataire de services de paiement doit procéder dans le délai d'un jour ouvré à une première analyse de cette opération. Cette analyse vise à apprécier, en prenant en compte les trois familles de paramètres mentionnées ci-après, si l'utilisateur est susceptible d'avoir consenti à l'opération ou s'il s'agit d'une opération non autorisée : • les paramètres techniques associés à l'opération (tels que l'origine de la transaction, le terminal utilisé pour l'achat ou la connexion à la banque en ligne et la localisation géographique), pour évaluer la possibilité que l'utilisateur en soit à l'origine ; • les modalités de l'authentification forte mise en œuvre (telles que le type de solution, l'intégrité des facteurs d'authentification et du canal de communication, la preuve d'une utilisation précédente de la solution par l'utilisateur ou au contraire le caractère récent de l'enrôlement), pour s'assurer du rôle effectif de l'utilisateur ; • les éléments de contexte dont il dispose tels que : les informations délivrées à l'utilisateur lors de l'authentification (cf. recommandation n° 11), les éventuelles alertes liées à l'opération et adressées à l'utilisateur par différents canaux de communication et les éléments rapportés par l'utilisateur (cf. recommandation n° 8), tels que les procédés manipulatoires auxquels il a pu être confronté. À l'issue de cette première analyse : • soit le prestataire de services de paiement constate que l'opération n'a pas été autorisée ou a un doute sur le consentement donné à l'opération, auquel cas il procède sans délai [d)] au remboursement de la transaction ; • soit le prestataire de services de paiement dispose de bonnes raisons de soupçonner une fraude de l'utilisateur [e)] qu'il communique à la Banque de France, auquel cas il peut refuser de rembourser immédiatement la transaction dans les conditions prévues à la recommandation n° 3 ; • soit le prestataire de services de paiement a suffisamment d'éléments de preuve pour considérer que l'opération a été autorisée par l'utilisateur [f)], que ce dernier a été gravement négligent [g)] ou qu'il n'a pas satisfait intentionnellement à ses obligations, auquel cas il peut refuser le remboursement de l'opération contestée au client, dans les conditions prévues à la recommandation n° 3. Dans les deux premiers cas, et à partir notamment des mêmes critères susmentionnés et des éléments nouveaux qu'aurait pu rapporter l'utilisateur, le prestataire de services de paiement est invité à poursuivre si nécessaire les investigations dans les conditions prévues aux recommandations n° 1 à 3 en vue de déterminer le droit à remboursement de l'utilisateur. *Références : articles L. 133-18, L. 133-19 et L. 133-23 du CMF.*	Prestataires de services de paiement

d) La réglementation précise que le remboursement doit être réalisé immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant la date de dépôt de la réclamation, et doit inclure les éventuels frais supplémentaires induits à titre transitoire par la comptabilisation de l'opération frauduleuse (frais de découverts, intérêts débiteurs, etc.).
e) Au sens de l'article L. 133-18 du Code monétaire et financier.
f) Au sens de l'article L. 133-6 du Code monétaire et financier.
g) Au sens des articles L.133-19 et L.133-23 du Code monétaire et financier.

Source : Observatoire de la sécurité des moyens de paiement.

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

T9 *ter* Recommandations de l'Observatoire à l'attention des consommateurs et de leurs représentants

Recommandations	Destinataires
Recommandation n° 7 : bonnes pratiques pour la sécurité des moyens de paiement Les consommateurs doivent s'efforcer de rester vigilants quant à la préservation de la protection des données de sécurité associées à un instrument de paiement (mot de passe, code confidentiel, cryptogramme, etc.), en respectant les bonnes pratiques en la matière : • ne jamais communiquer ces données à un tiers ; • ne pas conserver ces données de sécurité sur quelque support que ce soit, physique (carnet, Post-it, etc.) ou informatique (messagerie électronique, disque dur, portable, etc.) ; • ne pas répondre aux sollicitations de personnes se présentant comme des collaborateurs des prestataires de services de paiement (conseillers bancaires, service de lutte contre la fraude, etc.). Toujours utiliser un canal sécurisé et connu pour établir un contact avec son prestataire de services de paiement. Ne jamais ouvrir un lien reçu par messagerie électronique ou SMS dont l'origine n'est pas sûre ; • ne jamais confier son instrument de paiement à une tierce personne (proche, coursier, etc.) ; • être attentif aux communications de son prestataire de services de paiement et des autorités en matière de sécurité. Il est rappelé que le personnel du prestataire de services de paiement ne sera jamais amené à demander ces informations en cas d'appel de son client et n'en a pas besoin pour annuler une opération frauduleuse. En outre, les consommateurs sont invités à privilégier la solution d'authentification la plus sûre proposée par leur prestataire de services de paiement, dès lors qu'ils sont en mesure de l'utiliser. Il s'agit généralement des solutions reposant sur un élément matériel robuste comme l'application bancaire sur un ***smartphone*** (solution majoritaire en France) ou un dispositif physique autonome mis à disposition par le prestataire de services de paiement (lecteur de carte, clé USB, etc.). *Références : article L. 133-16 du Code monétaire et financier (CMF).*	Consommateurs
Recommandation n° 8 : devoir de transparence de la part des victimes de fraude Lors des démarches de déclaration auprès de leur prestataire de services de paiement ou des forces de l'ordre (qu'il s'agisse des démarches en ligne sur les plateformes Perceval ou Thésée [a)], ou du dépôt de plainte au commissariat de police ou dans une unité de gendarmerie), les consommateurs et leurs représentants veillent à fournir l'ensemble des éléments dont ils disposent concernant la fraude dont ils ont été victimes. Les utilisateurs veillent notamment à fournir tous les éléments connus sur : • la nature et le contexte de l'opération : par exemple leur niveau de connaissance du bénéficiaire, les procédés techniques ou manipulatoires que le fraudeur est supposé avoir mobilisés, l'instrument et les terminaux utilisés pour l'opération de paiement, les messages ou appels reçus, les actions réalisées sous le coup d'une manipulation par le fraudeur, etc. ; • les actions entreprises une fois la fraude découverte : par exemple le blocage de l'instrument, le signalement ou le dépôt de plainte auprès des forces de l'ordre, etc.	Consommateurs

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

Source : Observatoire de la sécurité des moyens de paiement.

2.4.4.4 Recommandations visant à prévenir la fraude

T9 *quater* Recommandations de l'Observatoire visant à prévenir la fraude

Recommandations	Destinataires
Recommandation n° 9 : application d'une authentification forte lors de l'accès à la banque en ligne depuis un nouveau point d'accès à internet ou un nouveau terminal Les prestataires de services de paiement sont invités à exiger une authentification forte en cas de consultation des comptes depuis la banque en ligne ou l'application mobile depuis un terminal ou un point d'accès à internet qui n'a pas été précédemment utilisé par le client.	Prestataires de services de paiement
Recommandation n° 10 : modalités d'enregistrement des IBAN[a] bénéficiaires de virements Les prestataires de services de paiement sont invités à indiquer clairement, à chaque ajout d'un bénéficiaire de virement, si un contrôle de concordance entre IBAN et nom du bénéficiaire a été mis en œuvre. À défaut, il doit être précisé à l'utilisateur que le champ « Nom du bénéficiaire » est exclusivement destiné à faciliter le suivi des opérations par le client qui émet des virements, et que son contenu ne fait l'objet d'aucun contrôle de concordance avec l'identité du titulaire de l'IBAN du bénéficiaire. Par ailleurs, les prestataires de services de paiement établis en France sont encouragés à explorer par anticipation la possibilité d'implémenter au plus tôt un service de confirmation du bénéficiaire comme envisagé par la Commission européenne dans sa proposition de révision du règlement SEPA[b].	Prestataires de services de paiement
Recommandation n° 11 : information et options présentées à l'utilisateur au moment de l'authentification forte Les prestataires de services de paiement veillent à présenter à l'utilisateur, à chaque étape du processus d'authentification, une information explicite quant à la nature de l'opération, et mentionnant notamment le montant, le bénéficiaire, le caractère unique ou récurrent de l'opération, la périodicité dans le cas d'une opération récurrente ainsi que le caractère irrévocable de la validation de l'ordre de paiement. Dans le cas d'un premier virement vers un compte donné, lorsque la concordance entre l'identité du bénéficiaire et l'IBAN fournis n'a pas fait l'objet d'un contrôle, le parcours d'authentification le rappelle explicitement. Par ailleurs, les prestataires de services de paiement veillent à ce que le parcours d'authentification propose de manière explicite une option permettant de refuser l'opération.	Prestataires de services de paiement
Recommandation n° 12 : simplicité d'accès aux procédures de blocage des instruments de paiement Les prestataires de services de paiement mettent à disposition de leurs utilisateurs des mécanismes de blocage pour chacun des instruments de paiement et veillent à ce qu'ils soient facilement accessibles, gratuits et utilisables à tout moment. *Références : articles L. 133-15 et L. 133-17 du Code monétaire et financier (CMF).*	Prestataires de services de paiement
Recommandation n° 13 : rôle des fournisseurs de services et technologies de l'information Les acteurs du secteur des technologies de l'information (opérateurs de téléphonie, hébergeurs de contenu, éditeurs de sites de référencement, moteurs de recherche, fournisseurs de services de messagerie, etc.) veillent à protéger les utilisateurs contre les risques d'usurpation d'identité et d'atteinte à l'intégrité et la confidentialité de leurs données. Ils œuvrent à empêcher l'utilisation de techniques frauduleuses telles que l'hameçonnage, le *spoofing* ou le *SIM swapping*.	Fournisseurs de services et technologies de l'information

a) IBAN, *international bank account number*.

b) Proposition du 26 octobre 2022 (2022/0341 (COD)) visant à rendre les paiements instantanés en euros accessibles à tous les particuliers et à toutes les entreprises qui possèdent un compte bancaire dans l'Union européenne ou dans un pays de l'Espace économique européen. SEPA – *Single Euro Payment Area*, espace unique de paiement en euros.

Source : Observatoire de la sécurité des moyens de paiement.

❷ Les retours de fonds en cas de fraude dans le contexte d'un virement SEPA

- L'établissement du donneur d'ordre émet un rappel de fond (*recall*) à destination de l'établissement du bénéficiaire lorsqu'une fraude est constatée sur un virement alors que ce dernier l'a déjà exécuté (c'est-à-dire remis les fonds au bénéficiaire).
- La demande de *recall* doit être faite dans les treize mois suivant l'opération.
- Une fois la demande reçue, l'établissement du bénéficiaire dispose de quinze jours pour répondre.
- Le retour des fonds n'est cependant pas garanti :
  - dans certains pays, comme la France, la banque du bénéficiaire doit avoir l'accord de son client pour débiter le compte de la somme rappelée ;
  - le compte à débiter doit disposer de la provision nécessaire, ce qui n'est plus le cas si le fraudeur a déjà fait transiter les fonds vers un autre compte.

❸ Quelques exemples de communication de sensibilisation à la fraude à destination du public

- Les mises en garde des établissements financiers adressées à leurs clients (générales ou ciblées), par courriel,sur leurs site web et application bancaire ;
- la campagne de prévention diffusée en 2023 par la Fédération bancaire française (« Ne donnez jamais ces données », à propos des codes, mots de passe et identifiants bancaires) ;
- le compte Instagram « Fraude Fight Club » créé conjointement par les banques, le groupement d'intérêt public Action contre la cybermalveillance, la Banque de France et plusieurs entreprises du secteur privé ;
- le communiqué de presse de l'Association française des sociétés financières spécifique aux arnaques aux faux courtiers ;
- les divers articles et communiqués relatifs aux techniques de manipulation exercée par les fraudeurs publiés par l'Autorité de contrôle prudentiel et de résolution sur le site internet Assurance Banque Épargne-Info Service ;
- les articles à disposition sur les sites internet des associations de protection des consommateurs ;
- la publication du rapport de l'OSMP, ainsi que les diverses interventions dans les médias sur le sujet.

❹ Récapitulatif des services de signalement d'e-mail, site ou SMS suspects

(Source : *www.cybermalveillance.gouv.fr*)

- **Cybermalveillance.gouv.fr :** plateforme de sensibilisation, assistance aux victimes de cybermalveillance et mise en relation avec des experts, pour les particuliers, les entreprises, les associations, les collectivités et les administrations.
- **Signal Spam :** signalement de mails suspects, soit par un module de signalement dédié (extension du navigateur web ou client de messagerie électronique), soit directement sur le site.
- **Phishing Initiative :** vérification de l'adresse d'un site suspect, incluant le cas échéant le blocage du site et sa demande de suppression.
- **33700 :** plateforme internet et numéro de téléphone de signalement de SMS/MMS suspects.
- Déclaration auprès de la société dont le site a été usurpé.

5 Glossaire

PSP : prestataire de services de paiement.

PSP acquéreur : PSP du bénéficiaire, c'est-à-dire du commerçant qui accepte des paiements par carte.

PSP émetteur : PSP qui émet la carte, c'est-à-dire PSP du payeur.

CIT (*Customer Initiated Transaction*) : opération initiée par le client. Cette catégorie couvre la majorité des paiements par carte effectués directement par le porteur de la carte sur les sites de e-commerce.

MIT (*Merchant Initiated Transaction*) : opération initiée par le commerçant. Cette catégorie correspond notamment aux paiements dont le montant exact n'est pas connu à l'avance, aux paiements récurrents (abonnements) ou encore aux paiements fractionnés (paiement en plusieurs fois), selon un fonctionnement comparable à celui d'un prélèvement SEPA : le client souscrit à un mandat, validé par authentification forte, par lequel il autorise le commerçant à initier un ou plusieurs paiements ultérieurs dans des conditions prédéfinies (montant unitaire, plafond, périodicité, etc.).

MOTO (*Mail Order, Telephone Order*) : paiements pour lesquels le porteur de la carte communique au commerçant par téléphone, courrier postal, courriel, télécopie (etc.), le numéro de sa carte et la date d'expiration, données que le commerçant saisit ensuite sur son terminal de paiement électronique. Ce mode de paiement est destiné au paiement d'achats effectués par téléphone (par exemple, réservation de voyage ou d'hôtel) ou par l'envoi d'un bon de commande sur support papier.

Chaînage : référence cryptographique d'authentification, sous forme d'une chaîne de caractères alphanumériques, communiquée par le PSP émetteur à la suite de l'authentification forte du client lors de la validation du mandat MIT. Cette référence permet aux PSP d'identifier le mandat authentifié fortement au titre duquel un ou plusieurs paiements sont ensuite émis par le commerçant.

***Soft decline* :** mécanisme par lequel le PSP acquéreur ou émetteur rejette un paiement par carte avec demande d'exemption tout en permettant au commerçant (ou à son prestataire d'acceptation technique) de présenter à nouveau la demande de paiement via le protocole 3-D Secure (opération dite de « *retry* »). Le rejet est transparent pour le porteur de la carte qui n'a pas à saisir de nouveau ses données de paiement ; en revanche, le porteur devra valider le paiement par authentification forte [1].

Vélocité : montant cumulé des paiements effectués à l'aide d'une même carte auprès d'un même commerçant durant la même période glissante de référence (24 heures).

1 Cf. sur le sujet la note « Trajectoire de mise en œuvre du *soft decline* pour finalisation du plan de migration pour l'authentification forte des paiements en ligne » publiée par l'Observatoire le 18 février 2021 : *https://abc-economie.banque-france.fr/*

❻ Liste des exclusions par secteur d'activité au mécanisme de limitation de la vélocité

Une liste des activités exclues de l'application de la limite de vélocité est définie, pour chaque catégorie de paiements (paiements MOTO, *Mail Order, Telephone Order*, réalisés par courrier, postal ou électronique [courriel], ou par téléphone/télécopie, et paiements par internet hors 3-D Secure), en fonction du code de catégorie de marchand (MCC, *Merchant Category Code*) attribué au commerçant.

La liste *infra* initialement définie pourra être modifiée, en fonction des taux de fraude et cas d'usage observés, par le groupe de travail « authentification forte » de l'Observatoire. La liste en vigueur sera disponible sur le site internet de l'Observatoire.

Paiements par internet hors 3-D Secure

8398 Œuvres sociales et caritatives

Paiements MOTO

1771 Béton
2741 Presse
3000 à 3299 Compagnies aériennes [1]
3350 à 3449 Entreprises de location de voitures [1]
3500 à 3999 Chaînes hôtelières [1]
4011 Transport ferroviaire
4112 Transport ferroviaire de passagers
4411 Transports maritimes
4511 Transports aériens
4722 Agences de voyages
4814 Services de télécommunication
4900 Services électriques, gaz, eau, sanitaire
5965 Vente sur catalogue
6010 Distribution de crédit
6012 Institutions financières
6300 Assurances
6513 Location de logement (bailleurs sociaux)
7011 Hébergement, hôtels, motels
7032 Colonies et camps de vacances ou activités sportives
7033 Autre hébergement touristique
7322 Recouvrement de créances
7512 Location et location bail de voitures
8111 Services juridiques et avocats
8398 Œuvres sociales et caritatives
9405 Achats entre agences d'une même administration

1 MCC attribués individuellement.

3

L'INFORMATIQUE QUANTIQUE ET LA SÉCURITÉ DES SYSTÈMES DE PAIEMENT PAR CARTE BANCAIRE

L'informatique quantique offre des perspectives prometteuses en finance, logistique, météorologie, chimie, et dans bien d'autres domaines. Mais **un cas d'usage bien identifié est problématique à un horizon de dix à vingt ans : le déchiffrement des communications électroniques sécurisées, dont les paiements**. Il s'agit d'une menace sérieuse vis-à-vis de la sécurité nationale qui est déjà prise en considération par les autorités publiques (le Mémorandum de sécurité nationale américain de mai 2022 et la loi française de programmation militaire d'août 2023). Le secteur des paiements doit s'en saisir, dès maintenant et à haut niveau, en raison des cycles de vie des matériels et logiciels de paiement par carte (puces, terminaux de paiement électronique [TPE], serveurs, etc.).

La confidentialité et l'intégrité des paiements par carte sont assurées par deux types d'algorithmes :

- Les algorithmes de chiffrement asymétrique (RSA, ECC, etc.) permettant l'authentification des appareils (cartes, TPE, etc.) et des serveurs entre eux, ainsi que l'échange de clés de chiffrement symétrique. Leur niveau de sécurité deviendrait nul avec l'avènement de l'ordinateur quantique (Shor, 1995) ;
- Les algorithmes de chiffrement symétrique (AES, Triple DES, etc.) permettant le chiffrement des données à froid ou en circulation. Leur niveau de sécurité exprimé en bits serait divisé par deux (Grover, 1996).

Cette étude propose une cartographie des principaux algorithmes implémentés dans le dispositif de paiement par carte et une analyse de leur exposition aux risques de la « menace quantique ». Sans action de résilience pour faire évoluer les algorithmes de chiffrement et de signature des systèmes de paiement par carte et ainsi renforcer leur résistance à la puissance de calcul des futurs ordinateurs quantiques, les risques à termes les plus importants sont :

- Le vol de données privées, voire confidentielles, chez les marchands piratés, soulevant des problématiques relatives au renseignement et à l'intelligence économique ;
- La génération de paiements frauduleux par la fabrication de *Yes Card* pour les paiements dits « hors ligne » ;
- La perte de confiance dans les infrastructures de paiement. Les schémas de cartes et les institutions bancaires émettrices ne seraient plus maîtres de leur politique de certification des cartes de paiement : à chaque fois qu'une clé de haut niveau sera cassée, un volume important de cartes devra être rappelé et réémis ;
- La simple prise de conscience par le public de ces risques pourrait provoquer une crise de confiance généralisée, menaçant ainsi la stabilité de nos économies.

L'étude montre que des solutions techniques existent, mais que leur mise en œuvre n'est pas triviale dans le cas des algorithmes asymétriques. L'OSMP recommande donc dès à présent aux acteurs des paiements de :

- **Inventorier** les différents dispositifs de sécurité de leurs systèmes d'information ;
- **Hiérarchiser** les données selon leur degré de sensibilité ;
- **Expérimenter** l'implémentation d'algorithmes asymétriques basée sur des systèmes hybrides et crypto-agiles ;
- **Constituer une feuille de route** validée à haut niveau ;
- **Sensibiliser les autorités de standardisation** qui définissent la sécurité des protocoles de paiement afin d'arrêter des choix en matière d'hybridation et de crypto-agilité et de poser des jalons ;
- **Œuvrer à la création d'un groupe de travail pérenne de haut niveau**, idéalement à l'échelle européenne, regroupant notamment les grandes institutions de paiement, les autorités publiques de supervision et de standardisation.

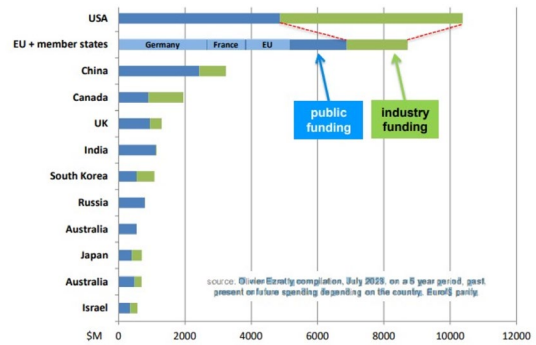
3.1 Introduction

L'informatique quantique permettra des avancées technologiques dans de nombreux domaines scientifiques. Mais elle pourrait aussi dégrader les dispositifs de sécurité informatique, si certaines informations chiffrées ne sont pas protégées de manière appropriée. L'objet de ce chapitre est d'initier une évaluation des risques que les progrès de l'informatique quantique, par ses capacités de calcul en matière de déchiffrement, pourraient faire peser sur l'industrie des paiements électroniques.

Formulé par Feyman en 1982, le principe du calculateur quantique repose sur les lois de la physique quantique. Notamment, la loi de superposition d'états permet de remplacer la notion de bit, qui dans l'informatique classique prend les valeurs booléennes de 0 et 1, par la notion de qubit dont la valeur est comparable à une sorte de probabilité d'être entre 0 et 1. Les qubits sont manipulés par des opérateurs quantiques, nommés portes quantiques. Leur jeu et l'optimisation des rejeux permettent d'accroître de façon exponentielle l'efficacité de calculs d'optimisation, que l'on retrouve dans des domaines aussi variés que la météorologie, la biochimie, la finance, la logistique, etc.

Toutefois, la technologie du calcul quantique, souvent désignée par les termes « informatique quantique », n'en est encore qu'à ses débuts. En effet, les machines quantiques actuellement opérationnelles n'offrent qu'un nombre limité de qubits exposés à une probabilité non négligeable d'erreurs, tenant tant aux principes mêmes de la physique quantique, qu'aux problèmes de maîtrise de l'environnement de la machine qui doit rester totalement isolée de toute influence extérieure. De nombreuses pistes de développement technologique sont explorées : circuits supraconducteurs, atomes froids, silicium, etc. Les industriels de l'informatique et des centaines de startups, notamment françaises, sont entrés dans la course en concurrençant directement les GAFAM [1]. Depuis 2020, au niveau mondial, les investissements privés dans les startups ont explosé pour dépasser les deux milliards de dollars sur les deux dernières années. Parallèlement, les autorités publiques de toutes les nations avancées, États-Unis en tête, mais aussi la Chine, l'Inde et la Russie, ont lancé des programmes de soutien massifs au développement de cette technologie. En 2021, le gouvernement français a élaboré un plan d'investissement de 1,8 milliard d'euros sur cinq ans.

G1 Investissements publics et privés dans la recherche sur le calcul quantique consolidés sur les cinq dernières années
(en millions de dollars américains)



Notes : Travail de consolidation des budgets publics (*public funding*) comme privés (*industry funding*) dont le périmètre déjà très étendu ne peut garantir une exhaustivité totale. Juillet 2023, dépenses passées, présentes ou futures, selon le pays, sur une période de cinq ans. EU + *member states* : Union européenne + États membres.
Source : Olivier Ezratty (conférencier, enseignant, conseiller de l'État autour des technologies quantiques et auteur de l'ouvrage Comprendre l'informatique quantique, *novembre 2018).*

Si les perspectives de développement de l'informatique quantique sont très encourageantes pour l'avenir, un cas d'usage spécifique fera peser un risque sur la sécurité des systèmes d'information, peut-être dès 2030 : le décryptage des clés des algorithmes de chiffrement. Des hackeurs pourraient utiliser cette technologie pour déchiffrer l'intégralité des communications électroniques actuelles, ou pour usurper l'identité d'une personne après avoir percé le secret de sa signature électronique. Ce risque est identifié sous le terme de « menace quantique ».

Il existe deux grandes familles d'algorithmes de chiffrement :

- les algorithmes symétriques, qui reposent sur l'échange d'une clé secrète réservée aux participants de l'échange d'information ;
- les algorithmes asymétriques qui reposent sur un couple clé privée-clé publique, la première étant le seul secret et la seconde, calculée à partir de la première, pouvant être librement partagée *(cf. section 2* infra*)*.

Dans les deux cas, plus une clé est longue en matière de bits, plus il est difficile de la déchiffrer.

La sécurité du chiffrement repose :

- à la fois sur la sécurité de la procédure d'échange de clé et sur la difficulté à retrouver la clé secrète à partir d'un texte chiffré dans le cas des algorithmes symétriques ;
- sur la difficulté à retrouver la clé privée, soit à partir de la clé publique, soit à partir du texte chiffré dans le cas des algorithmes asymétriques.

Ces algorithmes sont répandus dans l'initiation de toutes les communications sécurisées comme les signatures électroniques, les connexions Internet SSL/TLS, les VPN [2]

d'entreprises, etc. Mais ils ne sont pas identiquement exposés à la menace quantique.

En 1995, le mathématicien Peter Shor [3] a démontré qu'un ordinateur quantique suffisamment puissant pourrait radicalement réduire la difficulté des problèmes mathématiques sur lesquels repose la cryptographie asymétrique actuelle : le temps de calcul de la clé pourrait être ramené de plusieurs années à quelques heures.

Ainsi seul le remplacement des algorithmes actuels par de nouveaux basés sur des problèmes mathématiques différents offrirait un niveau de sécurité satisfaisant.

Une année plus tard, le mathématicien Lov Grover [4] a démontré que, pour les algorithmes de chiffrement symétrique, la complexité de la recherche exhaustive de clés pourrait être diminuée substantiellement. Cette menace serait toutefois plus simple à circonscrire, puisque les experts s'accordent sur le fait que doubler la taille des clés suffirait à la contenir à moyen terme [5].

Les paiements électroniques se sont fortement développés lors des dernières décennies, notamment en raison de la croissance du commerce en ligne. La sécurisation des communications dans la chaîne de paiement joue un rôle essentiel dans la protection des données sensibles et la confiance des utilisateurs. Les deux principaux moyens de paiement utilisés par les particuliers sont la carte bancaire et le virement. En 2022, ils représentaient respectivement 60 % et 17 % des transactions scripturales [6] en volume de transactions. Les algorithmes de chiffrement sont largement utilisés afin de garantir l'authentification des émetteurs et des bénéficiaires, ainsi que la confidentialité des données de transaction, à l'instar du code PIN de la carte.

Les experts mettent en avant trois risques majeurs envisageables en cas d'affaiblissement de la sécurité de ce type de données :

- **« stocker maintenant pour déchiffrer plus tard »** : les données et communications chiffrées très sensibles (relatives à la sécurité nationale par exemple) qui sont enregistrées aujourd'hui pourraient être déchiffrées dans le futur ;
- **l'usurpation d'identité** : à terme, toute organisation disposant d'un ordinateur quantique suffisamment puissant pourrait se faire passer pour une entreprise légitime, notamment dans le but de détourner de l'argent, créant, ce faisant, un risque de réputation pour cette dernière ;
- **la crise de confiance** : le grand public pourrait prendre conscience du risque associé à la menace quantique et donc provoquer une crise de confiance généralisée qui gèlerait rapidement toutes les transactions de paiement menaçant ainsi la stabilité de nos économies.

Évaluer le risque réel du développement de l'informatique quantique sur la sécurité des systèmes de paiement électronique devient par conséquent impératif. La portée de ce travail d'audit est colossale. L'étude ci-dessous se focalise sur le mode de paiement le plus utilisé au quotidien par les Français : la carte bancaire. À des fins de concision, le paiement mobile de proximité et la compensation sont exclus du périmètre d'analyse.

3.2 Présentation des principaux algorithmes de chiffrement et des dispositifs de sécurité associés

Ce chapitre a pour but de présenter de façon pédagogique les grands principes de la cryptographie qui structurent la sécurité des systèmes de communication et donc celui de l'industrie des paiements.

3.2.1 Les algorithmes classiques de chiffrement symétrique (clé secrète) et asymétrique (clé publique-clé privée)

3.2.1.1 Principe du chiffrement symétrique

En cryptographie symétrique, la sécurité est fondée sur la confidentialité d'une clé connue uniquement des utilisateurs légitimes. Un mécanisme de chiffrement symétrique permet, à l'aide d'une clé secrète **K**, de transformer un message en clair **M** en un message chiffré **C**. L'accès à **C** (par exemple sur un canal de communication public) sans connaissance de **K** ne permet pas de connaître **M**. La clé **K** permet de déchiffrer **C** pour retrouver **M**.

1 GAFAM est l'acronyme des géants du Web : Google, Apple, Facebook, Amazon et Microsoft qui sont les cinq grandes firmes américaines qui dominent le marché du numérique.

2 SSL, *Secure Sockets Layer*, décrit un protocole de cryptage du trafic de données entre un navigateur et un site Web. TLS, *Transport Layer Security*, est l'équivalent de SSL, mais il utilise des algorithmes de chiffrement plus avancés. VPN, *Virtual Private Network*, est aussi un protocole de connexion sécurisée, mais qui vérifie en plus la légitimité des utilisateurs à se connecter au site.

3 Cf. *https://arxiv.org/abs/quant-ph/9508027*

4 Cf. « A fast quantum mechanical algorithm for database search », 28e conference annuelle *Symposium on the Theory of Computing*, mai 1996, p. 212.

5 Autre possibilité : augmenter la taille de l'empreinte de 3/2 pour les fonctions de hachage.

6 C'est-à-dire hors transactions réalisées en espèce.

Les algorithmes de chiffrement symétrique sont conçus afin de dissuader toute attaque qui s'avérera chronophage et fastidieuse. En effet, sans être en possession de la clé **K**, la méthode la plus efficace pour déchiffrer les données reste l'attaque exhaustive (dite par « force brute ») qui consiste à tester, une à une, un maximum de clés différentes possibles.

Les algorithmes sont donc conçus de sorte que le nombre de clés à tester est tellement important qu'une attaque exhaustive n'entre pas dans les capacités d'un ordinateur classique.

En considérant une longueur de clé donnée, la quantité d'effort requis (le « facteur travail ») pour se livrer à une attaque exhaustive peut être quantifiée en tenant compte de la puissance de calcul, la mémoire, l'énergie et le coût. Des clés suffisamment longues entraînent un nombre d'échecs tellement important que le facteur travail dépasse les limites pratiques réalisables.

Or l'informatique quantique, par sa puissance de calcul démultipliée, pourrait réduire considérablement le facteur travail. Cette réduction serait si importante qu'elle reviendrait *a priori* à diminuer de moitié la longueur de la clé utilisée (soit une réduction à la racine carrée du nombre de clés à tester).

Par exemple, si pour une longueur de clé déterminée, il existe 100 000 000 clés possibles à tester, réduire de moitié la longueur de la clé implique un facteur travail résiduel équivalent aux tests de 10 000 clés seulement.

Les algorithmes symétriques les plus fréquemment utilisés sont AES [7] et Triple-DES [8].

3.2.1.2 Principe du chiffrement asymétrique

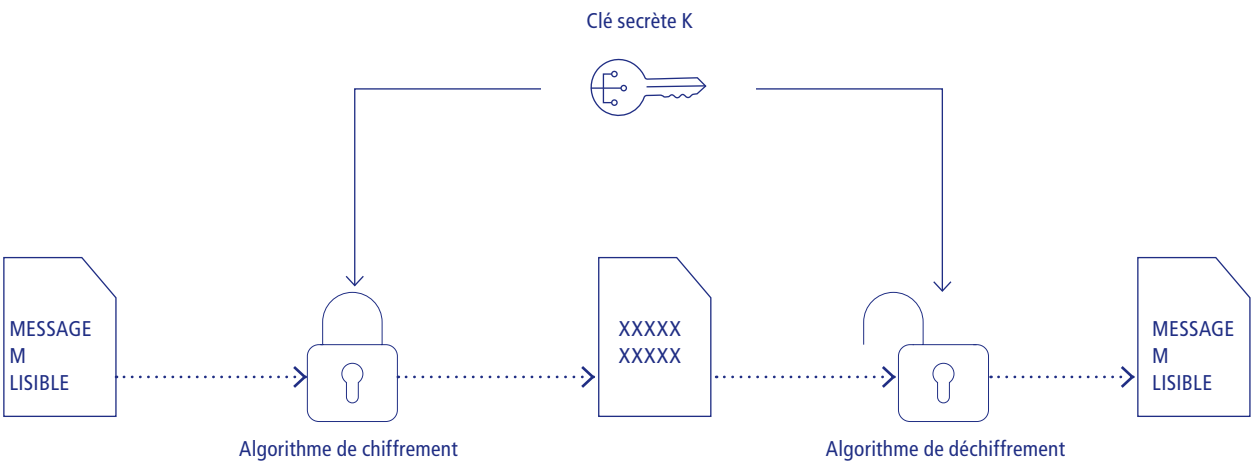
Un chiffrement asymétrique utilise une paire de clés : l'une publique et l'autre privée. L'usage normal est de rendre publique la clé publique **Pu** auprès de personnes ciblées (celles qui pourraient avoir besoin de communiquer avec l'utilisateur de la clé privée **Pr**). La clé privée **Pr**, quant à elle, n'est connue que d'un seul utilisateur bien identifié.

Le chiffrement asymétrique permet à toute personne ayant accès à la clé publique **Pu** d'envoyer des messages confidentiels à l'attention du détenteur de la clé privée **Pr**. En effet, la clé publique **Pu** permet de transformer un message en clair **M** en un message chiffré **C**. L'opération de déchiffrement transformant **C** en **M** ne peut être opérée ensuite que par le seul détenteur de clé privée **Pr**.

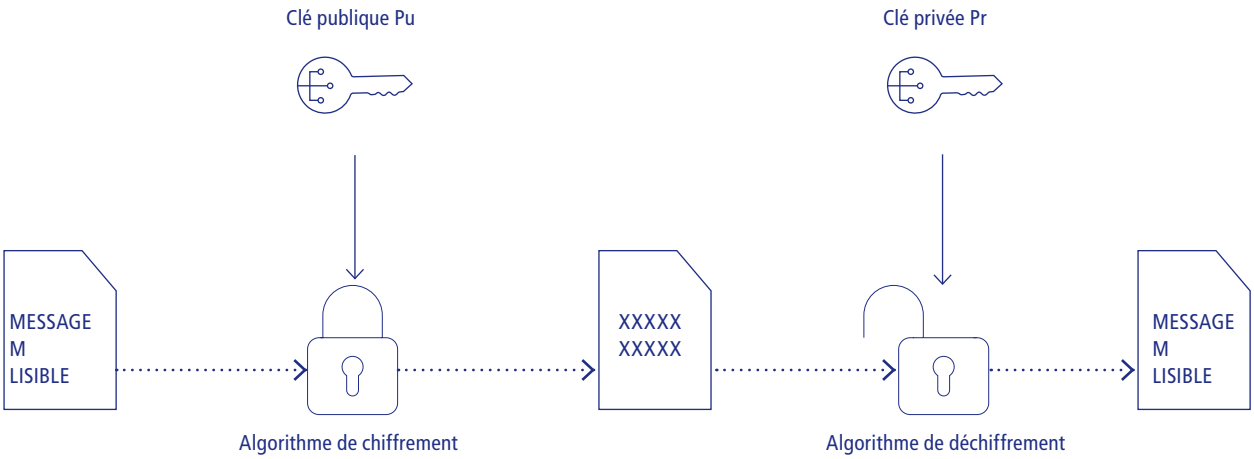
Réciproquement, le chiffrement asymétrique permet d'authentifier l'expéditeur d'un message. L'émetteur chiffre son message **M** à l'aide de sa clé privée **Pr** pour obtenir un message chiffré **C**. Tout détenteur de la clé publique peut déchiffrer le message **C** en **M**, et ainsi identifier l'émetteur du message qui en tant que détenteur de la clé privée **Pr** est le seul à avoir pu chiffrer le message **M**.

Le chiffrement asymétrique est basé sur des opérations mathématiques de factorisation par des nombres premiers, faciles à effectuer dans un sens, mais dont le chemin inverse s'avère plus complexe. En effet, il est beaucoup plus facile de calculer par exemple 1303 x 1307 que de déterminer quels sont les deux nombres à multiplier pour obtenir 1 703 021. Attaquer ce type de chiffrement consiste à résoudre ces problèmes mathématiques plutôt que d'effectuer une recherche exhaustive de clé, comme dans le cas du chiffrement symétrique. Par conséquent,

S1 Chiffrement symétrique



S2 Chiffrement asymétrique



T1 Recommandations en matière de sécurité des algorithmes actuellement les plus utilisés dans le monde des paiements

Algorithme de chiffrement	Famille	Obsolète	Recommandé jusqu'en 2023	Recommandé	Recommandé dans un environnement *post*-quantique
DES (*Data Encryption Standard*)	Symétrique	DES-2keys	Triple-DES	x	x
AES (*Advanced Encryption Standard*)	Symétrique			128/192/256	256
RSA (initiales du nom des concepteurs : Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman)	Asymétrique	< 2 048 bits	< 3 071 bits	3 072 bits ou plus	x
ECC (*Elliptic Curve Cryptography*)	Asymétrique				x

Source : Agence nationale de la sécurité des systèmes d'information (Anssi) – https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf.

une combinaison de calcul quantique et de techniques de tri pourrait réduire considérablement le temps et les efforts nécessaires pour mener une telle attaque.

Les algorithmes asymétriques les plus fréquemment utilisés sont le RSA [9] et la cryptographie sur les courbes elliptiques (ECC, *Elliptic Curve Cryptography*). La plupart des protocoles de communication reposent sur un chiffrement asymétrique, notamment pour sécuriser un échange initial de clés symétriques entre partenaires communicants.

3.2.1.3 Familles d'algorithme menacées par l'informatique quantique

En pratique, la menace quantique reste encore théorique. Les meilleurs ordinateurs quantiques disposent d'une puissance de calcul de 399 qubits [10] physiques. Or, selon certains chercheurs, 20 millions de qubits seraient nécessaires pour casser une clé RSA d'une longueur standard en huit heures [11], en considérant l'imprécision des qubits actuels.

À terme, la même puissance de calcul pourrait être atteinte par un nombre de qubits moins important, en fonction des progrès en matière de correction d'erreurs. Les experts estiment que la capacité de calcul suffisante pourrait être atteinte autour de 2 035 qubits [12].

7 *Advanced Encryption Standard*.

8 *Data Encryption Standard*. Ce dernier n'est plus recommandé par l'Anssi, contrairement à l'AES, en raison de certaines fragilités (p.15, *Guide de sélection des algorithmes cryptographiques*, Anssi, 2021).

9 Initiales du nom des concepteurs de l'algorithme : Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman.

10 *IBM Development Roadmap IBM, https://www.ibm.com/quantum/technology*

11 Craig Gidney et Martin Ekerå, « How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits » (2021) : *https://quantum-journal.org/papers/q-2021-04-15-433/*

12 Cf. *Quantum threat timeline report* 2022, Global Risk Institute, p. 21-67 : *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/*

En revanche, une moindre menace pèse sur les algorithmes de chiffrement symétrique de type AES. En utilisant la force brute de l'algorithme de Grover, le calcul quantique permettrait de diviser par deux leur degré de sécurité [13] qui est défini par la longueur de la clé secrète. Par conséquent, l'Agence nationale de la sécurité des systèmes d'information (Anssi) recommande d'augmenter la longueur des clés à 256 bits pour les chiffrements issus d'algorithmes AES, afin de résister aux futures attaques basées sur l'informatique quantique.

3.2.2 Les dispositifs de sécurité rencontrés dans le secteur du paiement par carte

3.2.2.1 Principe du hachage

Une fonction de hachage est un procédé à sens unique permettant d'obtenir une suite d'octets, c'est-à-dire une empreinte appelée *hash*, caractérisant un ensemble de données quelconques. Pour tout ensemble de données de départ, l'empreinte obtenue est toujours la même. Par conséquent, la fonction de hachage permet ainsi de s'assurer de l'intégrité d'un document.

3.2.2.2 Principe du HMAC

Un *hash-based message authentication code* (HMAC) est un type de code d'authentification de message qui combine une fonction de hachage cryptographique et une clé secrète symétrique. D'une part, le *hash* issu de la fonction associée permet à deux partenaires communicants de vérifier l'intégrité des données et, d'autre part, la clé secrète symétrique de s'assurer de l'authenticité de l'émetteur.

3.2.2.3 Principe de signature électronique

Un mécanisme de signature électronique se compose de trois fonctions :

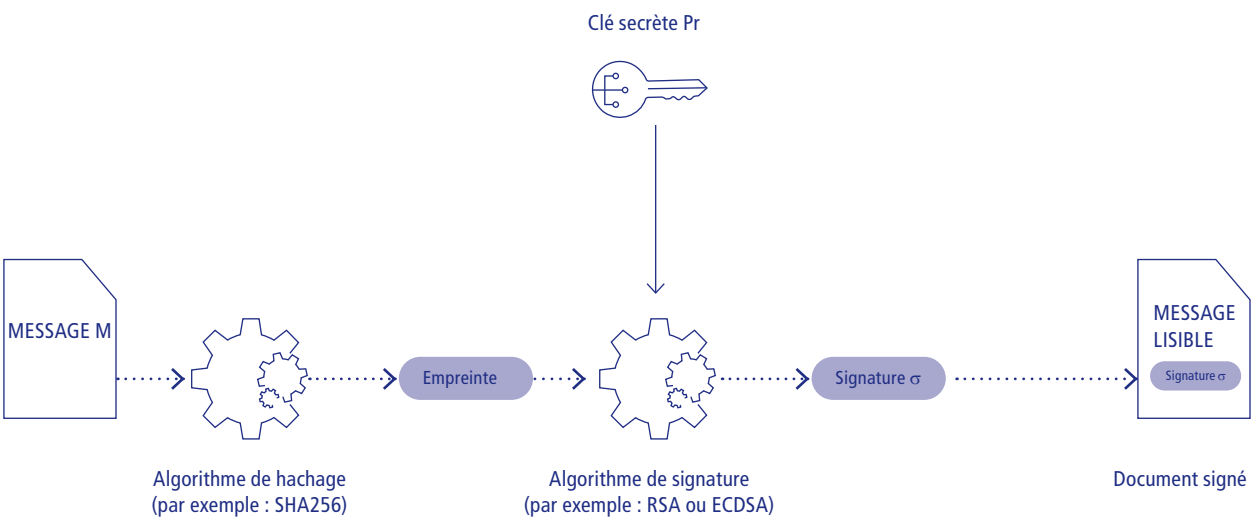
- la fonction de génération de clés construit une « bi-clé » asymétrique, c'est-à-dire une clé électronique constituée de deux clés mathématiquement liées entre elles : une clé privée **Pr** et une clé publique **Pu** ;
- la fonction de génération de signature utilise le *hash* d'un message **M** et la clé privée **Pr** pour calculer une signature **σ** ;
- la fonction de vérification de signature permet au récepteur du message **M** de valider la signature (réponse vrai/faux) en comparant le *hash* du message **M**, que le récepteur recalcule lui-même au *hash* de **M** contenu dans la signature **σ** qu'il déchiffre à partir de la clé publique **Pu**, pour s'assurer que les *hashes* sont identiques.

3.2.2.4 Principe du certificat

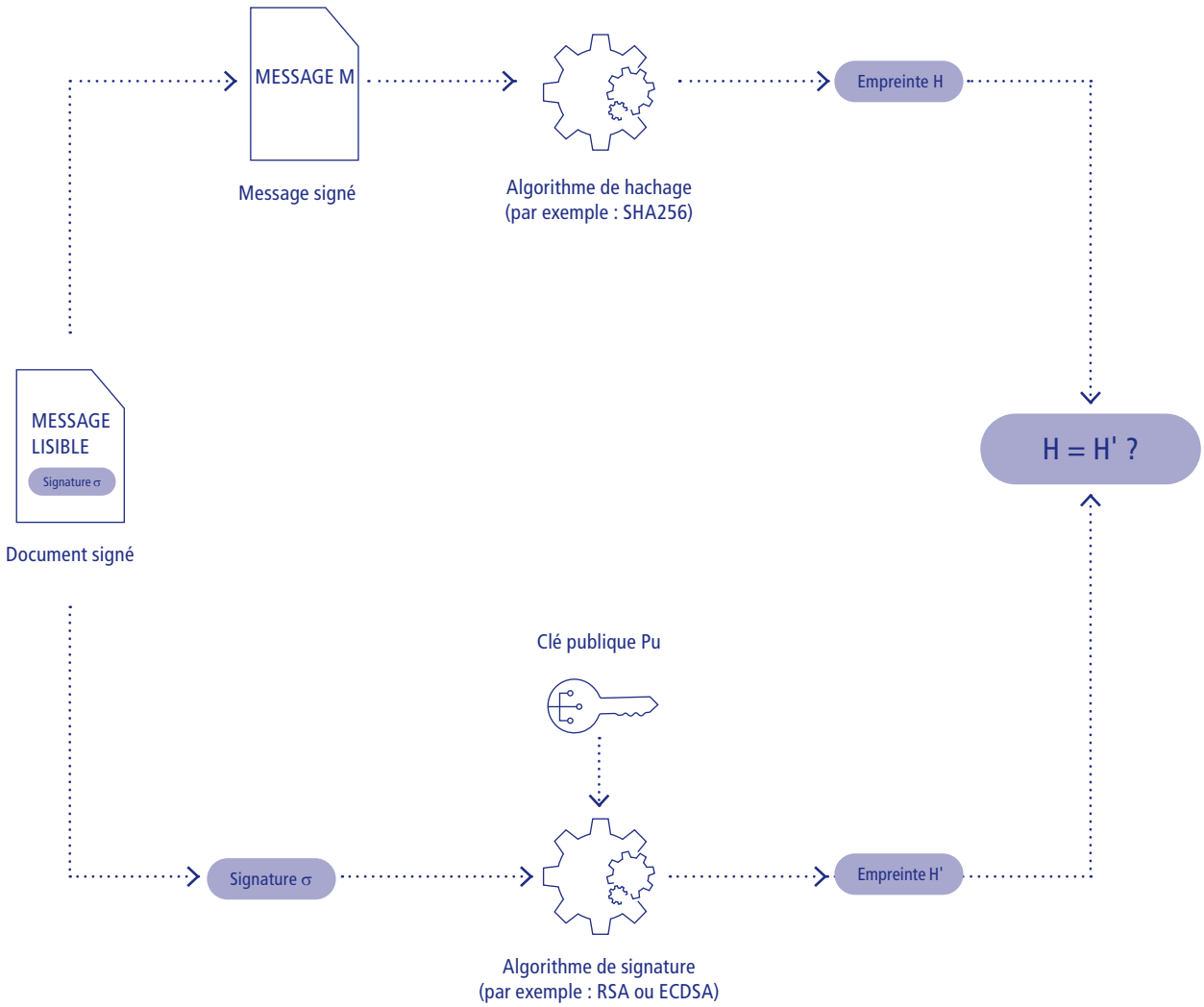
Ce mécanisme permet à une entité de prouver son identité auprès de sa contrepartie, par l'intermédiaire d'une autorité de certification.

Pour certifier son identité, toute entité doit entamer une procédure dédiée auprès d'une autorité de certification reconnue par ses contreparties. Après étude, l'entité reçoit un certificat qui se compose de deux parties : des informations en clair sur l'entité elle-même (notamment : nom, adresse et clé publique de l'entité) et un *hash* signé de ces informations, c'est-à-dire chiffré, avec la clé privée de l'autorité de certification. Les clés publiques de l'autorité de certification sont distribuées à tous les interlocuteurs potentiels.

S3 Signature d'un document



S4 Vérification de la signature



Lors de la procédure d'identification entre deux entités, le récepteur s'assure d'abord que le certificat de l'entité émettrice n'a pas expiré, ni été révoqué. Puis, il vérifie la validité de la signature en déchiffrant le ***hash*** contenu dans le certificat grâce à la clé publique de l'autorité de certification et le compare avec un ***hash*** qu'il calcule lui-même à partir des informations en clair. Si les deux ***hashes*** sont identiques, le récepteur valide l'identité de l'entité émettrice.

Selon le même principe d'utilisation de clés publiques, l'entité certifiée peut elle-même produire des sous-certificats pour des entités dont elle est responsable. Une chaîne imbriquée de certificats est ainsi créée, l'intégrité des certificats en bout de chaîne étant garantie par l'intégrité des certificats de haut niveau.

Par conséquent, toute la confiance accordée à une infrastructure à clé publique est fondée sur l'intégrité de l'autorité de certification qui n'a d'autre possibilité que d'auto-signer son propre certificat avec une clé privée dite « racine » [14].

13 Mais d'autres algorithmes plus performants sont à l'étude et permettraient d'aller plus loin, réduisant encore plus la résistance d'un algorithme symétrique.

14 Ainsi lorsque cette dernière est compromise, toutes les chaînes de certificats dépendant de cette autorité de certification sont suspectes, ce qui peut créer une crise de confiance à grande échelle et donc considérablement altérer la fluidité des échanges électroniques.

3.2.2.5 Principe de la connexion sécurisée : SSL/TLS

Les connexions sécurisées d'un ordinateur à un serveur, ou entre deux serveurs, se sont généralisées ces dernières années. Il s'agit notamment des connexions à des sites qui font apparaître un cadenas dans la barre d'adresse des navigateurs Web.

Les protocoles SSL/TLS permettent de tester la légitimité de la machine à se connecter à un serveur. Cette sécurisation se fait grâce à un protocole qui comporte plusieurs étapes. La première est la reconnaissance des certificats des serveurs. À cette fin, les clés publiques des autorités de certification sont intégrées au préalable dans les navigateurs Web des utilisateurs et les serveurs des sites Internet. La seconde étape consiste en la transmission d'une clé symétrique qui va permettre de chiffrer toutes les informations communiquées lors de l'échange. Le mécanisme le plus utilisé pour l'établissement de clé secrète entre deux entités est le protocole de Diffie-Hellman.

Les connexions VPN, quant à elles, sont davantage sécurisées car elles testent aussi la légitimité de l'utilisateur de la machine à se connecter à un serveur au moyen de protocoles d'authentification forte.

3.3 Les risques à terme sur les systèmes de paiement par carte en l'absence d'actions correctives

Les paiements par carte font référence à trois types de transactions différents :

- les paiements de proximité réalisés en magasin à partir de terminaux de paiement électronique (TPE) ;
- les retraits d'espèces effectués auprès de distributeurs automatiques de billets (DAB) ;
- les paiements à distance sur Internet.

Les deux premiers ont pour point commun de recourir à la technologie EMVco embarquée dans les puces des cartes.

3.3.1 La sécurité relative aux algorithmes de chiffrement des transactions impliquant la technologie EMVco

La présentation ci-dessous s'appuie sur les standards de sécurité EMVco actuellement les plus répandus dans les dispositifs de paiement de proximité par carte et de retrait. Les montées de version récentes des spécifications EMVCo ont pour conséquence la migration progressive vers de nouveaux algorithmes de chiffrement, sans pour autant altérer la nature de la menace quantique.

3.3.1.1 Présentation simplifiée du système d'information associé au paiement via EMVco

Le bon fonctionnement des paiements de proximité par carte bancaire et des retraits d'espèces dépend **de l'interconnexion de trois systèmes de communication sécurisés** *(cf. schéma 5* infra*)*.

Le premier système de communication est intégré dans la puce de la carte de paiement respectant les standards internationaux de sécurité édictés par l'organisme de normalisation EMVco [15]. Ces standards requièrent *a minima* deux fonctions de sécurité associées à des algorithmes de chiffrement :

- Deux certificats d'authentification basés sur du chiffrement asymétrique de type RSA 1984 [16] bits sont implémentés dans les puces des cartes de paiement :
  - Le certificat de l'établissement émetteur de la carte (en général un établissement bancaire) est signé par la clé privée du réseau auquel la carte est raccordée (Cartes bancaires, MasterCard, Visa, etc.). La clé publique correspondante est au préalable diffusée sur le parc d'acceptation des TPE et des DAB ;
  - Le certificat de la carte est signé par la clé privée de l'établissement émetteur. La vérification de légitimité de la carte par le TPE est possible à partir de la clé publique contenue dans le certificat de l'établissement émetteur. Le certificat de la carte contient également une clé publique utilisée par le TPE quand ce dernier doit envoyer des informations à la carte, notamment lors de la vérification du code PIN *(cf. PIN hors ligne défini dans la section « 3.1.2 Les modes de transactions des paiements de proximité et des retraits »)* ;
- Un cryptogramme est calculé par la carte en utilisant l'algorithme de chiffrement symétrique Triple DES (2k-TDEA) pour chaque transaction [17]. La clé maîtresse est enregistrée dans le serveur d'autorisation de l'établissement émetteur de la carte. Une clé dérivée de la clé maîtresse est enregistrée dans la puce de la carte, qui, à chacune des transactions qu'elle envoie au serveur d'autorisation par le TPE ou le DAB [18], dérive une sous-clé pour chiffrer le cryptogramme. En retour, le serveur d'autorisation chiffre, à partir de la clé maîtresse, un message de demande d'autorisation qu'il envoie à la carte. Celle-ci vérifie simultanément l'intégrité et l'authenticité des informations de paiement contenu dans le message pour pouvoir valider le paiement ou le retrait d'espèce [19].

Le second système de communication permet la connexion du TPE, ou du DAB, avec le serveur de l'établissement propriétaire, en général l'établissement qui acquiert la transaction de paiement :

- La sécurisation de la connexion entre un TPE et le serveur de paiement de l'établissement acquéreur repose sur le protocole « Carte Bancaire Accepteur Acquéreur » (CB2A). Celui-ci implique notamment le protocole TLS : les authentifications du TPE et du serveur sont réalisées à partir de certificats intégrant un algorithme de signature RSA 2048 [20], et l'échange de clés symétriques secrètes de AES 128 est assuré par un algorithme d'échange de clés RSA également ou de type Diffie-Hellman ;
- En ce qui concerne les retraits d'espèces, les DAB se connectent au serveur de retrait de l'établissement propriétaire. La connexion est réalisée suivant les protocoles TR34 et TR31, spécifiques à l'industrie des paiements, qui impliquent l'échange de clés asymétriques (RSA) et symétriques (Triple DES ou AES selon les implémentations).

Enfin, la connexion entre le serveur d'autorisation de l'acquéreur et le serveur d'autorisation de l'émetteur de la carte est assurée par l'infrastructure de paiement interbancaire nommée e-RSB, sous la supervision de la société STET. La connexion entre la banque de l'acquéreur et la banque de l'émetteur est réalisée selon le protocole « Carte bancaire acquéreur-émetteur » (CBAE) [21]. Le dispositif de sécurité est assuré par un chiffrement symétrique AES 128, dont la gestion des clés secrètes est confiée à des officiers de sécurité spécialisés.

3.3.1.2 Les modes de transaction des paiements de proximité et des retraits

Les paiements de proximité par carte chez un commerçant peuvent être réalisés selon trois modes différents qui n'impliquent pas les mêmes dispositifs de sécurité :

- **Transaction avec demande d'autorisation en ligne et vérification du code PIN hors-ligne :** le TPE peut vérifier si la carte est légitime par le dispositif de certificats [22] et le code PIN saisi par le porteur de carte sur le clavier sécurisé du TPE est transmis à la carte pour vérification en local. Selon le choix de l'émetteur, le canal entre la carte et le terminal peut être chiffré à l'aide du dispositif de certificats. En complément, la sécurité de la transaction s'appuie sur un cryptogramme chiffré en Triple DES produit par la puce de la carte et inclus dans la demande d'autorisation véhiculée jusqu'au système d'autorisation de l'émetteur. Ce type de transaction est majoritairement utilisé pour les paiements qui requièrent systématiquement la composition du code PIN par le porteur de la carte (montants supérieurs à 50 euros) ;
- **Transaction hors ligne :** l'authentification de la carte et la vérification du code PIN sont réalisées comme décrit précédemment. À la différence, la sécurité relative au cryptogramme chiffré en Triple DES n'est plus opérationnelle. L'échange d'informations ne repose alors que sur les clés asymétriques. La décision de traiter la transaction en mode hors ligne dépend de plusieurs facteurs : la possibilité d'accéder au réseau Internet (en raison de l'inaccessibilité dans les transports en commun pour les valideurs, de zones blanches, de l'indisponibilité du serveur ou de coupure de réseau) ou encore de la politique de risque de l'émetteur et/ou de l'acquéreur. En mars 2023, ces transactions représentent environ 30 % du nombre de transactions de proximité ;
- **Transactions avec demande d'autorisation en ligne et vérification en ligne du code PIN :** i) l'authentification de la carte est réalisée au niveau du TPE par le dispositif de certificats, et ii) la transaction et le code PIN sont validés au niveau du serveur d'autorisation de la banque émettrice par des cryptogrammes qui leur sont propres, chiffrés en Triple DES (voire, selon la banque émettrice, en AES pour le code PIN). Ce mode de transaction est le plus sécurisé. Si le nombre de transactions associé reste encore marginal, le potentiel de croissance est très important dans la décennie à venir en raison du développement de la technologie *SoftPOS* (*Software Point of Sales*) qui permet de substituer un smartphone au TPE classique.

En ce qui concerne les retraits d'espèces, les dispositifs de sécurité opérationnels sont proches du mode **« Transaction en ligne et vérification en ligne du code PIN »**.

3.3.2 La sécurité relative aux algorithmes de chiffrement des transactions impliquant la technologie 3-D Secure

Dans le cadre de l'application de la deuxième directive sur les services de paiement (DSP 2), la généralisation des dispositifs d'authentification forte par le protocole 3-D Secure, a permis de renforcer la sécurité des paiements par carte à distance.

15 Il regroupe MasterCard, Visa, American Express, Discover, JCB (Japan Credit Bureau, Japon) et Union Pay (Chine).

16 Il s'agit de la norme maximale autorisée par EMVco. Dans le nouveau standard, le chiffrement de type RSA est remplacé par un chiffrement de type ECC, aussi exposé au risque quantique.

17 Dans le nouveau standard, les clés de chiffrement de type Triple DES sont remplacées par un chiffrement AES 128 ou AES 256.

18 *Authorization ReQuest Cryptogram* (ARQC).

19 *Authorization ResPonse Cryptogram* (ARPC).

20 112 bits de résistance si l'on compare avec une primitive cryptographique symétrique.

21 Carte bancaire acquéreur-émetteur : protocole d'autorisation, de télécollecte, de téléparamétrage et de gestion du réseau.

22 Il s'agit d'une option réalisée en fonction des choix de l'émetteur.

Le dispositif s'appuie sur un réseau de connexions complexes entre plusieurs serveurs qui peut se résumer ainsi :

i. **Initiation de la transaction :** lorsque le porteur de la carte effectue un achat en ligne, il remplit les informations de paiement sur le site Web du commerçant, telles que le numéro de la carte (PAN, *Primary Account Number*), la date d'expiration et le cryptogramme visuel ;
ii. **Cheminement de la demande au serveur d'authentification de la banque émettrice :** si le commerçant participe au système 3-D Secure, le site du commerçant envoie une demande d'authentification au *Directory Server* (DS). Chaque schéma de carte détient son propre DS qui joue le rôle d'intermédiaire entre le serveur du commerçant et le serveur d'authentification de la banque ayant émis la carte du porteur. Ce dernier se nomme le serveur de contrôle d'accès (ACS, *Access Control Server*) ;
iii. **Génération de la preuve d'authentification par le serveur ACS :** le serveur ACS de la banque reçoit la demande d'authentification et envoie un message au porteur de la carte afin qu'il procède à son authentification forte. En France, cette étape implique très majoritairement une notification envoyée sur le mobile du porteur de carte pour que ce dernier se connecte à son application bancaire ou reporte un code temporaire envoyé par SMS en complément d'un deuxième code secret (principe du « SMS renforcé »). Si le serveur ACS de la banque confirme que l'authentification est réussie, il génère une preuve d'authentification. Si l'authentification échoue, la transaction est immédiatement refusée. Dans tous les cas, le serveur ACS envoie une réponse au *Directory Server* qui la retransmet au site du commerçant ;
iv. **Cheminement de la demande d'autorisation du paiement :** celui-ci est comparable à celui du paiement de proximité. Si l'authentification est réussie, le site du commerçant génère une demande d'autorisation intégrant la preuve d'authentification du porteur. La demande est envoyée au serveur d'autorisation de l'émetteur de la carte par le serveur d'autorisation de l'acquéreur et le réseau interbancaire de paiement. Les contrôles applicables sont comparables et comprennent en outre la vérification de la validité de la preuve d'authentification. Une fois que la transaction est approuvée par l'émetteur de la carte, le porteur reçoit une confirmation de paiement du commerçant, et la transaction est complétée.

Les deux principaux dispositifs de sécurité embarqués sont :

- les connexions entre les sites de commerçant [23] et le *Directory Server*, et entre le *Directory Server* et les serveurs ACS des émetteurs, sont sécurisées par des échanges de certificats intégrant des algorithmes de chiffrement asymétrique de type RSA 2048 et des clés de session AES 128 ;
- la preuve d'authentification, calculée par le serveur ACS et vérifiée par le système d'autorisation de l'émetteur, repose sur un algorithme HMAC-SHA-256 [24] avec une clé secrète de 256 bits.

3.3.3 L'impact potentiel de l'informatique quantique sur le niveau de sécurité des dispositifs de chiffrement des paiements par carte

L'Anssi transcrit le niveau de sécurité d'un mécanisme cryptographique notamment au moyen d'un indice de résistance traduisant la complexité à casser une clé d'un algorithme de chiffrement. Cet indice s'appuie sur le nombre d'opérations requises par la meilleure attaque connue contre ce mécanisme.

Par exemple, dans le cas d'un algorithme symétrique, un indice de 128 bits de sécurité signifie que 2^{128} opérations sont potentiellement nécessaires pour le casser [25].

Les indices de résistance du dispositif de sécurité relatif au paiement de proximité par carte et au retrait sont illustrés sur le schéma 5. Pour information, un algorithme asymétrique RSA 2048 offre une sécurité équivalente à un indice de 112 bits de résistance pour un algorithme symétrique.

La sécurité offerte par les certificats est essentiellement basée sur des algorithmes asymétriques RSA, vulnérables au calcul quantique, et sur des algorithmes symétriques qui ont une force de sécurité inférieure à l'AES 256. Par conséquent, un ordinateur quantique suffisamment puissant dégraderait les indices de résistance de la façon suivante, comme indiqué sur le schéma 6 :

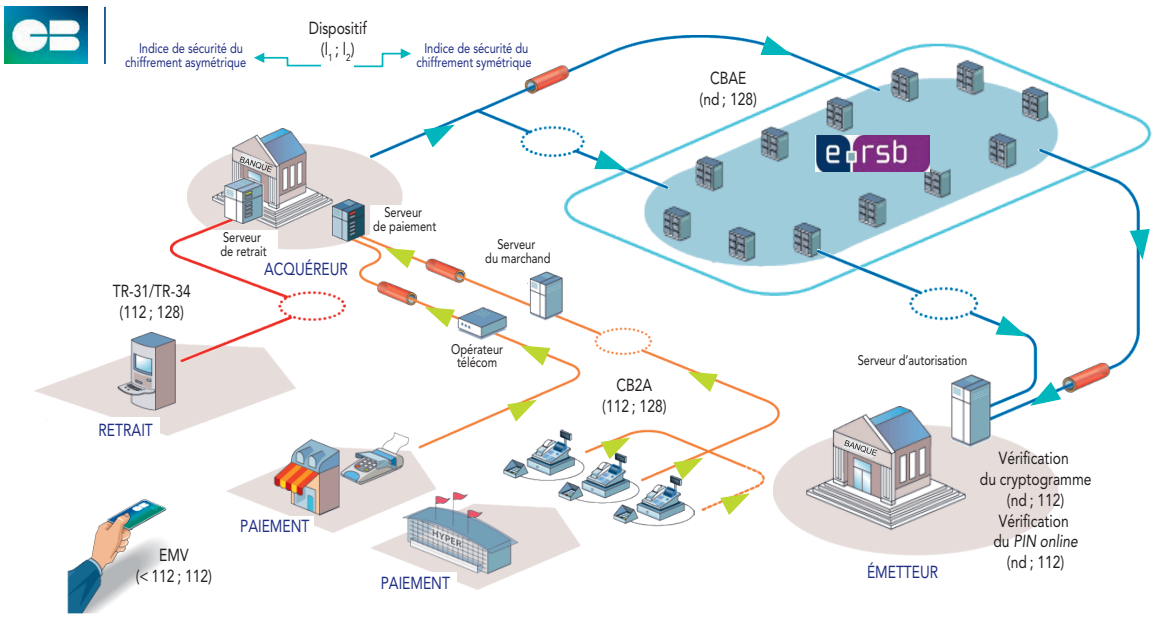
- Le cryptogramme EMV, calculé par la carte à chaque transaction et vérifié par le système d'autorisation émetteur, serait affaibli, et passerait d'un indice de résistance de 112 bits à 56 bits ;
- Les mécanismes d'authentification de la carte et de vérification du code PIN hors ligne seraient intégralement menacés, passant d'un indice de résistance de 112 bits à 0 bit ;

23 Souvent par un serveur de Prestataires d'acceptation technique.

24 SHA (*Secure Hash Algorithm*) est une fonction de hachage cryptographique utilisée par des autorités administratives pour la signature de certificats.

25 Cf. *Guide de sélection d'algorithmes cryptographiques – Guide Anssi*, p.47-58, *https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf*

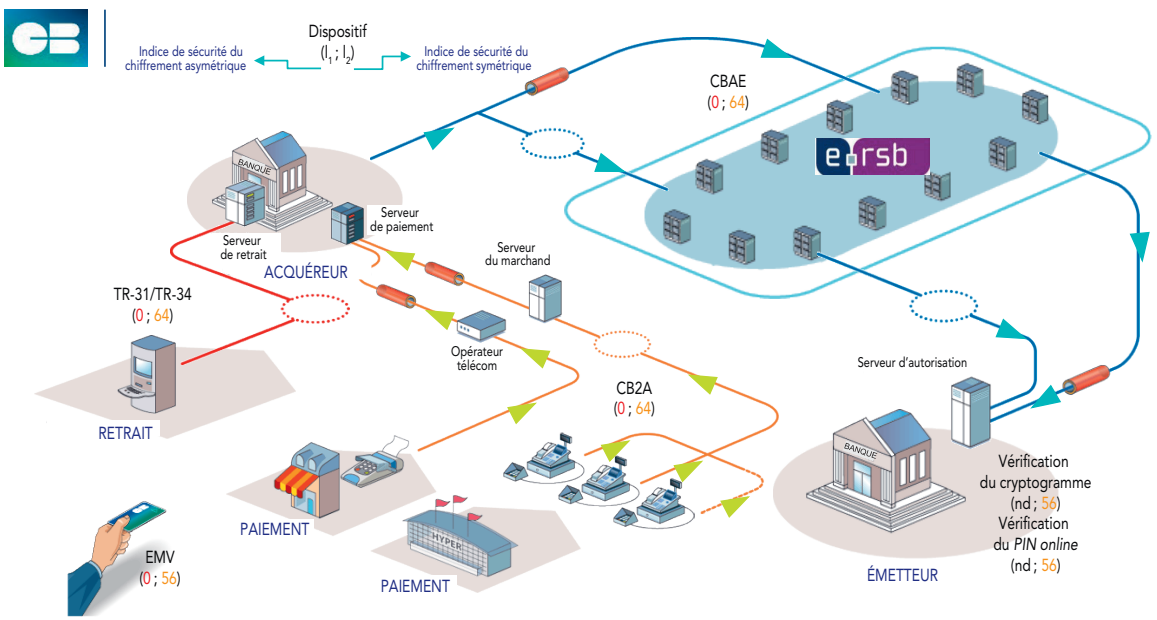
S5 Indices de résistance du dispositif de sécurité relatif au paiement de proximité par carte et au retrait



Note : CBAE, Carte bancaire acquéreur-émetteur ; CB2A, CB accepteur-acquéreur ; EMV, EuropayMastercard Visa ; nd, non disponible.

Source : Groupement des cartes bancaires.

S6 Indices de résistance face aux attaques par calcul quantique



Note : CBAE, Carte bancaire acquéreur-émetteur ; CB2A, CB accepteur-acquéreur ; EMV, EuropayMastercard Visa ; nd, non disponible.

Source : Groupement des cartes bancaires.

- Le lien sécurisé entre les systèmes d'acceptation (TPE et DAB) et les systèmes d'acquisition pourrait être affaibli. En effet, ces liens s'appuient majoritairement sur des algorithmes RSA pour échanger une clé de session symétrique. Si le mécanisme RSA est affaibli, la clé de session pourrait être retrouvée par l'attaquant ;
- La sécurité implémentée au niveau du réseau d'autorisation serait affaiblie, passant d'un indice de résistance de 128 bits à 64 bits.

L'impact sur les indices de résistance associé au dispositif 3-D Secure est équivalent : l'indice de résistance associé au chiffrement asymétrique devient nul et celui associé au chiffrement symétrique est divisé par deux.

3.3.4 Les risques que fait peser l'informatique quantique sur l'usage de la carte

Le système de paiement par carte, s'il n'évolue pas, deviendra à terme totalement vulnérable :

- **Au vol de données privées, voire confidentielles :** les identités des personnes [26] et les caractéristiques de leurs transactions pourraient être volées et déchiffrées. Dans le cadre d'un paiement de type transaction avec demande d'autorisation en ligne et vérification du code PIN hors-ligne, le PIN pourrait être exposé car, lorsqu'il est transmis chiffré à la carte, sa confidentialité ne repose que sur les dispositifs de certificats ;
- **À la génération de paiements frauduleux via la fabrication de *Yes Card* :** les paiements de proximité hors ligne sont exposés car ils ne dépendent que des dispositifs de certificats reposant sur des algorithmes asymétriques ;
- **À la perte de confiance globale dans les infrastructures de paiement :** si les clés privées racines structurant l'ensemble du dispositif d'authentification des certificats étaient cassées, les schémas de cartes et les institutions bancaires émettrices ne seraient plus maîtres de leur politique de certification. Si une clé de haut niveau venait à être cassée, l'impact serait très élevé car sa révocation impliquerait le rappel et la réémission d'un volume de cartes potentiellement important.

Ce jugement peut toutefois être nuancé. Il existe déjà des solutions alternatives de chiffrement qui pourraient être déployées d'ici la réalisation de la menace.

Ainsi, conformément aux recommandations de l'Anssi, les algorithmes symétriques implémentés devront migrer du Triple DES ou de l'AES 128 vers de l'AES 256. Cette mesure préservera un certain niveau de sécurité associé aux paiements autorisés en ligne : les transactions dont le PIN est vérifié en ligne seraient immunisées face à l'ordinateur quantique. Ce type de transaction devrait d'ailleurs prendre une part de plus en plus importante dans les paiements du quotidien en raison du développement de la technologie *SoftPOS* [27]. Si cette migration ne pose pas de difficulté technique particulière, les délais de mise à niveau, qui peuvent s'étaler sur plusieurs années, constituent une contrainte à prendre en compte afin d'éviter tout blocage du système.

En revanche, les choix techniques relatifs à la migration *post*-quantique des algorithmes de chiffrement asymétrique (vérification des certificats au niveau de la carte, connexion TLS, etc.) sont moins triviaux. C'est la raison pour laquelle des efforts de Recherche et Développement sont dès à présent impulsés, notamment dans le monde des paiements.

3.4 Les expériences d'implémentation d'algorithmes « *post*-quantiques »

L'Anssi a publié en 2023 une liste non exhaustive d'algorithmes de chiffrement et de signature présumés résistants à la puissance de calcul des futurs ordinateurs quantiques [28]. On les désigne couramment sous le vocable d'algorithmes « *post*-quantiques ».

3.4.1 L'introduction d'algorithmes *post*-quantiques dans les puces de carte bancaire

L'architecture, la taille de la mémoire et les composants des puces doivent permettre une exécution du paiement qui respecte les standards édictés par EMVco. Notamment, le temps d'exécution ne doit pas excéder les 300 millisecondes (ms). Les industriels ont initié des expériences consistant à évaluer les répercussions de l'implémentation des algorithmes *post*-quantiques sur le respect de ces normes.

Concernant les empreintes mémoires, les résultats montrent que la taille de la mémoire vive [29] (RAM, *random-access memory*) actuelle est insuffisante, surtout pour les algorithmes de signature *post*-quantiques :

Signature	Mécanisme d'échange de clé
CRYSTALS-Dilithium (ou Dilithium)	CRYSTALS-Kyber (ou Kyber)
Falcon	FrodoKEM
SPHINCS+	
XMSS / LMS	

Source : Agence nationale de la sécurité des systèmes d'information (Anssi).

- les différents tests d'implémentation des algorithmes Falcon et de Dilithium sur une puce nécessitent tous une taille de mémoire vive 5 à 8 fois plus importante que le RSA, à force de sécurité équivalente ;
- l'algorithme d'échange de clés Kyber requiert une taille de RAM 4 à 6 fois plus importante.

Concernant les temps de communication et les volumes de données échangées, l'augmentation des tailles des paramètres des clés et des signatures implique une hausse quasi proportionnelle du volume de données, et donc des temps d'échange entre la carte et le TPE.

En ce qui concerne les temps du calcul cryptographique en tant que tels, ils restent relativement compétitifs sur carte à puce comparés à des algorithmes de chiffrement classiques dont le niveau de sécurité est relativement élevé, à l'instar du RSA 3072 bits pour la signature et du Diffie Hellman 3072 pour l'échange de clés. Les résultats des expériences comparatives sont les suivants :

- Les temps de signature de l'algorithme Dilithium sont équivalents à ceux du RSA 3072, mais en moyenne seulement. En effet, les temps de signature deviennent non déterministes, c'est-à-dire qu'ils peuvent varier aléatoirement de façon importante. Les temps de signature de l'algorithme Falcon 512 sont en revanche relativement stables, mais ils sont deux fois plus importants que le temps moyen associé au Dilithium ;
- Les temps d'échange de clé de Kyber 512 et Saber [30] sont dix fois plus rapides que ceux associés au Diffie Hellman 3072.

Ces tests d'implémentation d'algorithmes *post*-quantiques pointent les limites des contraintes actuelles du marché. Une évolution sera nécessaire afin de répondre aux problématiques suivantes :

- La taille des mémoires RAM des puces devra certainement évoluer. Il existe déjà sur le marché des cartes équipées de puces offrant la quantité de RAM requise, mais elles ne sont pas encore utilisées sur le marché des paiements. L'évolution est donc techniquement possible ;
- En fonction des évolutions futures de la technologie de calcul implémentée dans les puces [31], la norme de 300 ms devra potentiellement évoluer pour s'adapter aux performances en matière de temps de traitement du paiement. Ce temps pourrait en outre être soumis à des variations significatives, par exemple en cas d'implémentation de l'algorithme Dilithium. Enfin, dans une période intermédiaire de migration vers le *post*-quantique, l'implémentation d'algorithmes hybrides devra probablement être prise en compte. Cela permettra d'assurer la compatibilité des nouvelles puces avec tous les dispositifs de lecture, indépendamment de leur conformité aux technologies *post*-quantiques. Toutefois, le temps d'exécution sera accru car il émanera du temps de traitement de l'algorithme classique additionné à celui de l'algorithme *post*-quantique ;
- Les performances du paiement sans contact, en fort développement depuis 2020, pourraient être dégradées. En effet, les technologies sans contact fonctionnent avec un faible niveau d'énergie. Les performances de calcul s'en trouvent ainsi limitées et donc également l'implémentation de certains algorithmes de chiffrement *post*-quantiques ou de solutions d'hybridation.

T2 Différence de ressources entre algorithmes de chiffrement classiques et *post*-quantiques à niveau de sécurité équivalent 128 bits

Algorithmes *post*-quantiques		RAM nécessaire par rapport RSA/ECC	Temps de calcul par rapport RSA/DH
Signature	Falcon	x 5 à 8	x 2
	Dilithium		≈
Échange de clés	Kyber	x 4 à 6	/ 10
	Saber		/ 10

Note : RAM, *random-access memory* (mémoire vive) ; RSA, (Ronald) Rivest, (Adi) Shamir et (Leonard) Adleman (initiales du nom des concepteurs de l'algorithme) ; ECC, *Elliptic Curve Cryptography* (cryptographie sur les courbes elliptiques) ; DH, (Whitfield) Diffie-(Martin) Hellman (initiales du nom des concepteurs d'une méthode d'échange de clés).
Sources : Thales et STMicroelectronics.

3.4.2 L'introduction d'algorithmes *post*-quantiques dans les HSM

Le *Hardware Security Module* (HSM) est un matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.

Le HSM est indispensable à toute infrastructure de gestion de clés, notamment pour la protection des clés maîtresses que détiennent les autorités de certification. Le HSM est un boîtier qui autodétruit ses données en cas de manipulation

26 Pour les paiements sans contact, le nom du porteur de carte n'est pas lisible.

27 Technologie permettant de remplacer les TPE classiques par des *smartphones*.

28 Cf. « ANSSI views on the Post-Quantum Cryptography transition (2023 follow up) », Anssi, 21 décembre 2023.

29 La mémoire vive est la mémoire où sont exécutés les calculs.

30 SABER est un algorithme d'échange de clé *post*-quantique qui ne figure pas à ce jour dans la liste de recommandations de l'Anssi.

31 Des accélérateurs de calculs permettent de produire plus rapidement les opérations coûteuses issues des algorithmes RSA et ECC. Ces accélérateurs n'existent pas encore ou ne sont pas encore présents sur les cartes à puce actuelles pour les algorithmes *post*-quantiques.

physique. En matière de logiciel, il offre un mécanisme de répartition du secret de la clé privée parmi plusieurs personnes désignées. Seul le rassemblement physique de ces personnes permet de réaliser des opérations sur la clé privée maîtresse, ce qui garantit son intégrité.

Ces dispositifs sont directement applicables à l'industrie des paiements. En effet, les schémas de carte et les banques émettrices servent d'autorité de certification pour la production des certificats implémentés dans les puces des cartes de paiement.

L'implémentation d'algorithmes de chiffrement asymétrique *post*-quantiques dans les HSM nécessite de s'appuyer sur des bibliothèques de programmes spécifiques. Les performances de certains types d'HSM, comme le montrent certaines expérimentations, doivent être améliorées [32] pour un usage optimal dans l'ère *post*-quantique. Techniquement, l'accroissement des performances ne présente pas de difficulté. Toutefois, elles impliquent un certain coût.

3.4.3 L'introduction d'algorithmes *post*-quantiques dans des serveurs de VPN dans les banques centrales

Un VPN (Réseau Privé Virtuel) est un logiciel qui s'installe sur plusieurs appareils reliés à Internet. Son but est de créer un tunnel de communication sécurisé entre un client [33] et un serveur. Cette technologie s'est démocratisée ces dernières années, notamment en raison de la généralisation du télétravail.

La Banque de France et la Bundesbank, en collaboration avec la Banque des Règlements internationaux (BRI), ont expérimenté la transmission de messages de paiement au travers d'un VPN IPsec strongSwan [34]. Celui-ci est doté de certificats X.509, très répandus dans la sécurisation des communications électroniques [35]. Le but était de démontrer que les algorithmes *post*-quantiques sont compatibles avec l'utilisation de réseaux publics.

Le dispositif de l'expérience suppose au préalable que :

- le HSM, les modules et les bibliothèques de programmes cryptographiques soient compatibles avec les algorithmes *post*-quantiques utilisés ;
- les autorités de certification fournissent des certificats hybrides *post*-quantiques (avec clés Dilithium), en parallèle de certificats classiques (avec clés RSA).

Dans le cadre du projet, les certificats ont été adaptés de façon *ad hoc* par les équipes. Il s'agit de certificats avec lien hybride (hybridation en parallèle, *cf. définition dans la section 5.1*). Le premier de type classique intègre un algorithme RSA 2048 pour la signature digitale et le mécanisme d'échange de clés. Le second intègre des algorithmes *post*-quantiques. Différentes combinaisons d'algorithmes *post*-quantiques et de forces de sécurité associées [36] ont été testées *(cf. tableau 3)*.

Chaque configuration a été testée une centaine de fois. Au final, la différence de temps de connexion du VPN hybride *post*-quantique est relativement marginale par rapport à l'utilisation d'un algorithme classique *(cf. graphique 2)*. Une fois que le tunnel est monté en AES-256, l'envoi d'un message d'un fichier XML de 1MB (1 mégabyte) n'entraîne aucune différence de temps puisque le chiffrement utilise les algorithmes symétriques classiques.

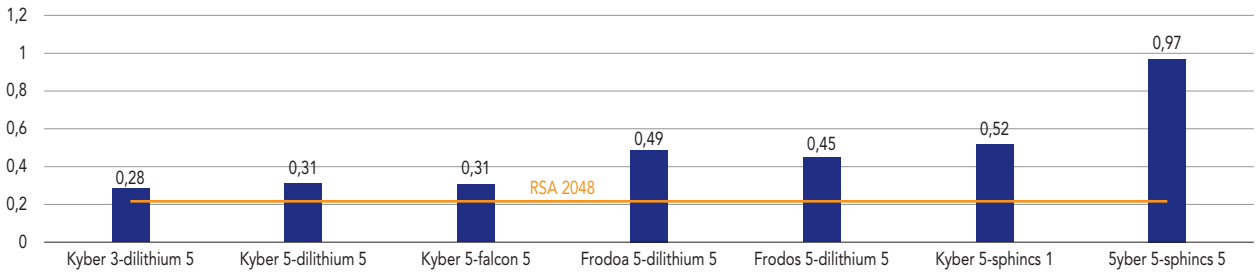
Il y a toujours un arbitrage entre sécurité et performance du VPN : plus le niveau de sécurité requis est important et plus le temps d'établissement du « tunnel » VPN est

T3 Combinaisons d'algorithmes classiques et *post*-quantiques testées dans l'expérience

Mécanisme d'encapsulement de clé	Niveau de force de sécurité face au calcul quantique	Signature digitale	Niveau de force de sécurité face au calcul quantique
RSA 2048	0	RSA 2048	0
CRYSTALS-Kyber	3	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	Falcon	5
FrodoKEM (AES)	5	CRYSTALS-Dilithium	5
FrodoKEM (Shake)	5	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	Sphincs+	1
CRYSTALS-Kyber	5	Sphincs+	5

Note : CRYSTALS, *Cryptographic Suite for Algebraic Lattices* (suite cryptographique pour les réseaux algébriques).
Source : Banque de France.

G2 Temps moyen de connexion entre deux serveurs selon les différentes combinaisons d'algorithmes *post*-quantiques (en secondes)



Sources : Banque de France, Banque des règlements internationaux (BRI).

important. Si la performance est privilégiée par rapport au niveau de sécurité, la combinaison des algorithmes Kyber et Falcon constituerait le meilleur arbitrage.

Néanmoins, l'expérience a été réalisée sur une seule connexion à la fois. Une multitude de connexions simultanées nécessiterait sans doute un redimensionnement des serveurs et l'estimation du temps de connexion serait à réexaminer pour d'autres cas d'usage, en particulier pour une connexion TLS.

3.5 Les enjeux techniques de la migration vers des algorithmes *post*-quantiques

La migration implique des contraintes techniques certaines et le facteur temps est primordial. En effet, le parc d'équipements sur le terrain (TPE, automates de paiement, automates de retrait, HSM, etc.) a souvent une durée de vie relativement longue, en général de sept à dix ans. Pour les cartes, cette contrainte existe, mais reste moins prégnante car leur durée de vie, de trois à cinq ans, est mieux maîtrisée.

La migration sera donc réalisée à des rythmes différents selon les infrastructures et sur une période relativement étendue durant laquelle les algorithmes *post*-quantiques pourraient relever des failles de sécurité à ce jour encore inconnues. Les dispositifs de chiffrement *post*-quantiques doivent donc être conçus de façon hybride et agile, conformément aux recommandations de l'Anssi [37].

3.5.1 L'hybridation

Le principe de l'hybridation consiste à utiliser simultanément les algorithmes courants avec des algorithmes *post*-quantiques. L'objectif est double :

- Assurer la compatibilité avec les systèmes d'information qui n'ont pas encore migré vers le *post*-quantique ;
- Renforcer mutuellement la sécurité conférée par les algorithmes classiques et celle des algorithmes asymétriques *post*-quantiques. En effet, durant la période de migration, la sécurité sera garantie par l'exécution d'algorithmes classiques matures (dont l'implémentation est éprouvée depuis plusieurs décennies) et celle des algorithmes *post*-quantiques qui ne montera que progressivement en maturité.

L'hybridation peut recouvrir différentes méthodes et être réalisée soit au niveau des protocoles de communication (TLS, IPSec, etc.), soit au niveau de certains objets cryptographiques, comme les certificats. Si l'on prend l'exemple des certificats X.509, au moins trois formes d'hybridation possibles existent aujourd'hui, chacune présentant ses propres avantages et inconvénients :

- **Le certificat hybride catalyste :** ce format stocke les algorithmes *post*-quantiques dans des extensions. À l'exception de ces dernières, ce certificat ressemble exactement à un certificat traditionnel. Ainsi un serveur qui n'a pas migré en *post*-quantique peut donc être capable d'analyser et de vérifier le certificat selon le protocole classique. Cela suppose toutefois qu'il traite les extensions non critiques et inconnues comme des données opaques. Par conséquent, ce format est dit « rétrocompatible », mais la sécurité garantie par l'algorithme *post*-quantique peut donc être contournée ;

32 Les HSM implémentés sur des serveurs *mainframe*, très répandus dans les établissements bancaires, disposent dès à présent de la puissance suffisante.

33 Un utilisateur ou un serveur.

34 **IPsec** : Il s'agit d'un certain type de VPN assez répandu répondant à des protocoles spécifiques d'authentification et d'échange de clés. **strongSwan** : il s'agit d'un logiciel libre permettant l'implémentation de VPN IPsec sur diverses plateformes.

35 Les applications courantes des certificats X.509 incluent : SSL/TLS et HTTPS pour une navigation Web authentifiée et cryptée, courriel signé et chiffré via le S/MIME (*Secure/Multipurpose Internet Mail Extensions*) protocole, signature de code, signature de documents, authentification client, pièce d'identité électronique émise par le gouvernement, etc.

36 Ces forces de sécurité sont déterminées selon une échelle élaborée par l'Institut national des normes et de la technologie (NIST, *National Institute of Standards and Technology*).

37 Cf. « Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie *post*-quantique », 14 avril 2022 ; et « ANSSI views on the Post-Quantum Cryptography transition (2023 follow up) », 21 décembre 2023.

- **Le certificat hybride concaténé :** celui-ci concatène l'algorithme classique avec un algorithme *post*-quantique, en remplacement du seul algorithme classique. Le protocole d'échange entre le client et le serveur n'est en soi pas modifié. Cependant, le serveur doit avoir migré au préalable vers des programmes *post*-quantiques pour être en mesure de traiter les algorithmes concaténés. La sécurité est donc renforcée, mais le dispositif n'est plus rétrocompatible ;
- **Les certificats avec lien hybride (ou hybridation parallèle) :** il s'agit d'une solution intermédiaire composée de deux certificats reliés. L'un est classique et l'autre pure *post*-quantique. Cette solution est flexible dans la durée pour gérer des solutions hybrides ou pures *post*-quantiques. Toutefois, son implémentation nécessite une mise à niveau du protocole d'authentification entre le client et le serveur. En outre, en cas de migration de ces derniers, il implique le traitement de deux certificats qui risque d'allonger matériellement les temps de connexion.

Les agences de sécurité européennes recommandent fortement le déploiement de solutions hybrides. Dans cette perspective, l'Anssi a annoncé l'attribution de visas de sécurité pour des produits incluant ces solutions hybrides à compter de 2024-2025 [38].

En matière d'hybridation, les choix de format et de combinaison d'algorithmes sont nombreux et se répercutent sur toute l'infrastructure de gestion de clés [39] (IGC, en anglais PKI – *Public Key Infrastructure*), les applications consommatrices de cette PKI *post*-quantiques, les protocoles et donc leur programmation. Ces choix doivent donc être arrêtés et intégrés dans le plan de migration des organisations.

La phase d'hybridation restera recommandée tant que la maturité des algorithmes *post*-quantiques n'est pas reconnue par les autorités compétentes.

3.5.2 La crypto-agilité

Aujourd'hui, la cryptographie est souvent incorporée directement dans le code source des logiciels ou des matériels.

Le principe de la crypto-agilité consiste à rendre cette cryptographie plus évolutive et configurable. En particulier, au niveau des algorithmes, un enjeu est de prévoir la capacité de basculer d'un algorithme *post*-quantique, affecté par une faille de sécurité, à un autre non compromis. En effet, les nouveaux algorithmes *post*-quantiques s'appuient sur des problèmes mathématiques plus ou moins matures qui n'ont pas encore prouvé leur robustesse à long terme. Ainsi, dans les années à venir, la communauté scientifique pourrait identifier des faiblesses mathématiques ou d'implémentation. À cet égard, deux algorithmes de chiffrement (SIKE [40] et Rainbow [41]) ont récemment fait l'objet d'attaques réussies par des ordinateurs classiques, dans le cadre du processus dédié de présélection organisé par le NIST [42].

Actuellement, les agréments octroyés aux constructeurs de cartes et le temps de leur renouvellement nécessitent que les algorithmes soient robustes sur une période de six à huit ans. Cette période est toutefois potentiellement trop longue en cas de faille de sécurité découverte sur un algorithme *post*-quantique donné.

Le remplacement des algorithmes *post*-quantiques par de plus robustes nécessitent des interfaces agiles et un code générique, de la bibliothèque de programmes basiques jusqu'aux applications terminales. Ainsi les migrations impliqueraient des efforts limités de refonte de spécifications des protocoles de transaction.

Le principe de crypto-agilité en temps réel pourrait être mis en œuvre en embarquant un algorithme actif et des algorithmes dormants dans la puce des cartes de paiement. Les différentes combinaisons pourraient être activées via un script émetteur. Aussi faudrait-il construire des canaux sécurisés, et donc *post*-quantiques, de mise à jour à distance des logiciels implémentés dans les parcs de TPE et de DAB.

3.6 Conclusions et recommandations

Cette étude a permis de montrer que, si les infrastructures de paiement par carte ne se montrent pas résilientes face au développement de la technologie quantique, elles seront menacées par des risques majeurs : la fin de la confidentialité des opérations de paiement, le vol de données, la génération de paiements frauduleux non identifiables *a priori*, des risques de réputation importants et une potentielle crise de confiance des usagers. Ce constat est généralisable à l'ensemble des infrastructures de paiement et menace donc la stabilité de nos économies.

Néanmoins, la réalisation de ce scénario catastrophe reste encore soumise à de nombreuses inconnues sur l'horizon de disponibilité d'ordinateurs quantiques suffisamment puissants pour casser les clés des algorithmes de chiffrement. Selon les experts, l'horizon serait de l'ordre de dix à vingt ans.

Le 4 mai 2022, le président des États-Unis a signé un mémorandum de sécurité nationale enjoignant aux administrations fédérales d'inventorier leurs dispositifs

de sécurité en vue d'établir une feuille de route, en collaboration avec l'industrie et le monde universitaire, pour une migration vers des algorithmes *post*-quantiques reconnus par le NIST [43]. L'industrie de la finance et des paiements étant également des secteurs sensibles, la Réserve fédérale (la Fed) s'investit dans cette dynamique et un groupe de travail dédié au chiffrement *post*-quantique a été ouvert au comité X9 de l'Institut national de normalisation américain [44].

En France, la loi de programmation militaire du 1er août 2023 [45] prévoit, dans le volet innovation des armées, une analyse technico-opérationnelle sur la thématique de la transition vers la cryptographie *post*-quantique.

Au-delà de la problématique sécuritaire, la menace quantique représente une opportunité industrielle d'envergure pour les entreprises françaises et européennes du secteur informatique, et l'occasion pour les acteurs du paiement de forger une position de *leadership* dans la standardisation de leurs protocoles.

L'Observatoire de la sécurité des moyens de paiement (OSMP) recommande dès à présent à l'ensemble des acteurs du paiement d'œuvrer à deux niveaux pour la préparation des projets de migration.

3.6.1 Anticiper les besoins au sein des acteurs du paiement

1) **Inventorier les différents dispositifs de sécurité des systèmes d'information, et évaluer les vulnérabilités notamment par rapport aux standards actuels et au risque quantique.**
   Il s'agit de réaliser l'inventaire des algorithmes cryptographiques utilisés dans l'ensemble des applications et logiciels utilisés dans les organisations, en interne ou en externe par l'intermédiaire d'Internet. Certains établissements disposent déjà de ce type de cartographie. Dans le cas contraire, des outils permettant la détection automatisée des algorithmes asymétriques dans les systèmes d'information seraient à implémenter. Le cas échéant, des contrôles manuels devraient être réalisés.
2) **Hiérarchiser les données selon leur degré de sensibilité.**
   Dès à présent, il s'agit de répertorier les données sensibles qui doivent rester confidentielles sur une très longue durée afin de s'assurer que leur méthode de chiffrement restera suffisamment robuste à cet horizon de temps [46].
3) **Réaliser des expériences d'implémentation d'algorithmes asymétriques.**
   Les choix cryptographiques ne sont pas triviaux en matière d'algorithmes asymétriques et leur implémentation requiert une certaine expérience. La migration aura des répercussions sur une large étendue de protocoles et d'infrastructures et soulèvera de nombreuses questions, allant des bibliothèques logicielles jusqu'au dimensionnement des serveurs. Le changement, voire la complexification des codes, associé respectivement à la crypto-agilité et à l'hybridation, devrait s'accompagner de tests et d'utilisation d'outils spécifiques pour analyser la réaction des dispositifs informatiques (Protocoles TLS, VPN, signatures électroniques, etc.). Ces expérimentations devraient être lancées sur les applications les plus sensibles afin de prioriser leur migration.
   Sur le long terme, un dispositif de surveillance devrait être mis en place dans l'établissement afin d'assurer une implémentation pertinente et continue des algorithmes *post*-quantiques en matière de paramétrage, de configuration et de cohérence globale des protocoles.
4) **Constituer une feuille de route au niveau de chaque acteur de la chaîne de paiement.**
   Une feuille de route, également appelée plan de transition *post*-quantique, validée à haut niveau dans chaque institution, doit éclairer les choix des équipes techniques en matière de renouvellement des équipements et logiciels en tenant compte de leurs différents cycles de vie et en priorisant les actions dans les domaines les plus sensibles. Pour les plus grandes institutions, le délai de migration de l'ensemble du système d'information est estimé au minimum à quatre ou cinq ans.
   En amont, une équipe projet dédiée devrait être constituée afin d'optimiser les scénarios de migration, les budgets associés et la formation nécessaire du personnel, sachant que les ingénieurs et les techniciens sur le marché risquent d'être très sollicités.

38 Cf. *https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf*

39 La PKI est un ensemble de technologies, de procédures et de logiciels conçus pour gérer de manière sécurisée le cycle de vie des certificats numériques.

40 SIKE (*Supersingular Isogeny Key Encapsulation*), cf. Castryck et Decru, « An Efficient Key Recovery Attack on SIDH », *Lecture Notes in Computer Science*, vol. 14008, Springer : https://link.springer.com/

41 Cf. Beullens, « Breaking Rainbow Takes a Weekend on a Laptop », *Paper 2022/14*, IBM Research, 2022 : *https://eprint.iacr.org/2022/214*

42 Le *National Institute of Standards and Technology* (NIST) est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des normes de concert avec l'industrie.

43 Cf. *https://www.whitehouse.gov/*

44 Cf. *https://x9.org/quantum-computing/*

45 Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la Défense nationale.

46 Le chiffrement AES-256 est recommandé par l'Anssi pour la conservation des données à froid.

3.6.2 Favoriser les économies d'échelle dans le secteur des paiements

5) **Sensibiliser les autorités de standardisation qui définissent la sécurité des protocoles de paiement.**
   À l'instar du NIST américain, les autorités de certification nationales et européennes devraient aider les organisations à identifier « où » et « comment » les algorithmes de chiffrement asymétrique sont utilisés dans leurs systèmes d'information. Elles doivent permettre une réduction du risque en fournissant *a minima* des outils, des guides et des pratiques (relatifs à la formation du personnel, aux procédures et à la technologie employée) qui peuvent être utilisés dans les organisations pour la planification du remplacement et de la mise à niveau du matériel, des logiciels et des services qui sont vulnérables à la menace quantique. Cette démarche devrait être réalisée en collaboration avec les professionnels des secteurs public et privé.
   Plus spécifiquement dans le secteur des paiements, les organismes de standardisation sont invités partager les principaux résultats des tests de migration réalisés en faisant ressortir les enjeux relatifs aux choix de migration intra-sectorielle. La définition de normes sur les algorithmes de chiffrement *post*-quantiques devra être souple et adaptative afin de tenir compte de la nécessité de l'hybridation et de la crypto-agilité. Enfin, des choix parmi les algorithmes *post*-quantiques devront s'imposer afin d'éviter la constitution de produits trop complexes freinant les migrations.
6) **Œuvrer à la création d'un groupe de travail pérenne de haut niveau, idéalement à l'échelle européenne, regroupant notamment les grandes institutions de paiement, les autorités publiques de supervision et de standardisation.**
   Le mandat consisterait à définir une feuille de route globale de migration de l'industrie des paiements, selon des jalons clairement définis, et d'en assurer le suivi.

À plus long terme, ce groupe de haut niveau pourrait servir d'instance de réflexion dans le secteur des paiements au déploiement de l'Internet quantique, l'Internet de demain dont la principale propriété est de prévenir toute tentative d'attaque extérieure sur la confidentialité des données.

ANNEXES

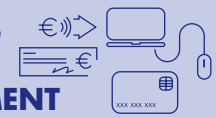
A1 CONSEILS DE PRUDENCE POUR L'UTILISATION DES MOYENS DE PAIEMENT

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

PREMIÈRE PARTIE – PRÉVENIR LA FRAUDE

FICHE 1

CONSEILS APPLICABLES À L'ENSEMBLE DES MOYENS DE PAIEMENT

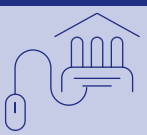


▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

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

FICHE 2

CONNEXION À L'ESPACE DE BANQUE EN LIGNE



▷ CONSEILS À DESTINATION DE TOUS LES CLIENTS

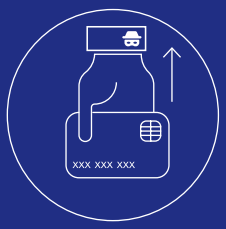
- Pour accéder à votre banque en ligne, choisissez un navigateur Internet connu, un moteur de recherche de confiance et pour les accès sur *smartphone* téléchargez l'application bancaire sur les magasins officiels d'applications.
- N'accédez pas à votre banque en ligne depuis un ordinateur public ou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

FICHE 3

CONSEILS APPLICABLES AUX PAIEMENTS PAR CARTE

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Campagnes
de *phishing* et *smishing*

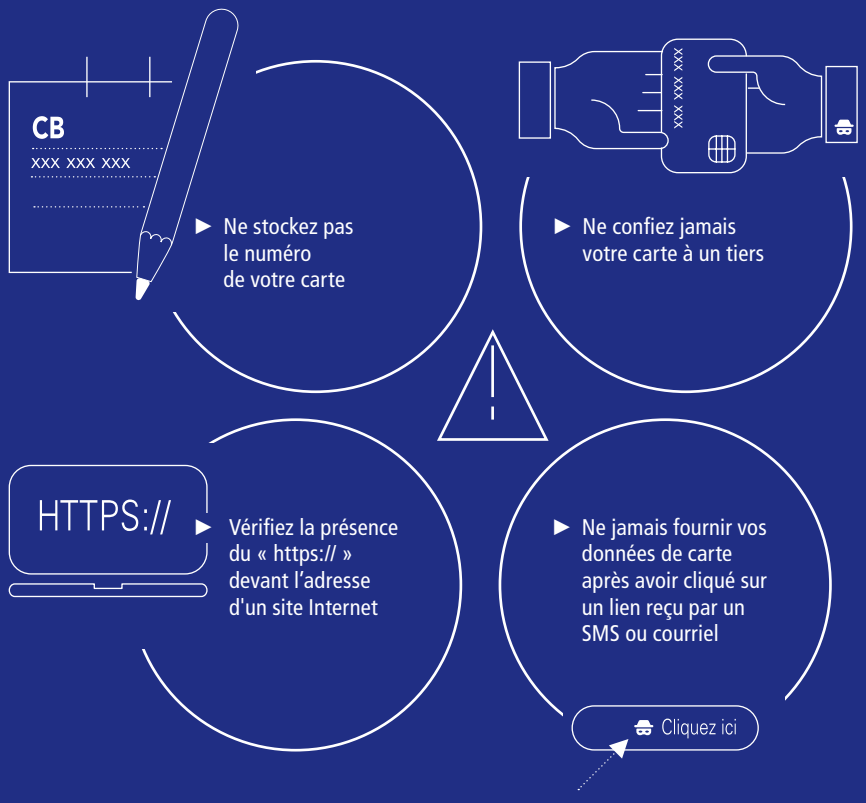


Vol de carte

Manipulation psychosociale

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

CONSEILS À DESTINATION DES UTILISATEURS



PRINCIPAUX CAS DE FRAUDE À LA CARTE RENCONTRÉS

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

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

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

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

▷ CONSEILS À DESTINATION DES UTILISATEURS DE CARTE DE PAIEMENT

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

▼ En pratique

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

2 • Si vous n'êtes pas satisfait par la réponse de votre banque, **soumettez votre litige au médiateur** désigné par votre banque à partir de deux mois après la date de votre première demande et dans un délai d'un an.

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

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

FICHE 4

CONSEILS APPLICABLES AUX VIREMENTS

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Ingénierie sociale

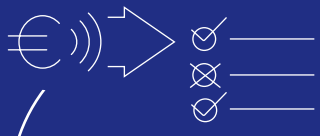
Logiciels malveillants

Campagnes
de *phishing* et *smishing*

CONSEILS À DESTINATION DES UTILISATEURS

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

- Mettez à jour vos systèmes d'exploitation et antivirus



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

PRINCIPAUX CAS DE FRAUDE AU VIREMENT RENCONTRÉS

▼ LES MANIPULATIONS PAR INGÉNIERIE SOCIALE

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

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

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

▼ LES ATTAQUES INFORMATIQUES

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

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

▷ CONSEILS À DESTINATION DE TOUS LES ÉMETTEURS DE VIREMENT

- Suivez les consignes de sécurité pour accéder à votre banque en ligne *(cf. fiche n° 2).*
- N'ajoutez comme bénéficiaire sur votre espace de banque en ligne que les personnes de confiance dont vous avez vérifié les coordonnées bancaires, le cas échéant par le biais d'un contre-appel.
- Mettez à jour régulièrement vos systèmes d'exploitation et déployez-y des antivirus.
- N'authentifiez que les opérations dont vous êtes à l'origine.

▷ CONSEILS À DESTINATION DES ENTREPRISES

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

FICHE 5

CONSEILS APPLICABLES AUX PRÉLÈVEMENTS

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS

Émission illégitime d'ordres de prélèvement

Usurpation d'IBAN

Entente frauduleuse entre le créancier et le débiteur

CONSEILS À DESTINATION DES UTILISATEURS

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

- Soyez vigilant sur la communication de votre IBAN

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

PRINCIPAUX CAS DE FRAUDE AU PRÉLÈVEMENT RENCONTRÉS

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

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

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

▷ CONSEILS À DESTINATION DE TOUS LES DÉBITEURS

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

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

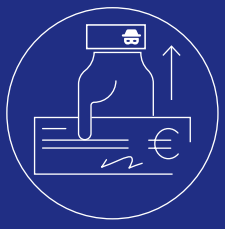
- Faites preuve de vigilance sur la communication de votre IBAN en la réservant à vos créanciers de confiance.

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

FICHE 6

CONSEILS APPLICABLES AUX CHÈQUES

PRINCIPAUX CAS DE FRAUDE RENCONTRÉS



Vol de chèque(s)
ou chèquier

Falsification
d'un chèque

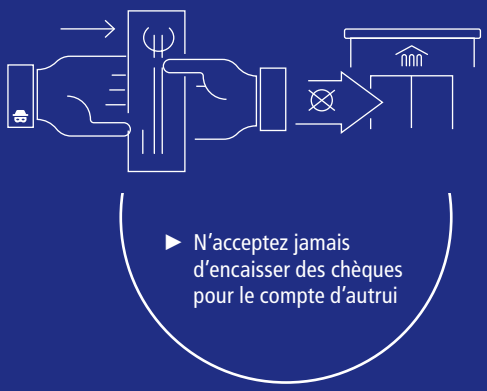
Contrefaçon
d'un chèque

Fraude à la « mule »

CONSEILS À DESTINATION DES UTILISATEURS

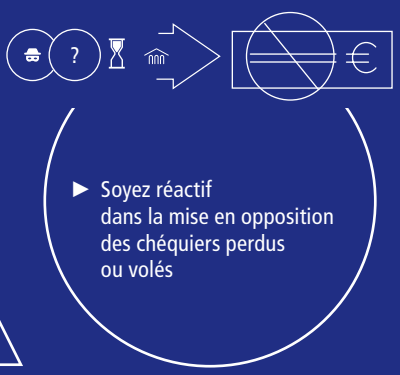
► Privilégiez la remise de chéquiers en agence

► Conservez votre chéquier en sécurité



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

► Restez vigilant lorsque vous acceptez un chèque



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

PRINCIPAUX CAS DE FRAUDE AU CHÈQUE RENCONTRÉS

▼ ORIGINE DES CHÈQUES FRAUDULEUX

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

▼ UTILISATION DES CHÈQUES FRAUDULEUX

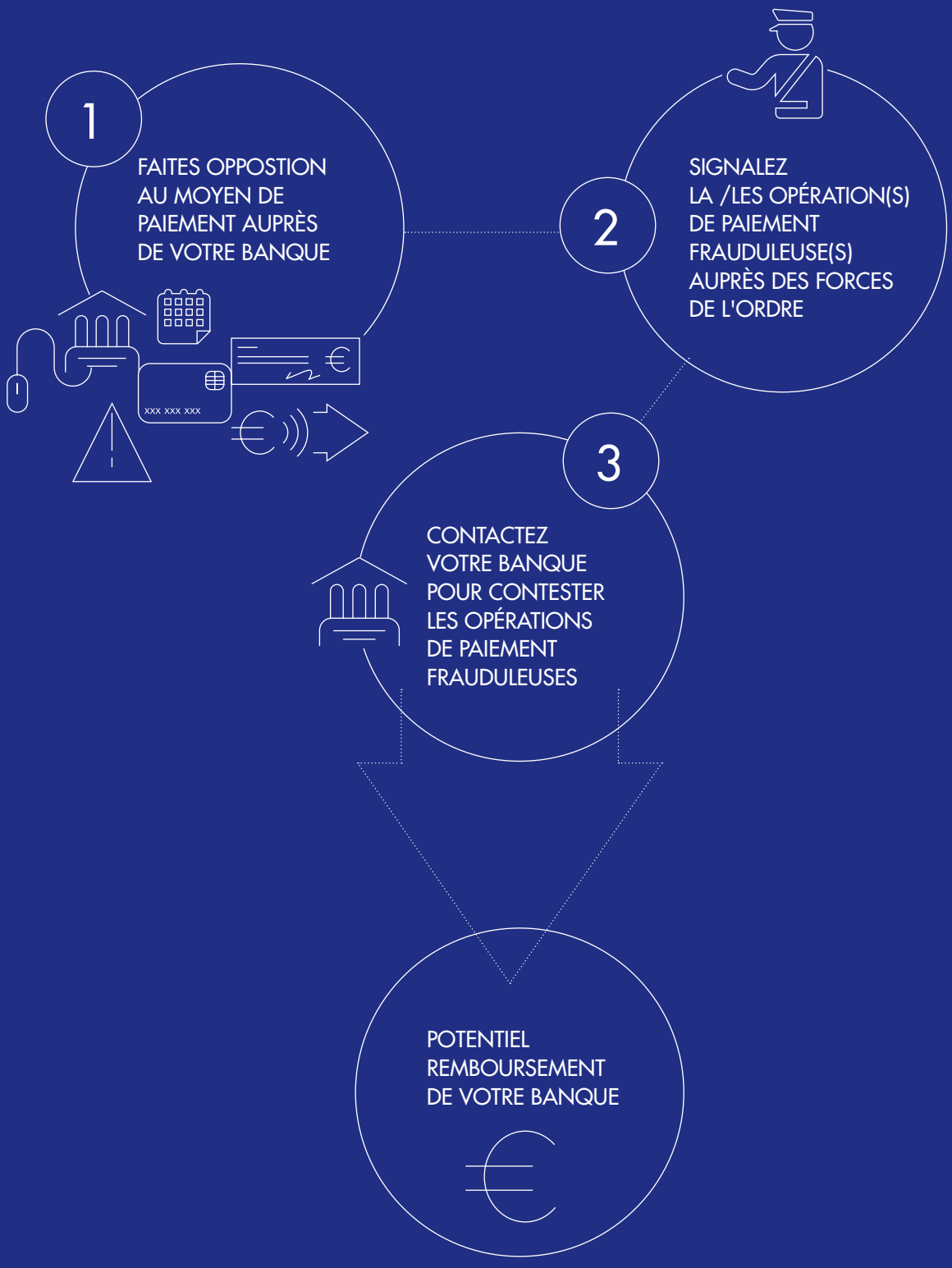
- Remise de chèques frauduleux à des bénéficiaires légitimes contre la remise de biens et de services (commerçants, sociétés de location, etc.)
- Processus de « cavalerie » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement d'un décaissement des fonds par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

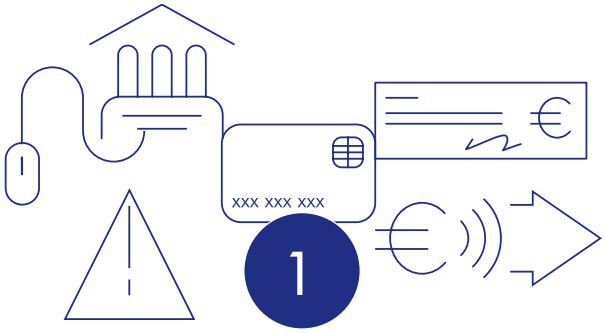
▷ CONSEILS À DESTINATION DE TOUS LES UTILISATEURS DE CHÈQUES

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

▷ CONSEILS À DESTINATION DES COMMERÇANTS

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


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



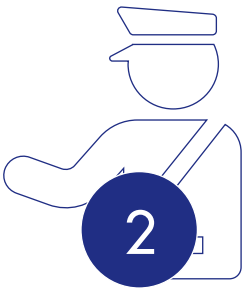
FAIRE OPPOSITION

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

▼ En pratique

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

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



SIGNALER LA FRAUDE AUPRÈS DES FORCES DE L'ORDRE

- **Il est recommandé de systématiquement signaler les cas de fraude aux moyens de paiement aux forces de l'ordre,** en privilégiant les démarches sur les plateformes Perceval pour les fraudes à la carte bancaire sur Internet et Thésée [1] pour les autres arnaques et escroqueries sur Internet, notamment dans le cas des fraudes au virement.

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

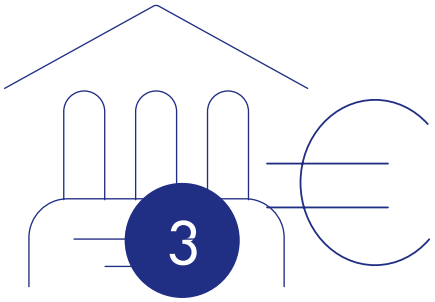
  Toutefois, l'utilisateur peut aussi porter plainte auprès d'un commissariat de police ou d'une unité de gendarmerie en cas de vol de votre moyen de paiement et en cas d'utilisation frauduleuse de celui-ci ou des données qui lui sont liées. Afin de gagner du temps lors de votre rendez-vous, une pré-plainte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

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

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

.../...

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



CONTACTER VOTRE BANQUE POUR POTENTIELLEMENT OBTENIR UN REMBOURSEMENT

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

▼ En pratique

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

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

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

▼ En pratique

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

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

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

Votre banque procédera alors sans délai au remboursement [2] de cette ou de ces opération(s) de paiement contestée(s) sauf si :

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

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

▼ En pratique

Plusieurs scénarios peuvent se produire :

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

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

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

Votre banque doit impérativement :

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

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

Le service dédié aux réclamations vous apportera une réponse qualitative et motivée le plus rapidement possible, et en tout état de cause dans un délai n'excédant pas deux mois, sauf dispositions plus contraignantes [3].

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

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

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

▼ En pratique

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

2 • Si vous n'êtes pas satisfait par la réponse de votre banque, **soumettez votre litige au médiateur** désigné par votre banque à partir de deux mois après la date de votre première demande et dans un délai d'un an.

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

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

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

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

A2 MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

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

PÉRIMÈTRE CONCERNÉ

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

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

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

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

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

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

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

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

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

ATTRIBUTIONS

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

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

En outre, le ministre chargé de l'Économie et des Finances peut, aux termes de l'article R. 141-2 du Code monétaire et financier, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

COMPOSITION

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

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

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

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

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

MODALITÉS DE FONCTIONNEMENT

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

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

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

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

A3 LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

En application de l'article R. 142-22 du Code monétaire et financier, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre de l'Économie. Le dernier arrêté de nomination date du 17 janvier 2024.

PRÉSIDENT

Denis BEAU
Premier sous-gouverneur de la Banque de France

REPRÉSENTANTS DU PARLEMENT

Éric BOCQUET
Sénateur

Michaël TAVERNE
Député

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

- La secrétaire générale ou son représentant :
  Nathalie AUFAUVRE

REPRÉSENTANTS DES ADMINISTRATIONS

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

Sur proposition du ministre de l'Économie, de l'Industrie et du Numérique :
- La directrice générale de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse ou son représentant :
  Cécile DUBARRY
- Le directeur général du Trésor ou son représentant :
  Jean-Baptiste BERNARD
- Le président de l'Institut d'émission des départements d'outre-mer (IEDOM) et directeur général de l'Institut d'émission d'outre-mer (IEOM) :
  Ivan ODONNAT
- La cheffe de bureau à la direction générale de la concurrence, de la consommation et de la répression des fraudes :
  Marie-Hélène AUFFRET

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

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

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

REPRÉSENTANTS DES ÉMETTEURS DE MOYENS DE PAIEMENT

Thomas GOUSSEAU
Association française des établissements de paiement et de monnaie électronique (Afepame)

Corinne DENAEYER
Association française des sociétés financières (ASF)

Sébastien MARINOT
BNP Paribas

Mireille MERCIER
Office de coordination bancaire et financière (OCBF)

Jean-Paul ALBERT
Société Générale

Évelyne BOTTOLLIER-CURTET
Groupe BPCE

Jérôme RAGUÉNÈS
Fédération bancaire française (FBF)

Marie-Anne LIVI
Crédit Agricole

REPRÉSENTANTS DES OPÉRATEURS DE SYSTÈMES DE PAIEMENT

Sophie MAHUSSIER
American Express France

Violette BOUVERET
Mastercard France

Philippe LAULANIE
Groupement des cartes bancaires

Romain BOISSON
Visa Europe France

Régis FOLBAUM
STET

Pierre-Emmanuel DEGERMANN
Worldline

Narinda YOU
EPI Company

REPRÉSENTANTS DES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES

Romain BONENFANT
Fédération Française des Télécoms

Amélia NEWSOM-DAVIS
Association française de Multimédia Mobile (AF2M)

REPRÉSENTANTS DES CONSOMMATEURS

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

Mélissa HOWARD
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN
Union nationale des associations familiales (Unaf)

Hervé MONDANGE
Association Force ouvrière consommateurs (Afoc)

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

REPRÉSENTANTS DES COMMERÇANTS ET DES ENTREPRISES

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

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

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

Bertrand PINEAU
Mercatel

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

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

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

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

REPRÉSENTANTS D'ASSOCIATIONS DE PERSONNES EN SITUATION DE HANDICAP

Hamou BOUAKKAZ
Valentin Haüy

Nicolas MERILLE
APF France Handicap

PERSONNALITÉS QUALIFIÉES

Marie-Christine CAFFET
Médiation bancaire

David NACCACHE
École normale supérieure (ENS)

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

CADRE GÉNÉRAL

Définition de la fraude aux moyens de paiement

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

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

Transactions couvertes

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

Sont également exclus de la fraude :

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

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

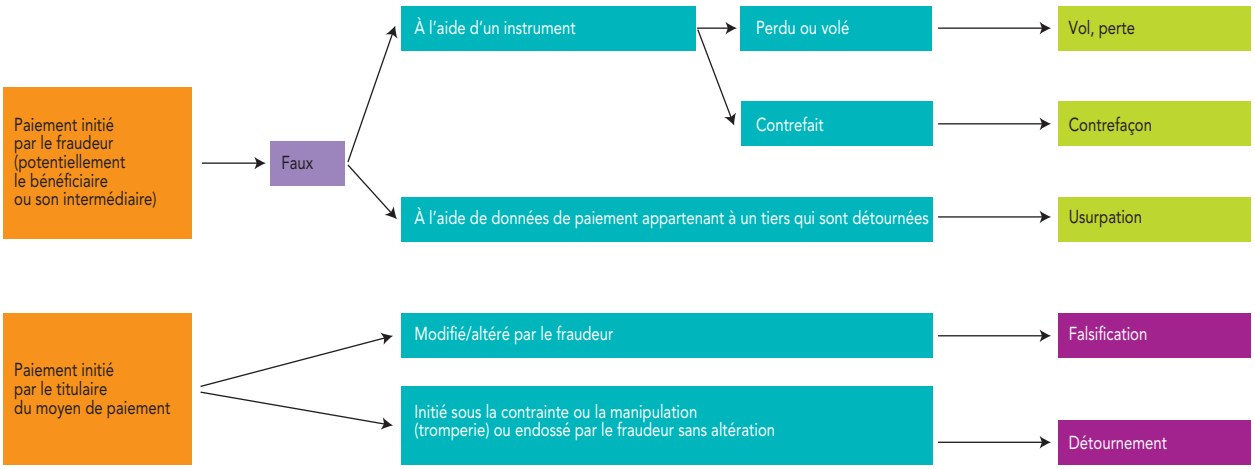
Origine des données de fraude

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

1 Ces orientations ont été établies au titre de l'article 96, paragraphe 6, de la deuxième directive européenne concernant les services de paiements dans le marché intérieur (Directive UE 2015/2366 dite « DSP 2 »).

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

Présentation schématique des différentes typologies de fraude



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

Typologie de la fraude aux moyens de paiement

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

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

Ventilation géographique de la fraude aux moyens de paiement

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

MESURE DE LA FRAUDE À LA CARTE DE PAIEMENT

Transactions couvertes

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

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 3-D Secure avec authentification forte	Paiement réalisé sur Internet au travers de l'infrastructure 3-D Secure avec une authentification forte du porteur.
Paiement hors 3D-Secure avec authentification forte	Paiement réalisé sur Internet, en dehors de l'infrastructure 3D-Secure, avec une authentification forte déléguée à un tiers, conformément aux règles d'externalisation applicables dans le cadre de la DSP 2 (exemple : portefeuille mobile de type *X-Pay* proposé sous la responsabilité de l'émetteur, délégation de l'authentification forte auprès du commerçant sous la responsabilité de l'émetteur, etc.).
Paiement 3-D Secure sans authentification forte	Paiement réalisé sur Internet au travers de l'infrastructure 3-D Secure sans authentification forte du porteur, c'est-à-dire en appliquant une exemption prévue par la réglementation européenne issue de la deuxième directive européenne sur les services de paiement (DSP 2) ou en cas d'incident ne permettant pas de la mettre en œuvre. Les authentifications monofacteurs (exemple : SMS OTP – *one time password* – seul) sont également comprises dans cette catégorie.
Paiement non authentifié	Tout paiement réalisé en dehors de l'infrastructure 3-D Secure, recouvrant : • paiement non assujetti aux règles européennes sur l'authentification forte (DSP 2) [a], comme le paiement initié par le créancier sur la base d'un accord préexistant entre le payeur et le créancier pour l'effectuer (par exemple : *Merchant Initiated Transaction* – MIT) et le paiement dit « *one-leg* » (l'émetteur ou l'acquéreur du paiement est situé hors de l'Union européenne) ; • paiement assujetti aux règles européennes sur l'authentification forte, mais dont le motif d'exemption à l'authentification forte est formalisé dans le flux d'autorisation ; • paiement assujetti aux règles européennes sur l'authentification forte, mais non conforme.

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

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

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

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

MESURE DE LA FRAUDE AU VIREMENT

Instruments de paiement couverts

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

Origine des données de fraude

Les données de fraude au virement sont fournies par la Banque de France et proviennent des déclarations réglementaires semestrielles de fraude qui lui sont faites par les prestataires de services de paiement [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, sont effectuées à partir de l'ancienne approche de fraude brute.

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

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

MESURE DE LA FRAUDE AUX EFFETS DE COMMERCE

Instruments de paiement couverts

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

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

Typologie et origine des données de fraude

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

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

MESURE DE LA FRAUDE SUR LES OPÉRATIONS DE TRANSMISSION DE FONDS

Service de paiement couvert

Les opérations de transmission de fonds correspondent au service de paiement 6° établi à l'article L. 314-1 du Code monétaire et financier, conformément aux dispositions de la deuxième directive européenne sur les services de paiement (DSP 2). Il s'agit d'un service de paiement pour lequel les fonds sont reçus de la part d'un payeur, sans création de comptes de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, et/ou pour lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci.

Origine des données sur la fraude

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

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

Service de paiement couvert

Le service d'initiation de paiement correspond au service de paiement 7° établi à l'article L. 314-1 du Code monétaire et financier, conformément aux dispositions de la DSP 2. Il s'agit d'un service consistant à initier via un prestataire de service d'initiation de paiement (PSIP) agréé un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement (PSP). Cette opération prend généralement la forme d'un virement.

Origine des données sur la fraude

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

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

DISPOSITIONS SPÉCIFIQUES POUR LA FRAUDE SUR LES TRANSACTIONS EN MONNAIE ÉLECTRONIQUE

Instruments de paiement couverts

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

On distingue deux catégories de support de monnaie électronique :

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

Origine des données sur la fraude

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

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

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

Des tableaux complémentaires, ainsi que l'ensemble des tableaux contenus dans cette annexe, sont disponibles pour téléchargement à l'adresse suivante :
https://www.banque-france.fr/system/files/2024-09/rapport-osmp-2023_dossier-statistique_annexe-5.pdf

PANORAMA DES MOYENS DE PAIEMENT

T1 Cartographie des moyens de paiement scripturaux en 2023

(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
	2023	Variation 2023/2022	Part	2023	Variation 2023/2022	Part	
Paiement carte [a]	19 685	7,8	61,1	806	8,1	2,3	41
dont sans contact	*10 792*	*18,6*	*33,5*	*175*	*18,0*	*0,5*	*16*
dont paiement par mobile	*1 609*	*90,4*	*5,0*	*36*	*98,1*	*0,1*	*22*
Chèque	891	- 11,6	2,8	467	- 13,4	1,4	524
Virement	5 658	9,7	17,6	30 589	- 21,4	89,0	5 407
dont VGM [b]	*73*	*279,8*	*0,2*	*8 758*	*- 44,9*	*25,5*	*119 689*
dont virement instantané (SCT Inst)	*364*	*83,9*	*1,1*	*174*	*46,3*	*0,5*	*478*
Prélèvement	4 621	- 6,0	14,3	2 139	4,8	6,2	463
Effet de commerce	120	59,5	0,4	217	- 2,0	0,6	1 812
Monnaie électronique	97	29,7	0,3	1	144,5	0,0	13
Transmission de fonds	8	120,5	0,0	1	33,8	0,0	146
Total	**31 080**	**5,4**	**96,5**	**34 222**	**- 19,4**	**99,6**	**1 101**
Retrait par carte [a]	1 127	- 0,8	3,5	136	2,0	0,4	120
Total transactions	**32 207**	**5,2**	**100,0**	**34 357**	**- 19,3**	**100,0**	**1 067**

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

Source : Observatoire de la sécurité des moyens de paiement.

T2 Évolution historique des paiements scripturaux

a) En volume

(en millions de transactions)

	2016	2017	2018	2019	2020	2021	2022	2023
Carte	11 134	12 581	13 179	14 485	13 852	16 129	18 258	19 685
dont sans contact	*635*	*1 300*	*2 374*	*3 779*	*5 159*	*7 369*	*9 103*	*10 792*
dont par mobile	*0*	*5*	*11*	*48*	*129*	*357*	*845*	*1 609*
Chèque	2 137	1 927	1 747	1 587	1 175	1 106	1 008	891
Virement	3 753	3 870	4 038	4 269	4 483	4 843	5 158	5 658
dont virement instantané (SCT Inst)	*nd*	*nd*	*0*	*14*	*45*	*107*	*198*	*364*
Prélèvement	3 963	4 091	4 211	4 370	4 622	5 020	4 914	4 621
Effet de commerce	82	81	81	78	71	75	75	120
Monnaie électronique	38	55	65	62	36	63	75	97
Transmission de fonds	20	18	16	16	15	2	3	8
Total paiements scripturaux	**21 107**	**22 605**	**23 320**	**24 851**	**24 238**	**27 238**	**29 491**	**31 080**
Retrait par carte	1 491	1 481	1 439	1 392	1 064	1 086	1 136	1 127

b) En montant

(en milliards d'euros)

	2016	2017	2018	2019	2020	2021	2022	2023
Carte	499	530	568	600	578	660	746	806
dont sans contact	*7*	*13*	*25*	*43*	*80*	*125*	*148*	*175*
dont par mobile	*0,005*	*0,1*	*0,2*	*1*	*3*	*8*	*18*	*36*
Chèque	1 077	1 002	891	814	614	589	540	467
Virement	23 697	24 069	24 296	25 164	32 712	38 723	38 895	30 589
dont virement instantané (SCT Inst)	*nd*	*nd*	*0,086*	*7*	*27*	*50*	*119*	*174*
Prélèvement	1 492	1 579	1 645	1 711	1 684	1 895	2 041	2 139
Effet de commerce	266	260	252	232	197	212	222	217
Monnaie électronique	1	1	1	1	1	1	1	1
Transmission de fonds	0,8	1,6	2	2	2	1	1	1
Total paiements scripturaux	**27 032**	**27 440**	**27 653**	**28 522**	**35 786**	**42 081**	**42 445**	**34 222**
Retrait par carte	129	135	137	137	116	124	133	136

nd, non disponible.

Note : SCT Inst, SEPA *Instant Credit Transfer*.

Source : Observatoire de la sécurité des moyens de paiement.

T3 Répartition de la fraude sur les moyens de paiement en 2023

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

	Volume			Valeur			Taux de fraude	Montant moyen
	2023	Variation 2023/2022	Part	2023	Variation 2023/2022	Part	2023	
Paiement carte [a]	6 635 955	- 0,9	93,2	455 204 894	8,2	38,1	0,0564	69
dont sans contact	*733 359*	*- 7,9*	*10,3*	*18 786 086*	*- 18,5*	*1,6*	*0,0108*	*26*
dont par mobile	*110 133*	*- 32,4*	*1,5*	*7 294 895*	*- 33,3*	*0,6*	*0,0205*	*66*
Chèque (nouvelle approche) [b]	203 514	- 6,7	2,9	363 549 771	- 8,1	30,4	0,0778	1 786
Chèque (ancienne approche)	253 338	- 4,8	3,6	585 506 445	5,2	49,0	0,1253	2 311
Virement	90 436	17,7	1,3	311 627 465	- 0,5	26,1	0,0010	3 446
dont virement instantané (SCT Inst)	*48 630*	*46,5*	*0,7*	*69 003 730*	*30,8*	*5,8*	*0,0396*	*1 419*
Prélèvement	77 876	57,5	1,1	22 320 813	12,4	1,9	0,0010	287
Effet de commerce	34	3 300,0	0,0	1 296 652	10 634,8	0,1	0,0006	38 137
Monnaie électronique	4 310	121,6	0,1	251 938	225,7	0,0	0,0201	58
Transmission de fonds	102	- 33,8	0,0	55 333	- 28,3	0,0	0,0049	542
Total paiements	**7 012 227**	**- 0,4**	**98,5**	**1 154 306 867**	**0,4**	**96,6**	**0,0053**	**165**
Retrait par carte [a]	110 221	- 10,8	1,5	40 608 913	- 5,9	3,4	0,0300	368
Total transactions	**7 122 448**	**- 0,6**	**100,0**	**1 194 915 780**	**0,2**	**100,0**	**0,0043**	**168**

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

Source : Observatoire de la sécurité des moyens de paiement.

T4 Évolution historique de la fraude sur les moyens de paiement

a) En volume
(en unités)

	2016	2017	2018	2019	2020	2021	2022	2023
Carte	5 300 847	5 364 312	6 068 959	7 071 095	7 421 137	6 764 752	6 692 988	6 635 955
dont sans contact	*125 860*	*248 991*	*445 919*	*603 509*	*537 061*	*604 278*	*796 027*	*733 359*
dont par mobile	*nd*	*22*	*2 070*	*3 494*	*33 761*	*83 266*	*162 869*	*110 133*
Chèque (nouvelle approche)	nd	nd	nd	nd	190 001	232 277	218 122	203 514
Chèque (ancienne approche)	120 295	114 906	166 421	183 488	220 685	272 970	266 216	253 338
Virement	5 585	4 642	7 736	15 934	35 893	46 718	76 846	90 436
dont virement instantané (SCT Inst)	*nd*	*nd*	*5*	*729*	*7 131*	*12 913*	*33 193*	*48 630*
Prélèvement	1 176	25 801	309 377	43 519	6 485	251 010	49 453	77 876
Effet de commerce	4	3	5	1	62	1	1	34
Monnaie électronique	nd	nd	nd	nd	nd	2 001	1 945	4 310
Transmission de fonds	nd	nd	nd	nd	nd	962	154	102
Total fraude paiements scripturaux	**5 427 907**	**5 509 664**	**6 552 498**	**7 314 037**	**7 684 262**	**7 297 721**	**7 039 509**	**7 012 227**
Retrait par carte	202 158	177 562	158 908	165 505	113 067	129 083	123 574	110 221
Total fraude transactions	**5 630 065**	**5 687 226**	**6 711 406**	**7 479 542**	**7 797 329**	**7 426 804**	**7 163 083**	**7 122 448**

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

Source : Observatoire de la sécurité des moyens de paiement.

b) En valeur
(en euros)

	2016	2017	2018	2019	2020	2021	2022	2023
Carte	378 455 912	344 962 084	401 604 986	428 249 931	439 489 315	421 410 285	420 585 823	455 204 894
dont sans contact	*1 410 566*	*2 748 790*	*5 234 852*	*8 479 354*	*11 292 261*	*16 274 668*	*23 047 180*	*18 786 086*
dont par mobile	*nd*	*1 227*	*73 682*	*216 236*	*2 792 574*	*5 610 270*	*10 942 984*	*7 294 895*
Chèque (nouvelle approche)	nd	nd	nd	nd	401 611 189	465 021 167	395 416 196	363 549 771
Chèque (ancienne approche)	276 716 554	296 072 847	450 108 464	539 215 175	538 059 139	625 703 442	556 796 815	585 506 445
Virement	86 284 101	78 286 492	97 327 128	161 642 174	266 969 099	287 264 068	313 163 442	311 627 465
dont virement instantané (SCT Inst)	*nd*	*nd*	*29 800*	*2 203 240*	*10 562 419*	*22 406 942*	*52 768 218*	*69 003 730*
Prélèvement	39 935 882	8 726 403	58 346 253	10 990 025	1 891 051	25 318 677	19 853 012	22 320 813
Effet de commerce	1 018 149	153 100	226 217	74 686	538 918	12 079	12 079	1 296 652
Monnaie électronique	nd	nd	nd	nd	nd	137 340	77 349	251 938
Transmission de fonds	nd	nd	nd	nd	nd	246 362	77 162	55 333
Total fraude paiements scripturaux	**782 410 598**	**728 200 926**	**1 007 613 048**	**1 140 171 991**	**1 246 947 522**	**1 199 409 978**	**1 149 185 062**	**1 154 306 867**
Retrait par carte	48 650 966	42 038 924	37 630 659	41 651 788	33 950 879	42 950 169	43 148 054	40 608 913
Total fraude transactions	**831 061 564**	**770 239 850**	**1 045 243 707**	**1 181 823 779**	**1 280 898 401**	**1 242 360 147**	**1 192 333 116**	**1 194 915 780**

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

Source : Observatoire de la sécurité des moyens de paiement.

T5 Paiements par carte émise en France

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

	2018		2019		2020	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**11 222 954**	**443 193 792**	**12 171 755**	**459 066 750**	**11 193 795**	**424 105 649**
dont paiements sans contact (y compris paiements par mobile)	*2 374 029*	*25 219 537*	*3 778 756*	*42 903 452*	*5 159 657*	*79 664 370*
dont paiements par mobile	*11 399*	*200 876*	*47 885*	*850 983*	*129 105*	*2 734 667*
Paiements à distance (hors internet)	**63 021**	**4 696 704**	**77 150**	**4 838 911**	**134 114**	**7 567 877**
Paiements sur internet	**1 893 443**	**119 903 848**	**2 236 049**	**135 352 563**	**2 524 317**	**146 563 476**
Retraits	**1 439 414**	**136 638 334**	**1 391 930**	**136 507 651**	**1 064 095**	**115 958 207**
Total	**14 618 833**	**704 432 677**	**15 876 884**	**735 765 875**	**14 916 322**	**694 195 208**

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)

	2021		2022		2023	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**12 935 438**	**475 079 750**	**14 868 338**	**537 503 850**	**15 903 747**	**570 896 450**
dont paiements sans contact (y compris paiements par mobile)	*7 368 699*	*125 082 420*	*9 102 931*	*148 006 593*	*10 792 452*	*174 706 103*
dont paiements par mobile	*357 355*	*7 596 769*	*845 223*	*17 937 091*	*1 609 423*	*35 539 253*
Paiements à distance (hors internet)	**76 931**	**7 995 010**	**105 781**	**16 994 865**	**96 368**	**15 880 261**
Paiements sur internet	**3 116 285**	**177 056 237**	**3 283 604**	**191 418 128**	**3 685 180**	**219 662 525**
dont paiements 3-D Secure avec authentification forte	*787 664*	*85 221 641*	*1 034 950*	*112 713 734*	*1 282 644*	*136 151 668*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*nd*	*135 611*	*4 119 307*
dont paiements 3-D Secure sans authentification forte	*444 723*	*19 267 910*	*781 313*	*27 091 534*	*800 728*	*27 212 160*
dont paiements hors 3-D Secure sans authentification forte	*1 883 898*	*72 566 685*	*1 467 342*	*51 612 860*	*1 466 199*	*52 179 389*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*877 839*	*30 771 262*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*nd*	*31 151*	*1 997 096*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*250 843*	*9 039 674*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*306 366*	*10 371 359*
Retraits	**1 086 289**	**123 867 648**	**1 135 675**	**132 879 066**	**1 127 043**	**135 511 148**
Total	**17 214 942**	**783 998 644**	**19 393 398**	**878 795 909**	**20 812 338**	**941 950 384**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

T5 *bis* Nombre de cartes et supports

T6 Transactions frauduleuses par carte émise en France

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

	2018			2019			2020		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**1 142 861**	**64 546 992**	**0,015**	**1 203 233**	**64 992 145**	**0,014**	**972 228**	**47 994 762**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	*445 919*	*5 234 852*	*0,021*	*603 509*	*8 479 354*	*0,020*	*537 061*	*11 292 261*	*0,014*
dont paiements par mobile	*2 070*	*73 682*	*0,037*	*3 494*	*216 236*	*0,025*	*33 761*	*2 792 574*	*0,102*
Paiements à distance (hors internet)	**406 712**	**28 562 421**	**0,608**	**409 319**	**31 806 788**	**0,657**	**411 344**	**26 899 103**	**0,355**
Paiements sur internet	**4 519 386**	**308 495 573**	**0,257**	**5 458 543**	**331 450 998**	**0,245**	**6 037 565**	**364 595 450**	**0,249**
Retraits	**158 908**	**37 630 659**	**0,028**	**165 505**	**41 651 788**	**0,031**	**113 067**	**33 950 879**	**0,029**
Total	**6 227 867**	**439 235 645**	**0,062**	**7 236 600**	**469 901 719**	**0,064**	**7 534 204**	**473 440 194**	**0,068**

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)

	2021			2022			2023		
	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	**942 376**	**52 426 587**	**0,011**	**1 055 575**	**62 861 464**	**0,012**	**966 134**	**61 618 923**	**0,011**
dont paiements sans contact (y compris paiements par mobile)	*604 278*	*16 274 668*	*0,013*	*796 027*	*23 047 180*	*0,016*	*733 359*	*18 786 086*	*0,011*
dont paiements par mobile	*83 266*	*5 610 270*	*0,074*	*162 869*	*10 942 984*	*0,061*	*110 133*	*7 294 895*	*0,021*
Paiements à distance (hors internet)	**124 596**	**22 193 382**	**0,278**	**174 364**	**42 028 102**	**0,247**	**186 499**	**42 177 372**	**0,266**
Paiements sur internet	**5 697 780**	**346 790 316**	**0,196**	**5 463 049**	**315 696 257**	**0,165**	**5 483 322**	**351 408 599**	**0,160**
dont paiements 3-D Secure avec authentification forte	*496 017*	*103 029 680*	*0,121*	*624 473*	*124 258 815*	*0,110*	*722 396*	*132 754 198*	*0,098*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*159 680*	*8 966 661*	*0,218*
dont paiements 3-D Secure sans authentification forte	*364 223*	*26 046 078*	*0,135*	*625 296*	*25 695 176*	*0,095*	*593 808*	*22 929 848*	*0,084*
dont paiements hors 3-D Secure sans authentification forte	*4 837 540*	*217 714 555*	*0,300*	*4 213 280*	*165 742 266*	*0,321*	*4 007 438*	*186 757 892*	*0,358*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*1 995 881*	*87 685 148*	*0,285*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*416 116*	*30 632 806*	*1,534*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*553 018*	*16 515 229*	*0,183*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*1 042 423*	*51 924 709*	*0,501*
Retraits	**129 083**	**42 950 169**	**0,035**	**123 574**	**43 148 054**	**0,032**	**110 221**	**40 608 913**	**0,030**
Total	**6 893 835**	**464 360 454**	**0,059**	**6 816 562**	**463 733 877**	**0,053**	**6 746 176**	**495 813 807**	**0,053**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2023

(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	**647 705**	**67,0**	**37 753 346**	**61,3**	**14 720**	**1,5**	**2 065 985**	**3,4**	**86 229**	**8,9**	**5 180 634**	**8,4**
dont paiements sans contact (y compris paiements par mobile)	*518 047*	*70,6*	*12 067 959*	*64,2*	*5 286*	*0,7*	*115 996*	*0,6*	*69 048*	*9,4*	*2 927 912*	*15,6*
dont paiements par mobile	*46 558*	*42,3*	*3 459 004*	*47,4*	*363*	*0,3*	*32 991*	*0,5*	*32 390*	*29,4*	*2 053 646*	*28,2*
Paiements à distance (hors internet)	**16 273**	**8,7**	**3 188 540**	**7,6**	**111**	**0,1**	**8 899**	**0,0**	**472**	**0,3**	**147 974**	**0,4**
Paiements sur internet	**324 358**	**5,9**	**23 817 989**	**6,8**	**2 992**	**0,1**	**192 755**	**0,1**	**238 292**	**4,3**	**10 280 753**	**2,9**
dont paiements 3-D Secure avec authentification forte	*52 736*	*7,3*	*9 924 112*	*7,5*	*532*	*0,1*	*61 051*	*0,0*	*6 645*	*0,9*	*1 117 341*	*0,8*
dont paiements hors 3-D Secure avec authentification forte	*3 728*	*2,3*	*192 619*	*2,1*	*116*	*0,1*	*9 855*	*0,1*	*4 639*	*2,9*	*286 923*	*3,2*
dont paiements 3-D Secure sans authentification forte	*22 800*	*3,8*	*1 671 647*	*7,3*	*183*	*0,0*	*7 603*	*0,0*	*11 712*	*2,0*	*330 786*	*1,4*
dont paiements hors 3-D Secure sans authentification forte	*245 094*	*6,1*	*12 029 611*	*6,4*	*2 161*	*0,1*	*114 246*	*0,1*	*215 296*	*5,4*	*8 545 703*	*4,6*
dont paiements initiés par le commerçant (MIT)	*202 601*	*10,2*	*8 584 383*	*9,8*	*1 089*	*0,1*	*35 474*	*0,0*	*37 263*	*1,9*	*1 503 421*	*1,7*
dont paiements « one-leg »	*11 328*	*2,7*	*1 325 783*	*4,3*	*344*	*0,1*	*22 250*	*0,1*	*14 413*	*3,5*	*1 318 207*	*4,3*
dont paiements non 3-D Secure conformes à la DSP 2	*11 492*	*2,1*	*445 549*	*2,7*	*454*	*0,1*	*11 864*	*0,1*	*2 012*	*0,4*	*45 446*	*0,3*
dont paiements non 3-D Secure non conformes à la DSP 2	*19 673*	*1,9*	*1 673 896*	*3,2*	*274*	*0,0*	*44 658*	*0,1*	*161 608*	*15,5*	*5 678 629*	*10,9*
Retraits	**83 317**	**75,6**	**32 189 560**	**79,3**	**4 657**	**4,2**	**1 593 329**	**3,9**	**3 354**	**3,0**	**843 585**	**2,1**
Total	**1 071 653**	**15,9**	**96 949 435**	**19,6**	**22 480**	**0,3**	**3 860 968**	**0,8**	**328 347**	**4,9**	**16 452 946**	**3,3**

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

Source : Observatoire de la sécurité des moyens de paiement.

T7 Typologies de la fraude sur les paiements par carte émise en France en 2023 (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	**30 089**	**3,1**	**3 023 807**	**4,9**	**187 391**	**19,4**	**13 595 151**	**22,1**	**966 134**	**61 618 923**
dont paiements sans contact (y compris paiements par mobile)	*18 656*	*2,5*	*724 062*	*3,9*	*122 322*	*16,7*	*2 950 157*	*15,7*	*733 359*	*18 786 086*
dont paiements par mobile	*9 488*	*8,6*	*450 353*	*6,2*	*21 334*	*19,4*	*1 298 901*	*17,8*	*110 133*	*7 294 895*
Paiements à distance (hors internet)	**169 058**	**90,6**	**38 780 374**	**91,9**	**585**	**0,3**	**51 585**	**0,1**	**186 499**	**42 177 372**
Paiements sur internet	**4 897 807**	**89,3**	**313 568 198**	**89,2**	**19 873**	**0,4**	**3 548 904**	**1,0**	**5 483 322**	**351 408 599**
dont paiements 3-D Secure avec authentification forte	*660 474*	*91,4*	*120 457 312*	*90,7*	*2 009*	*0,3*	*1 194 382*	*0,9*	*722 396*	*132 754 198*
dont paiements hors 3-D Secure avec authentification forte	*150 056*	*94,0*	*8 392 243*	*93,6*	*1 141*	*0,7*	*85 021*	*0,9*	*159 680*	*8 966 661*
dont paiements 3-D Secure sans authentification forte	*557 980*	*94,0*	*20 816 973*	*90,8*	*1 133*	*0,2*	*102 839*	*0,4*	*593 808*	*22 929 848*
dont paiements hors 3-D Secure sans authentification forte	*3 529 297*	*88,1*	*163 901 670*	*87,8*	*15 590*	*0,4*	*2 166 662*	*1,2*	*4 007 438*	*186 757 892*
dont paiements initiés par le commerçant (MIT)	*1 751 336*	*87,7*	*77 429 884*	*88,3*	*3 592*	*0,2*	*131 986*	*0,2*	*1 995 881*	*87 685 148*
dont paiements « one-leg »	*385 102*	*92,5*	*27 090 943*	*88,4*	*4 929*	*1,2*	*875 623*	*2,9*	*416 116*	*30 632 806*
dont paiements non 3-D Secure conformes à la DSP 2	*537 238*	*97,1*	*15 705 353*	*95,1*	*1 822*	*0,3*	*307 017*	*1,9*	*553 018*	*16 515 229*
dont paiements non 3-D Secure non conformes à la DSP 2	*855 621*	*82,1*	*43 675 490*	*84,1*	*5 247*	*0,5*	*852 036*	*1,6*	*1 042 423*	*51 924 709*
Retraits	**550**	**0,5**	**102 577**	**0,3**	**18 343**	**16,6**	**5 879 862**	**14,5**	**110 221**	**40 608 913**
Total	**5 097 504**	**75,6**	**355 474 956**	**71,7**	**226 192**	**3,4**	**23 075 502**	**4,7**	**6 746 176**	**495 813 807**

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

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2023

(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	**885 533**	**91,7**	**50 277 021**	**81,6**	**41 656**	**4,3**	**3 477 134**	**5,6**
dont paiements sans contact (y compris paiements par mobile)	*684 776*	*93,4*	*15 698 156*	*83,6*	*29 640*	*4,0*	*1 600 923*	*8,5*
dont paiements par mobile	*98 610*	*89,5*	*6 066 551*	*83,2*	*3 091*	*2,8*	*336 438*	*4,6*
Paiements à distance (hors internet)	**118 903**	**63,8**	**22 602 626**	**53,6**	**28 029**	**15,0**	**8 936 220**	**21,2**
Paiements sur internet	**1 913 224**	**34,9**	**152 815 486**	**43,5**	**2 349 387**	**42,8**	**120 406 288**	**34,3**
dont paiements 3-D Secure avec authentification forte	*314 857*	*43,6*	*72 017 359*	*54,2*	*299 991*	*41,5*	*45 596 872*	*34,3*
dont paiements hors 3-D Secure avec authentification forte	*36 576*	*22,9*	*2 353 042*	*26,2*	*90 765*	*56,8*	*5 352 650*	*59,7*
dont paiements 3-D Secure sans authentification forte	*258 701*	*43,6*	*12 634 204*	*55,1*	*260 511*	*43,9*	*7 911 532*	*34,5*
dont paiements hors 3-D Secure sans authentification forte	*1 303 090*	*32,5*	*65 810 881*	*35,2*	*1 698 120*	*42,4*	*61 545 234*	*33,0*
dont paiements initiés par le commerçant (MIT)	*1 044 582*	*52,3*	*49 260 633*	*56,2*	*634 013*	*31,8*	*27 045 718*	*30,8*
dont paiements « one-leg »	*0*	*0,0*	*0*	*0,0*	*0*	*0,0*	*0*	*0,0*
dont paiements non 3-D Secure conformes à la DSP 2	*70 590*	*12,8*	*4 496 448*	*27,2*	*476 009*	*86,1*	*11 630 803*	*70,4*
dont paiements non 3-D Secure non conformes à la DSP 2	*187 918*	*18,0*	*12 053 800*	*23,2*	*588 098*	*56,4*	*22 868 713*	*44,0*
Retraits	**102 357**	**92,9**	**38 832 083**	**95,6**	**2 882**	**2,6**	**845 142**	**2,1**
Total	**3 020 017**	**44,8**	**264 527 216**	**53,4**	**2 421 954**	**35,9**	**133 664 784**	**27,0**

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

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition géographique de la fraude sur les cartes émises en France en 2023 (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	**38 945**	**4,0**	**7 864 768**	**12,8**	**966 134**	**61 618 923**
dont paiements sans contact (y compris paiements par mobile)	*18 943*	*2,6*	*1 487 007*	*7,9*	*733 359*	*18 786 086*
dont paiements par mobile	*8 432*	*7,7*	*891 906*	*12,2*	*110 133*	*7 294 895*
Paiements à distance (hors internet)	**39 567**	**21,2**	**10 638 526**	**25,2**	**186 499**	**42 177 372**
Paiements sur internet	**1 220 711**	**22,3**	**78 186 825**	**22,2**	**5 483 322**	**351 408 599**
dont paiements 3-D Secure avec authentification forte	*107 548*	*14,9*	*15 139 967*	*11,4*	*722 396*	*132 754 198*
dont paiements hors 3-D Secure avec authentification forte	*32 339*	*20,3*	*1 260 969*	*14,1*	*159 680*	*8 966 661*
dont paiements 3-D Secure sans authentification forte	*74 596*	*12,6*	*2 384 112*	*10,4*	*593 808*	*22 929 848*
dont paiements hors 3-D Secure sans authentification forte	*1 006 228*	*25,1*	*59 401 777*	*31,8*	*4 007 438*	*186 757 892*
dont paiements initiés par le commerçant (MIT)	*317 286*	*15,9*	*11 378 797*	*13,0*	*1 995 881*	*87 685 148*
dont paiements « one-leg »	*416 116*	*100,0*	*30 632 806*	*100,0*	*416 116*	*30 632 806*
dont paiements non 3-D Secure conformes à la DSP 2	*6 419*	*1,2*	*387 978*	*2,3*	*553 018*	*16 515 229*
dont paiements non 3-D Secure non conformes à la DSP 2	*266 407*	*25,6*	*17 002 196*	*32,7*	*1 042 423*	*51 924 709*
Retraits	**4 982**	**4,5**	**931 688**	**2,3**	**110 221**	**40 608 913**
Total	**1 304 205**	**19,3**	**97 621 807**	**19,7**	**6 746 176**	**495 813 807**

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

Source : Observatoire de la sécurité des moyens de paiement.

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

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

	2018		2019		2020	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**10 864 788**	**421 977 639**	**11 774 183**	**437 193 670**	**10 978 602**	**413 760 411**
dont paiements sans contact (y compris paiements par mobile)	*2 320 822*	*24 439 724*	*3 690 364*	*41 558 002*	*5 081 519*	*78 386 853*
dont paiements par mobile	*10 949*	*190 953*	*45 249*	*794 288*	*126 945*	*2 687 300*
Paiements à distance (hors internet)	**34 893**	**2 707 270**	**34 859**	**2 773 069**	**60 243**	**5 428 918**
Paiements sur internet	**1 515 988**	**97 756 554**	**1 768 890**	**109 593 147**	**2 011 431**	**122 128 921**
Retraits	**1 385 723**	**129 786 224**	**1 339 625**	**130 198 441**	**1 038 647**	**112 337 533**
Total	**13 801 392**	**652 227 686**	**14 917 558**	**679 758 326**	**14 088 924**	**653 655 783**

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)

	2021		2022		2023	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**12 611 966**	**460 274 895**	**14 340 211**	**514 159 801**	**15 252 122**	**543 567 354**
dont paiements sans contact (y compris paiements par mobile)	*7 202 992*	*121 694 861*	*8 781 813*	*141 160 469*	*10 357 439*	*164 920 568*
dont paiements par mobile	*348 251*	*7 390 633*	*808 622*	*17 132 553*	*1 533 084*	*33 773 794*
Paiements à distance (hors internet)	**56 236**	**5 540 339**	**87 602**	**13 259 829**	**82 700**	**12 227 259**
Paiements sur internet	**2 399 865**	**142 184 895**	**2 393 161**	**146 642 890**	**2 580 907**	**164 682 672**
dont paiements 3-D Secure avec authentification forte	*661 960*	*72 184 112*	*809 038*	*88 956 221*	*977 983*	*105 884 327*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*nd*	*57 239*	*1 938 429*
dont paiements 3-D Secure sans authentification forte	*389 530*	*15 797 723*	*717 916*	*24 981 800*	*661 070*	*22 814 974*
dont paiements hors 3-D Secure sans authentification forte	*1 348 375*	*54 203 060*	*866 207*	*32 704 868*	*884 617*	*34 044 942*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*704 832*	*25 137 618*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*92 513*	*4 489 918*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*87 272*	*4 417 407*
Retraits	**1 056 936**	**119 485 544**	**1 101 989**	**128 161 781**	**1 085 417**	**129 282 806**
Total	**16 125 003**	**727 485 673**	**17 922 963**	**802 224 301**	**19 001 146**	**849 760 091**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

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

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

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

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

	2018			2019			2020		
	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	**977 654**	**41 383 109**	**0,010**	**1 069 418**	**44 175 058**	**0,010**	**793 350**	**36 280 495**	**0,009**
dont paiements sans contact (y compris paiements par mobile)	*426 713*	*4 967 274*	*0,020*	*582 050*	*7 912 021*	*0,019*	*522 873*	*10 502 092*	*0,013*
dont paiements par mobile	*1 717*	*50 491*	*0,026*	*3 215*	*197 048*	*0,025*	*29 807*	*2 447 707*	*0,091*
Paiements à distance (hors internet)	**159 916**	**9 512 197**	**0,351**	**64 113**	**7 498 207**	**0,270**	**74 832**	**8 964 315**	**0,165**
Paiements sur internet	**2 180 379**	**163 824 893**	**0,168**	**2 630 697**	**183 067 879**	**0,167**	**2 847 769**	**212 962 645**	**0,174**
Retraits	**109 924**	**30 893 412**	**0,024**	**122 260**	**35 935 625**	**0,028**	**102 962**	**32 477 429**	**0,029**
Total	**3 427 873**	**245 613 611**	**0,038**	**3 886 488**	**270 676 769**	**0,040**	**3 818 913**	**290 684 884**	**0,044**

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)

	2021			2022			2023		
	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	**825 325**	**43 515 617**	**0,009**	**989 454**	**53 593 598**	**0,010**	**885 533**	**50 277 021**	**0,009**
dont paiements sans contact (y compris paiements par mobile)	*576 537*	*14 002 613*	*0,012*	*754 985*	*20 231 615*	*0,014*	*684 776*	*15 698 156*	*0,010*
dont paiements par mobile	*75 039*	*4 801 997*	*0,065*	*152 726*	*9 566 583*	*0,056*	*98 610*	*6 066 551*	*0,018*
Paiements à distance (hors internet)	**77 941**	**10 604 251**	**0,191**	**120 708**	**24 857 056**	**0,187**	**118 903**	**22 602 626**	**0,185**
Paiements sur internet	**2 577 337**	**191 873 234**	**0,135**	**1 874 565**	**145 299 292**	**0,099**	**1 913 224**	**152 815 486**	**0,093**
dont paiements 3-D Secure avec authentification forte	267 556	69 544 332	0,096	314 967	72 922 674	0,082	314 857	72 017 359	0,068
dont paiements hors 3-D Secure avec authentification forte	nd	nd	nd	nd	nd	nd	36 576	2 353 042	0,121
dont paiements 3-D Secure sans authentification forte	159 344	11 208 886	0,071	342 714	17 460 124	0,070	258 701	12 634 204	0,055
dont paiements hors 3-D Secure sans authentification forte	2 150 437	111 120 015	0,205	1 216 884	54 916 494	0,168	1 303 090	65 810 881	0,193
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*1 044 582*	*49 260 633*	*0,196*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*0*	*0*	*0,000*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*70 590*	*4 496 448*	*0,100*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*187 918*	*12 053 800*	*0,273*
Retraits	**121 642**	**41 437 842**	**0,035**	**115 643**	**41 344 934**	**0,032**	**102 357**	**38 832 083**	**0,030**
Total	**3 602 245**	**287 430 944**	**0,040**	**3 100 370**	**265 094 880**	**0,033**	**3 020 017**	**264 527 216**	**0,031**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

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 2023

(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	743 394 922	43 609 426 035	345 222	27 987 056	0,464	0,064
Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager, etc.)	142 806 627	6 598 626 354	296 264	17 591 684	2,075	0,267
Voyage, transport	282 064 146	26 693 359 943	204 572	18 623 728	0,725	0,070
Téléphonie et communication	410 678 797	15 141 508 530	273 643	21 255 918	0,666	0,140
Alimentation	32 190 669	2 500 508 834	15 102	1 373 571	0,469	0,055
Équipement de la maison, ameublement, bricolage	70 571 937	12 134 281 628	39 672	14 390 135	0,562	0,119
Assurance	13 105 332	2 579 914 202	4 396	592 659	0,335	0,023
Santé, beauté, hygiène	44 992 745	2 911 493 933	22 083	1 943 418	0,491	0,067
Services aux particuliers et aux professionnels	514 891 901	38 017 635 080	646 729	43 168 306	1,256	0,114
Approvisionnement d'un compte, vente de particulier à particulier	122 260 388	11 661 875 830	112 888	20 409 951	0,923	0,175
Jeux en ligne	134 297 474	4 189 186 895	41 239	2 956 047	0,307	0,071
Divers	152 352 304	10 872 113 907	30 317	5 125 639	0,199	0,047
Total	**2 663 607 242**	**176 909 931 171**	**2 032 127**	**175 418 112**	**0,763**	**0,099**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France

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

	2018		2019		2020	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**11 286 513**	**453 608 003**	**12 277 149**	**468 895 511**	**11 284 433**	**428 180 387**
dont paiements sans contact (y compris paiements par mobile)	*2 370 247*	*25 007 584*	*3 802 953*	*42 931 374*	*5 187 488*	*79 877 184*
dont paiements par mobile	*11 911*	*209 710*	*56 169*	*1 014 657*	*145 527*	*2 979 437*
Paiements à distance (hors internet)	**50 543**	**5 757 108**	**48 998**	**5 586 755**	**69 950**	**7 087 913**
Paiements sur internet	**1 652 894**	**112 607 104**	**1 906 065**	**121 920 272**	**2 158 226**	**132 554 575**
Retraits	**1 418 919**	**136 201 131**	**1 375 145**	**136 636 741**	**1 062 376**	**116 986 747**
Total	**14 408 869**	**708 173 346**	**15 607 358**	**733 039 279**	**14 574 985**	**684 809 622**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Paiements par carte acceptée en France (suite)

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

	2021		2022		2023	
	Volume	Montant	Volume	Montant	Volume	Montant
Paiements de proximité et sur automate	**13 031 098**	**480 804 099**	**15 093 611**	**551 753 133**	**16 159 605**	**588 228 633**
dont paiements sans contact (y compris paiements par mobile)	*7 437 197*	*125 344 168*	*9 248 429*	*149 971 446*	*10 982 717*	*178 132 864*
dont paiements par mobile	*388 175*	*8 403 747*	*897 307*	*19 846 999*	*1 716 563*	*39 282 385*
Paiements à distance (hors internet)	**64 620**	**7 272 724**	**107 228**	**18 523 094**	**105 756**	**18 799 343**
Paiements sur internet	**2 565 276**	**155 816 405**	**2 589 260**	**166 197 062**	**2 821 038**	**190 607 365**
dont paiements 3-D Secure avec authentification forte	*708 194*	*78 650 830*	*871 961*	*99 937 461*	*1 049 797*	*120 158 448*
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*nd*	*86 343*	*3 228 632*
dont paiements 3-D Secure sans authentification forte	*409 008*	*18 152 505*	*748 083*	*27 403 752*	*707 064*	*26 605 058*
dont paiements hors 3-D Secure sans authentification forte	*1 448 074*	*59 013 071*	*969 216*	*38 855 848*	*977 834*	*40 615 228*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*730 327*	*26 600 426*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*nd*	*13 616*	*1 740 365*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*101 735*	*5 110 587*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*132 156*	*7 163 850*
Retraits	**1 083 643**	**125 105 264**	**1 134 543**	**134 637 455**	**1 117 986**	**135 559 666**
Total	**16 744 636**	**768 998 491**	**18 924 643**	**871 110 743**	**20 204 386**	**933 195 008**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

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

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

T13 Transactions frauduleuses par carte acceptée en France

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

	2018			2019			2020		
	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur	Volume	Valeur	Taux de fraude en valeur
Paiements de proximité et sur automate	**1 064 889**	**58 485 280**	**0,0129**	**1 170 399**	**64 448 538**	**0,0137**	**841 280**	**42 883 367**	**0,0100**
dont paiements sans contact (y compris paiements par mobile)	*438 088*	*5 174 314*	*0,0207*	*602 309*	*8 534 090*	*0,0199*	*538 313*	*12 238 895*	*0,0153*
dont paiements par mobile	*1 915*	*64 599*	*0,0308*	*3 890*	*307 230*	*0,0303*	*35 968*	*3 640 684*	*0,1222*
Paiements à distance (hors internet)	**206 957**	**27 274 865**	**0,4738**	**108 259**	**23 167 505**	**0,4147**	**105 972**	**17 644 315**	**0,2489**
Paiements sur internet	**2 537 264**	**225 819 184**	**0,2005**	**2 989 333**	**232 763 441**	**0,1909**	**3 176 400**	**248 966 265**	**0,1878**
Retraits	**114 727**	**32 353 075**	**0,0238**	**127 005**	**37 354 814**	**0,0273**	**104 960**	**33 084 175**	**0,0283**
Total	**3 923 837**	**343 932 404**	**0,0486**	**4 394 996**	**357 734 298**	**0,0488**	**4 228 612**	**342 578 122**	**0,0500**

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)

	2021			2022			2023		
	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	**874 166**	**49 441 754**	**0,0103**	**1 084 701**	**67 409 965**	**0,0122**	**999 344**	**67 688 751**	**0,0115**
dont paiements sans contact (y compris paiements par mobile)	601 803	15 600 613	0,0124	819 535	24 406 015	0,0163	769 976	21 898 465	0,0123
dont paiements par mobile	*84 421*	*5 793 427*	*0,0689*	*170 752*	*12 007 511*	*0,0605*	*127 622*	*10 042 616*	*0,0256*
Paiements à distance (hors internet)	**96 257**	**15 211 163**	**0,2092**	**144 965**	**35 446 137**	**0,1914**	**142 763**	**32 984 939**	**0,1755**
Paiements sur internet	**2 885 920**	**227 162 875**	**0,1458**	**2 252 283**	**190 461 573**	**0,1146**	**2 337 170**	**201 724 304**	**0,1058**
dont paiements 3-D Secure avec authentification forte	306 265	76 891 633	0,0978	346 366	80 959 973	0,0810	354 651	83 805 192	0,0697
dont paiements hors 3-D Secure avec authentification forte	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*71 563*	*5 522 986*	*0,1711*
dont paiements 3-D Secure sans authentification forte	*213 403*	*20 406 481*	*0,1124*	*405 445*	*26 105 266*	*0,0953*	*342 878*	*20 687 862*	*0,0778*
dont paiements hors 3-D Secure sans authentification forte	*2 366 252*	*129 864 761*	*0,2201*	*1 500 472*	*83 396 334*	*0,2146*	*1 568 078*	*91 708 264*	*0,2258*
dont paiements initiés par le commerçant (MIT)	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*1 098 829*	*52 343 346*	*0,1968*
dont paiements « one-leg »	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*92 524*	*12 994 451*	*0,7467*
dont paiements non 3-D Secure conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*80 195*	*5 068 095*	*0,0992*
dont paiements non 3-D Secure non conformes à la DSP 2	*nd*	*nd*	*nd*	*nd*	*nd*	*nd*	*296 530*	*21 302 372*	*0,2974*
Retraits	**124 077**	**42 256 276**	**0,0338**	**120 217**	**42 811 637**	**0,0318**	**106 749**	**40 292 502**	**0,0297**
Total	**3 980 420**	**334 072 068**	**0,0434**	**3 602 166**	**336 129 312**	**0,0386**	**3 586 026**	**342 690 496**	**0,0367**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

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

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

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

T13 *quater* Répartition de la fraude sur les paiements par carte acceptée en France en 2023

T13 *quinquies* Répartition géographique de la fraude sur les cartes acceptées en France en 2023

CHÈQUE

T14 Chèques échangés

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

	2018	2019	2020	2021	2022	2023
Volume	1 746,9	1 586,5	1 175,5	1 105,8	1 008,0	891,5
Montant	891,1	814,5	614,2	588,6	539,8	467,2
Montant moyen	**510,1**	**513,4**	**522,5**	**532,3**	**535,5**	**524,1**

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

	2018	2019	2020	2021	2022	2023
Volume	**166 421**	**183 488**	**220 685**	**272 970**	**266 216**	**253 338**
Taux de fraude (‰)	0,095	0,116	0,188	0,247	0,264	0,284
Valeur	**450 108 464**	**539 215 175**	**538 059 139**	**625 703 442**	**556 796 815**	**585 506 445**
Taux de fraude (%)	0,051	0,066	0,088	0,106	0,103	0,125
Montant moyen	**2 705**	**2 939**	**2 438**	**2 292**	**2 092**	**2 311**

b) Nouvelle approche

	2018	2019	2020	2021	2022	2023
Volume	**nd**	**nd**	**190 001**	**232 277**	**218 122**	**203 514**
Taux de fraude (‰)			0,162	0,210	0,216	0,228
Valeur	**nd**	**nd**	**401 611 189**	**465 021 167**	**395 416 196**	**363 549 771**
Taux de fraude (%)			0,065	0,079	0,073	0,078
Montant moyen	**nd**	**nd**	**2 114**	**2 002**	**1 813**	**1 786**

nd, non disponible.

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

Source : Observatoire de la sécurité des moyens de paiement.

T16 Typologie de la fraude au chèque

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

	2018		2019		2020		2021		2022		2023	
	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part	Nombre/ montant	Part
Volume												
Vol, perte	138 358	83,1	154 211	84,0	196 754	89,2	244 750	89,7	237 854	89,3	225 786	89,1
Falsification	17 178	10,3	16 459	9,0	13 894	6,3	18 074	6,6	18 885	7,1	18 009	7,1
Contrefaçon	8 092	4,9	9 574	5,2	7 207	3,3	5 119	1,9	5 969	2,2	5 700	2,2
Détournement, rejeu	2 793	1,7	3 244	1,8	2 830	1,3	5 026	1,8	3 508	1,3	3 843	1,5
Valeur												
Vol, perte	252 890 727	56,2	296 367 562	55,0	365 813 764	68,0	398 739 224	63,7	375 576 575	67,5	384 036 365	65,6
Falsification	145 737 424	32,4	145 881 745	27,1	102 801 337	19,1	100 395 756	16,0	93 152 894	16,7	100 520 775	17,2
Contrefaçon	36 739 051	8,2	76 511 582	14,2	32 340 420	6,0	33 725 041	5,4	32 648 566	5,9	29 819 343	5,1
Détournement, rejeu	14 741 262	3,3	20 454 286	3,8	37 103 618	6,9	92 823 421	14,8	55 418 781	10,0	71 129 963	12,1

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

Source : Observatoire de la sécurité des moyens de paiement.

T17 Virements émis par type de virement

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

	2018		2019		2020		2021		2022		2023	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4038**	**24211142**	**4251**	**25879217**	**4483**	**32713128**	**4843**	**38722734**	**5158**	**38894879**	**5658**	**30588908**
dont virements SEPA – SCT	*3974*	*10846914*	*4174*	*9602866*	*4384*	*10029108*	*4668*	*12980883*	*4689*	*9655892*	*4869*	*9921539*
dont virements SEPA instantanés – SCT Inst	*0*	*86*	*14*	*7074*	*45*	*26243*	*107*	*50053*	*198*	*118972*	*364*	*174049*
dont virements de gros montants – VGM [a]	*10*	*10130586*	*9*	*12266316*	*9*	*19042030*	*9*	*19661685*	*19*	*15907892*	*73*	*8757890*
dont autres virements	*53*	*3233556*	*54*	*4002960*	*45*	*3615748*	*59*	*6030114*	*252*	*13212124*	*351*	*11735430*
Total – hors VGM	**4028**	**14080556**	**4242**	**13612900**	**4474**	**13671098**	**4834**	**19061050**	**5138**	**22986988**	**5585**	**21831018**

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

Source : Observatoire de la sécurité des moyens de paiement.

T17 *bis* Virements émis par canal d'initiation

T17 *ter* Virements émis par destination géographique

T18 Transactions frauduleuses par type de virement

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

	2018			2019			2020		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**7736**	**97327128**	**0,0004**	**15934**	**161642174**	**0,0006**	**35893**	**266969099**	**0,0008**
dont virements SEPA – SCT	*6521*	*78314614*	*0,0007*	*13302*	*127572549*	*0,0013*	25254	191474396	0,0019
dont virements SEPA instantanés – SCT Inst	*5*	*29800*	*0,0345*	*729*	*2203240*	*0,0311*	7131	10562419	0,0402
dont virements de gros montants – VGM [a]	*14*	*4622598*	*0,0000*	*15*	*15476053*	*0,0001*	51	2439224	0,0000
dont autres virements	*1196*	*14360116*	*0,0004*	*1888*	*16390332*	*0,0004*	3457	62493060	0,0017
Total – hors VGM	**7722**	**92704530**	**0,0007**	**15919**	**146166121**	**0,0011**	**35842**	**264529875**	**0,0019**

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

Source : Observatoire de la sécurité des moyens de paiement.

T18 Transactions frauduleuses par type de virement (suite)

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

	2021			2022			2023		
	Volume	Valeur		Volume	Valeur		Volume	Valeur	
		Montant	Taux de fraude		Montant	Taux de fraude		Montant	Taux de fraude
Total	**46 718**	**287 264 068**	**0,0007**	**76 846**	**313 163 442**	**0,0008**	**90 436**	**311 627 465**	**0,0010**
dont virements SEPA – SCT	*33 199*	*246 527 533*	*0,0019*	*40 874*	*205 737 587*	*0,0021*	*38 625*	*202 099 216*	*0,0020*
dont virements SEPA instantanés – SCT Inst	*12 913*	*22 406 942*	*0,0448*	*33 193*	*52 768 218*	*0,0444*	*48 630*	*69 003 730*	*0,0396*
dont virements de gros montants – VGM [a]	*5*	*1 539 120*	*0,0000*	*49*	*1 934 774*	*0,0000*	*32*	*9 828 077*	*0,0001*
dont autres virements	*601*	*16 790 473*	*0,0003*	*2 730*	*52 722 863*	*0,0004*	*3 149*	*30 696 443*	*0,0003*
Total – hors VGM	**46 713**	**285 724 948**	**0,0015**	**76 797**	**311 228 668**	**0,0014**	**90 404**	**301 799 388**	**0,0014**

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

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

Source : Observatoire de la sécurité des moyens de paiement.

T18 *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)

	2018	2019	2020	2021	2022	2023
Volume	**7 736**	**15 934**	**35 893**	**46 718**	**76 846**	**90 436**
Taux (‰)	0,0019	0,0037	0,0080	0,0096	0,0149	0,0160
Valeur	**97 327 128**	**161 642 174**	**266 969 099**	**287 264 068**	**313 163 442**	**311 627 465**
Taux (%)	0,0004	0,0006	0,0008	0,0007	0,0008	0,0010
Montant moyen	**12 581**	**10 144**	**7 438**	**6 149**	**4 075**	**3 446**

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)

	2018		2019		2020		2021		2022		2023	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**5 525**	**51 069 661**	**13 769**	**98 525 485**	**28 211**	**87 061 255**	**35 865**	**87 370 131**	**57 443**	**120 006 990**	**63 528**	**135 231 281**
Part	71,4	52,5	86,4	61,0	78,6	32,6	76,8	30,4	74,8	38,3	70,2	43,4
Falsification	**151**	**485 131**	**125**	**3 438 923**	**203**	**3 377 807**	**875**	**5 387 862**	**179**	**2 838 371**	**269**	**2 293 923**
Part	2,0	0,5	1,6	2,1	0,6	1,3	1,9	1,9	0,2	0,9	0,3	0,7
Détournement	**1 037**	**40 250 639**	**1 534**	**56 514 755**	**5 731**	**157 318 883**	**8 523**	**168 094 274**	**16 991**	**148 732 203**	**24 997**	**150 088 618**
Part	13,4	41,4	19,8	35,0	16,0	58,9	18,2	58,5	22,1	47,5	27,6	48,2
Autres	**1 023**	**5 521 697**	**506**	**3 163 011**	**1 748**	**19 211 154**	**1 455**	**26 411 801**	**2 233**	**41 585 878**	**1 642**	**24 013 643**
Part	13,2	5,7	3,2	2,0	4,9	7,2	3,1	9,2	2,9	13,3	1,8	7,7

Source : Observatoire de la sécurité des moyens de paiement.

T21 Prélèvements émis par type de mandat

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

	2018		2019		2020		2021		2022		2023	
	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant	Volume	Montant
Total	**4211**	**1644553**	**4370**	**1710931**	**4622**	**1684258**	**5020**	**1895098**	**4914**	**2040963**	**4621**	**2139398**
Prélèvements par type de mandat												
dont prélèvements consentis par mandat électronique	nd	nd	nd	nd	nd	nd	1106	430781	1357	1045754	1254	1021908
dont prélèvements consentis par mandat papier	nd	nd	nd	nd	nd	nd	3914	1464317	3558	995210	3366	1117490
Prélèvements par mode d'initiation												
dont prélèvements initiés dans un fichier/lot	4151	1609405	4312	1672338	4560	1647504	4936	1819420	4645	1929438	4247	2010766
dont prélèvements initiés sur la base d'un paiement unique	60	35148	58	38593	61	36754	84	75678	269	111525	374	128632

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)

	2018	2019	2020	2021	2022	2023
Volume	**309377**	**43519**	**6485**	**251010**	**49453**	**77876**
Taux de fraude (‰)	0,0735	0,0100	0,0014	0,0500	0,0101	0,0169
Valeur	**58346253**	**10990025**	**1891051**	**25318677**	**19853012**	**22320813**
Taux de fraude (%)	0,0035	0,0006	0,0001	0,0013	0,0010	0,0010
Montant moyen	**189**	**253**	**292**	**101**	**401**	**287**

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)

	2018		2019		2020		2021		2022		2023	
	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur	Volume	Valeur
Faux	**309302**	**58329283**	**14601**	**3961260**	**6011**	**1388326**	**250493**	**25201709**	**43788**	**14206533**	**70212**	**22003546**
Part	100,0	100,0	33,6	36,0	92,7	73,4	99,8	99,5	88,5	71,6	90,2	98,6
Détournement	**72**	**16703**	**26223**	**6677467**	**62**	**10720**	**517**	**116968**	**5665**	**5646479**	**7664**	**317267**
Part	0,0	0,0	60,3	60,8	1,0	0,6	0,2	0,5	11,5	28,4	9,8	1,4

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

Source : Observatoire de la sécurité des moyens de paiement.

Monnaie électronique

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

T25 Usage de la monnaie électronique par typologie de transaction

T26 Transactions frauduleuses par monnaie électronique

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

T27 Paiements par effet de commerce

T28 Typologie de la fraude aux effets de commerce

Transmission de fonds

T29 Opérations par transmission de fonds

T30 Opérations frauduleuses par transmission de fonds

Service d'initiation de paiement

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

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

Éditeur
Banque de France

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

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

Secrétariat de rédaction
Aurélie Barberet, Pierre Bienvenu, Clément Bourgeois, Véronique Bugaj, Julien Cisamolo, Caroline Corcy, Yolaine Fischer, Anne-Marie Fourel, Trân Huynh, Marc-Antoine Jambu, Isabelle Maranghi, Adrien Mocek, Didier Névonnic, Cyril Ronfort, Marine Soubielle

Réalisation
Studio Création
Direction de la Communication

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

Impression
Navis
Imprimé en France

Dépôt légal
Septembre 2024
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