OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2019

BANQUE DE FRANCE
EUROSYSTÈME



www.observatoire-paiements.fr

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

© Observatoire de la sécurité des moyens de paiement – 2020

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

RAPPORT ANNUEL 2019

Adressé à
Monsieur le ministre de l'Économie et des Finances,
Monsieur le président du Sénat,
Monsieur le président de l'Assemblée nationale

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

SEPTEMBRE 2020

SOMMAIRE

SYNTHÈSE 5

CHAPITRE 1
L'IMPACT DE LA CRISE SANITAIRE SUR LES MOYENS DE PAIEMENT 7

1.1 La réponse du marché français à la crise de la Covid-19 et ses implications en matière de sécurité des paiements 7

1.1.1 Un marché des paiements qui a démontré sa résilience opérationnelle 7

1.1.2 Une évolution des modes de paiement qui pourrait s'inscrire dans la durée 7

1.1.3 Quel impact sur la sécurité des paiements ? 9

1.2 Les conséquences de la crise sur le plan de déploiement de l'authentification forte du payeur lors des paiements sur Internet 9

1.2.1 Le plan de migration de la Place française 9

1.2.2 L'état d'avancement de la migration dans le contexte de la crise sanitaire 10

1.2.3 Recommandations de l'Observatoire pour le pilotage du plan de migration 11

CHAPITRE 2
ÉTAT DE LA FRAUDE EN 2019 17

2.1 Vue d'ensemble 17

2.1.1 Cartographie des moyens de paiement 17

2.1.2 Fraude aux moyens de paiement 18

2.2 État de la fraude sur le paiement et le retrait par carte 19

2.2.1 Vue d'ensemble 19

2.2.2 Répartition de la fraude par zone géographique 21

2.2.3 Répartition de la fraude par type de transaction 21

2.2.4 Répartition de la fraude par typologie 23

2.3 État de la fraude sur le chèque 23

2.3.1 Vue d'ensemble 23

2.3.2 Répartition de la fraude par typologie 23

2.4 État de la fraude sur le virement 24

2.4.1 Vue d'ensemble 24

2.4.2 Répartition de la fraude par canal d'initiation 25

2.4.3 Répartition de la fraude par type de virement 25

2.4.4 Répartition de la fraude par zone géographique 25

2.4.5 Répartition de la fraude par typologie de fraude 26

2.5 État de la fraude sur le prélèvement 26

2.5.1 Vue d'ensemble 26

2.5.2 Répartition de la fraude par typologie 26

2.5.3 Répartition de la fraude par zone géographique 27

CHAPITRE 3
ÉTUDE DE VEILLE TECHNOLOGIQUE SUR LA SÉCURITÉ DES DONNÉES DE PAIEMENT 35

3.1 De nouveaux risques pour la sécurité des données de paiement 35

3.1.1 Les données de paiement : de quoi parle-t-on ? 35

3.1.2 Quatre évolutions structurantes participent à la dissémination des données de paiement 36

3.1.3 Des méthodes de plus en plus sophistiquées pour subtiliser les données de paiement sensibles 38

3.2 Protéger les données de paiement sensibles 39

3.2.1 Les données de la carte 39

3.2.2 L'IBAN 41

3.2.3 Les données d'accès aux espaces de banque en ligne ou mobile 42

3.3 De nouveaux « maillons » pour la sécurité des données de paiement : les prestataires de services d'information sur les comptes et les prestataires d'initiation de paiement 42

3.3.1 Les conditions d'exercice de ces nouveaux prestataires 42

3.3.2 La protection des données sensibles de paiement par les prestataires tiers 44

3.4 Mesures de sécurité recommandées par l'Observatoire 45

ANNEXES

A1	Conseils de prudence pour l'utilisation des moyens de paiement	52
A2	Protection du payeur en cas de paiement non autorisé	55
A3	Missions et organisation de l'Observatoire	57
A4	Liste nominative des membres de l'Observatoire	59
A5	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux	62
A6	Dossier statistique	71

ENCADRÉS

1	Les mesures de prévention de la fraude associées à l'élévation du plafond de paiement sans contact	13
2	Exemple de support d'information à l'attention des consommateurs	14
3	Conditions de montée en charge de l'émission de messages de *soft decline*	15
4	Statistiques de fraude sur les cartes : les contributeurs	31
5	Fraude aux paiements sans contact	32
6	Fraude nationale sur les paiements à distance selon le secteur d'activité	33
7	Indicateurs des services de police et de gendarmerie	34
8	La nouvelle plateforme Thésée de déclaration des escroqueries aux moyens de communication	46
9	Les dispositifs innovants de renforcement de la sécurité physique des cartes	47
10	Que faire en cas de fraude à la carte de paiement ?	47
11	L'utilisation d'alias : une forme de « tokenisation » de l'IBAN à des fins d'ergonomie	48
12	Le projet européen OBSIDIAN de partage d'information sur les IBAN comme moyen de lutte contre la fraude	49
13	Utilisation d'un smartphone : restez vigilant	49

SYNTHÈSE

Si le Rapport annuel de l'Observatoire de la sécurité des moyens de paiement *rend habituellement compte du bilan des actions conduites au cours de la période sous revue, l'Observatoire a également souhaité dresser, dans cette édition 2019, les premiers enseignements du contexte exceptionnel de crise sanitaire du premier semestre de l'année 2020.*

Le ***chapitre 1*** *est ainsi dédié à* ***l'analyse des impacts de la crise sanitaire sur le marché des paiements****, et se focalise sur deux aspects.*

- *D'une part, les effets de la crise sur l'utilisation des moyens de paiement scripturaux : à ce titre, l'Observatoire souligne le haut niveau de résilience assuré par le marché français des paiements. Ainsi, tous les moyens de paiement sont restés disponibles et pleinement opérationnels durant toutes les phases de la crise, en dépit des contraintes fortes pesant sur leurs opérateurs du fait du confinement et de contraintes sanitaires élevées. L'Observatoire note également que les pratiques en matière de paiement ont évolué durant la crise avec un recours plus fréquent aux paiements digitaux ou sans contact, offrant une meilleure maîtrise du risque sanitaire ; cette évolution, facilitée par le passage de trente à cinquante euros du plafond de paiement en mode sans contact, s'est faite au détriment de l'usage des paiements nécessitant un contact physique, tels le chèque, les espèces ou le paiement par carte avec saisie du code confidentiel. Si ces nouvelles habitudes de paiement semblent se confirmer au-delà de la période de confinement, il est toutefois trop tôt pour estimer leur impact à moyen et long terme, notamment en matière de sécurité ; ce sujet présente un intérêt majeur pour l'Observatoire, qui en rendra compte dans son rapport annuel 2020.*
- *D'autre part, la crise a affecté le déploiement de l'authentification forte des paiements sur Internet par rapport au plan adopté par l'Observatoire à l'automne 2019. Ainsi, l'enrôlement des porteurs de carte dans de nouvelles solutions d'authentification – notamment sur mobile en remplacement de l'usage de codes envoyés par SMS – a dû être temporisé par les banques afin de ne pas affecter la capacité des consommateurs à recourir au e-commerce dans une période où le commerce de proximité était moins accessible. De même, la migration des e-commerçants vers les nouvelles infrastructures d'authentification a été suspendue du fait de la priorité accordée à la gestion logistique de leurs opérations dans un environnement sanitaire complexe. L'Observatoire note toutefois que les actions de test et de fiabilisation de ces infrastructures ont pu se poursuivre durant la crise, et appelle désormais les banques et les commerçants à reprendre activement leur migration, afin d'assurer un haut niveau de conformité réglementaire au premier trimestre 2021, en ligne avec les exigences européennes. À ce titre, le plan national a été revu pour intégrer une marge de flexibilité supplémentaire ainsi que des actions complémentaires visant à sécuriser la migration.*

Le ***chapitre 2,*** *qui rend compte de l'****état de la fraude aux moyens de paiement en 2019****, souligne une nouvelle progression de la fraude sur le chèque, qui reste l'instrument le plus fraudé, tandis que le niveau de fraude sur les autres moyens de paiement demeure globalement maîtrisé.*

- *Le chèque enregistre un montant de fraude en progression de 20 % en 2019 pour atteindre près de 540 millions d'euros, soit 46 % du montant total de fraude scripturale mesuré par l'Observatoire. Comme l'usage de ce moyen de paiement continue à se réduire de 9 % par an, son taux de fraude poursuit sa progression pour s'établir à 0,066 %, soit l'équivalent d'un euro de fraude pour 1 510 euros de paiement. Le taux de fraude*

du chèque devient ainsi le plus élevé parmi les moyens de paiement scripturaux, puisqu'il dépasse désormais celui de la carte.

- *Le taux de fraude sur les cartes de paiement françaises est globalement stable à 0,064 %, soit l'équivalent d'un euro de fraude pour 1 560 euros d'opérations, dans un contexte où l'évolution des flux et de la fraude est parallèle (+ 7 % sur un an). Cette moyenne recouvre toutefois des situations très différentes, avec des taux de fraude maîtrisés au niveau national (0,040 %), en particulier sur les paiements de proximité (0,010 %), les paiements sans contact (0,019 %) ou les retraits (0,028 %), alors que les paiements à distance restent plus affectés (0,170 %) même si leur taux de fraude est en repli pour la huitième année consécutive. Les transactions internationales restent, quant à elles, plus vulnérables à la fraude (0,262 %), avec des taux de fraude qui se réduisent toutefois, notamment au sein de l'espace SEPA (*Single Euro Payments Area*) qui bénéficie de l'apport de la réglementation européenne en matière de sécurisation des paiements, avec le recours plus systématique à l'authentification forte (cf. chapitre 1).*

- *Si la fraude sur les virements progresse également, son montant (162 millions d'euros) reste toutefois modeste au regard des flux émis ; son taux de fraude demeure ainsi au niveau le plus bas parmi les moyens de paiement, à 0,0006 % soit un euro de fraude pour 160 000 euros de virements émis. L'Observatoire a mesuré, pour la première fois, le taux de fraude sur les virements instantanés SEPA, qui s'établit à 0,031 %. Si ce niveau est beaucoup plus élevé que celui de la moyenne des virements, il reflète surtout une utilisation par les particuliers via des canaux de type banque en ligne ou mobile, plus vulnérables à la fraude que les systèmes télématiques utilisés par les entreprises. À titre de comparaison, ce taux de fraude reste bien en deçà de celui des autres modes de paiement à distance utilisés par les particuliers, tels que la carte ou le chèque.*

- *La fraude sur les prélèvements se réduit fortement, après une année 2018 atypique, à 11 millions d'euros en 2019 (– 81 % sur un an). Son taux de fraude s'établit ainsi au même niveau que celui du virement, à 0,0006 %.*

Enfin, le ***chapitre 3*** *présente les travaux de veille conduits par l'Observatoire concernant* ***la sécurité des données de paiement****. En effet, le développement des usages numériques intégrant les informations liées aux paiements – qu'il s'agisse de l'intégration dans des applications mobiles, dans des objets connectés ou de l'accès à des services de conseil budgétaire personnalisés – a entraîné une dissémination de ces données. En réponse à ce phénomène, l'Observatoire s'est attaché à analyser les nouveaux risques portant sur la sécurité des données de paiement et à identifier les bonnes pratiques permettant d'en assurer la protection tout au long des chaînes de traitement. Les recommandations émises portent sur l'application de trois familles de mesures :*

- *le déploiement de dispositifs sécurisés pour la conservation des données à caractère sensible ou personnel, tant dans les systèmes d'information des acteurs du marché des paiements que dans les dispositifs mis à la disposition des utilisateurs (applications, objets connectés, etc.) ;*

- *la mise en place effective de l'authentification forte pour l'accès aux comptes de paiement et aux opérations de banque en ligne, conformément aux dispositions de la deuxième directive européenne sur les services de paiement ;*

- *l'appel sur une base régulière à la vigilance des utilisateurs, pour les inviter à adopter un comportement responsable en matière de protection de leurs propres données.*

1

L'IMPACT DE LA CRISE SANITAIRE SUR LES MOYENS DE PAIEMENT

1.1 La réponse du marché français à la crise de la Covid-19 et ses implications en matière de sécurité des paiements

Les mesures exceptionnelles prises par les pouvoirs publics en réponse à l'épidémie de Covid-19, notamment le confinement de la population entre le 16 mars et le 10 mai 2020, ont eu un impact direct sur le marché des paiements, et ce pour deux raisons distinctes :

- d'une part, du fait de leurs conséquences sur l'activité des entreprises et sur la consommation des ménages, traduites par une baisse globale des flux de paiement durant la période de confinement, ainsi que par une évolution des modes de paiement au profit de ceux dématérialisés ou sans contact ;
- d'autre part, par l'impact sur la capacité opérationnelle des acteurs du marché des paiements, qui ont dû gérer leur activité dans des conditions complexes et inhabituelles.

1.1.1 Un marché des paiements qui a démontré sa résilience opérationnelle

L'Observatoire salue l'efficacité avec laquelle les acteurs français des paiements ont su répondre présents face aux bouleversements liés à la crise sanitaire et proposer des réponses coordonnées aux défis soulevés par celle-ci. En dépit de conditions opérationnelles complexes, associant un recours important au télétravail et le maintien d'équipes de production sur site dans le respect de consignes sanitaires renforcées, le marché français des paiements scripturaux a démontré sa résilience en permettant une accessibilité et une disponibilité sans restriction de la totalité des services de paiement.

Au niveau de la Place française dans son ensemble, la coordination a été efficace grâce à l'activation du Groupe de Place Robustesse présidé par la Banque de France et à l'appui des différentes instances et fédérations professionnelles membres de l'Observatoire. Les principales difficultés rencontrées dans le secteur des paiements portaient sur deux moyens de paiement en particulier :

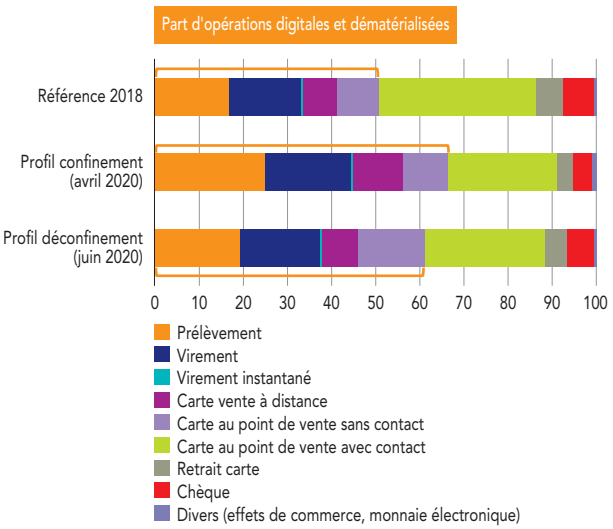
- Le chèque : la gestion des encaissements, en particulier des chèques de montant élevé (dits « circulants ») qui doivent être restitués par l'établissement du remettant à la banque émettrice, pouvait être affectée par la moindre disponibilités de transports ou par des capacités temporairement réduites des centres de traitement. La profession bancaire a identifié une solution permettant de recourir à un schéma de circulation alternatif en cas de défaillance des circuits classiques.
- La gestion des mandats de prélèvement SEPA[1] interentreprises : l'allégement de certaines charges professionnelles décidé par les pouvoirs publics a occasionné des demandes anticipées d'annulation de mandats de prélèvement par les entreprises, entraînant des rejets massifs de prélèvements émis par les créanciers publics et une forte mobilisation des unités de traitement des banques et des créanciers pour la régularisation des opérations rejetées à tort ou la signature de nouveaux mandats.

1.1.2 Une évolution des modes de paiement qui pourrait s'inscrire dans la durée

La période de confinement a conduit l'ensemble des agents économiques – consommateurs, entreprises et administrations – à faire évoluer leurs pratiques de paiement. En effet, alors que le ralentissement économique brutal a entraîné de façon logique une chute des flux de paiement (d'un tiers du nombre de transactions en avril 2020 par rapport à avril 2019), la structure des paiements a également évolué pour refléter à la fois la transition des échanges de proximité vers les échanges à distance du fait du confinement, et une utilisation plus systématique de modes de paiement dématérialisés ou sans contact dans les échanges de proximité résiduels pour des raisons sanitaires.

1 *Single Euro Payments Area.*

G1 Évolution de la structure des flux de paiement en volume imputable à la crise (en %)

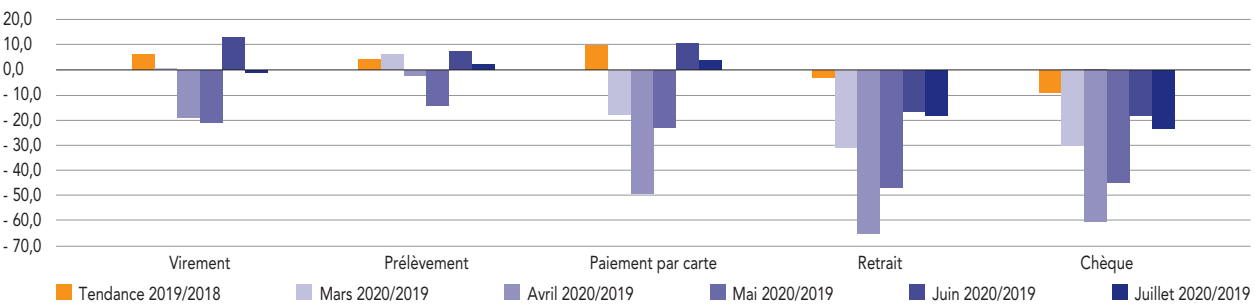


Source : Observatoire de la sécurité des moyens de paiement.

Si l'évolution de la structure des paiements a été particulièrement marquée durant la période de confinement, les premières semaines post-confinement ont mis en évidence que de nouvelles habitudes à caractère potentiellement durable ont été stimulées par la crise (*cf. graphique 2*) :

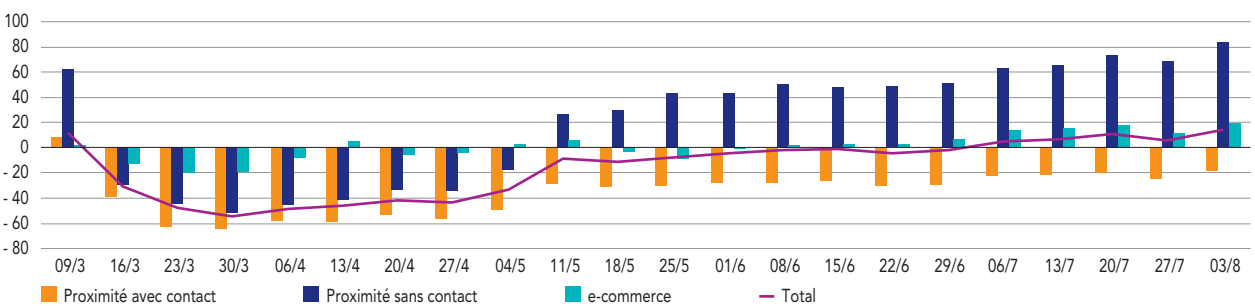
- Le paiement par chèque et les retraits d'espèces aux distributeurs sont les opérations qui ont accusé la baisse la plus significative durant le confinement, avec un repli qui a atteint – 60 % au mois d'avril 2020. Si leur utilisation s'est redressée depuis la fin du confinement, elle reste très en retrait par rapport à leur rythme pré-crise (de l'ordre de – 20 %). Le paiement par carte a ainsi remplacé en partie le recours aux paiements en espèces et par chèque au point de vente, a priori pour des raisons de perception d'un risque sanitaire mieux maîtrisé en particulier en sans contact, et cette substitution a perduré au-delà de la période de confinement.
- Si le paiement par carte a retrouvé dès le mois de juin 2020 son rythme de croissance pré-crise, la structure de ces paiements a fortement évolué (*cf. graphique 3*). Durant le

G2 Évolution des flux de paiement en volume par rapport à 2019 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

G3 Évolution des flux de paiement par carte par canal d'initiation – variation 2020/2019
(axe des abscisses : « semaine du » jour/mois exprimés en chiffre, axe des ordonnées : en %)



Source : Observatoire de la sécurité des moyens de paiement.

confinement, les flux de paiement de proximité se sont logiquement effondrés, tandis que ceux relatifs au e-commerce se sont maintenus à un niveau proche de leur rythme de 2019. Le déconfinement s'est traduit par une croissance très forte du nombre de paiements sans contact (supérieure à 60 % en volume et 120 % en montant par rapport à 2019 à compter de juillet 2020), qui a bénéficié de façon concomitante de l'élévation du plafond de paiement via ce canal. Les paiements de proximité avec saisie du code confidentiel, quant à eux, sont restés en repli de plus de 20 % par rapport à leur niveau de 2019.

- À l'inverse, les moyens de paiement SEPA ont retrouvé un niveau de croissance équivalent à celui d'avant crise. Ces moyens de paiement, utilisés majoritairement par les professionnels, semblent ainsi n'avoir été affectés que temporairement par la crise, l'effondrement des flux étant directement lié au ralentissement économique induit par le confinement.

1.1.3 Quel impact sur la sécurité des paiements ?

L'impact de la crise sur le développement de la fraude est délicat à appréhender de façon immédiate, dans la mesure où les déclarations de cas de fraude sont faites en règle générale plusieurs semaines à plusieurs mois après leur survenance. L'Observatoire anticipe toutefois que l'évolution du profil d'utilisation des moyens de paiement aura vraisemblablement un impact sur les taux de fraude 2020 :

- En matière de statistiques, la crise de la Covid-19 a conduit à une baisse de l'utilisation du chèque qui pourrait avoir un caractère durable, alors que ce moyen de paiement est proportionnellement le plus fraudé. À l'inverse, les moyens de paiement SEPA ont retrouvé un niveau de croissance comparable à la situation d'avant crise, et sont historiquement les moyens de paiement les moins vulnérables à la fraude. Dans l'hypothèse de taux de fraude constants, ces évolutions devraient jouer dans le sens d'un repli de la fraude globale aux moyens de paiement.
- La situation est plus complexe à appréhender pour ce qui concerne les paiements par carte, dont la répartition a été affectée significativement au cours des mois de crise. Ainsi, la part des montants réglés en mode contact est passée de 74 % à 60 % durant le confinement, pour remonter ensuite à 67 %, alors que la part de la vente à distance connaissait des évolutions en sens inverse (24 %, 32 %, puis 20 %) et que celle des paiements sans contact a progressé de façon continue (3 %, 8 %, puis 14 %). Cette nouvelle répartition des modes de paiement influera certainement sur le taux de fraude global. Les paiements de proximité en mode contact restent en effet les mieux sécurisés, à l'inverse des paiements à distance dont le taux de fraude est structurellement bien plus élevé. Enfin, le taux de fraude sur les paiements sans contact, maîtrisé depuis l'introduction de cette technologie, continuera à faire l'objet d'un suivi *ad-hoc* par l'Observatoire afin de mesurer l'impact de la hausse du plafond de paiement, porté de trente à cinquante euros le 11 mai 2020 (*cf. encadré 1 infra*).

1.2 Les conséquences de la crise sur le plan de déploiement de l'authentification forte du payeur lors des paiements sur Internet

Le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique est une disposition clé en matière de sécurité des paiements introduite par la deuxième directive européenne sur les services de paiement (DSP 2). Si cette directive est formellement en vigueur depuis le 6 janvier 2018, les normes techniques de réglementation relatives à l'authentification forte du client édictées par l'Autorité bancaire européenne (RTS SCA [2]), qui clarifient les conditions de mise en œuvre de cette dernière, devaient entrer en application le 14 septembre 2019 seulement.

Toutefois, l'Autorité bancaire européenne a publié le 16 octobre 2019 un avis (EBA-OP-2019-11) qui prend acte de la nécessité de laisser aux acteurs de marché, sous la responsabilité des autorités nationales, un délai additionnel courant jusqu'au 31 décembre 2020 pour se conformer aux dispositions du RTS (*Regulatory Technical Standard*, norme technique de réglementation) applicables aux paiements sur Internet ; ce délai est complété par une phase de bilan à conduire au premier trimestre 2021. En réponse, l'Observatoire a élaboré un plan de migration pour la Place française, dont la version finale a été publiée le 30 octobre 2019 sur son site Internet [3]. Ce plan fait l'objet d'un suivi périodique par un groupe de travail dédié.

1.2.1 Le plan de migration de la Place française

Le plan de migration vers l'authentification forte des paiements validé par l'Observatoire comporte deux volets :

- un volet à l'attention des consommateurs : l'enrôlement des porteurs de carte dans des dispositifs d'authentification conformes à la définition de l'authentification forte de la DSP 2, en remplacement de l'usage du code SMS à usage unique (ou SMS OTP – *one time password*) comme facteur unique d'authentification ;

2 *Regulatory Technical Standard on Strong Customer Authentication and Common and Secure Communication.*

3 Cf. *https://www.banque-france.fr/sites/default/files/medias/documents/2019-10-30_-_osmp_-_plan_de_migration_dsp2.pdf*

- un volet à l'attention des acteurs professionnels de la chaîne des paiements, y compris les e-commerçants : l'évolution de l'infrastructure d'authentification, notamment du protocole technique 3D-Secure en version 2, afin d'assurer la gestion des règles de responsabilité et des cas d'exemption à l'authentification forte prévus par la directive.

Ces deux volets font l'objet d'indicateurs de suivi assortis de cibles et d'échéances, ainsi que de plans d'action visant à accompagner la mise en conformité de la Place française.

1.2.2 L'état d'avancement de la migration dans le contexte de la crise sanitaire

Dans le contexte de confinement sanitaire de mi-mars à mi-mai 2020, les déploiements des plans d'équipement de masse ont dû être temporisés, tant côté consommateurs que côté commerçants.

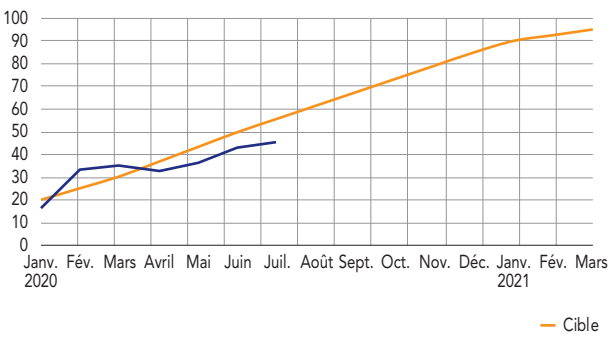
- L'enrôlement des porteurs dans les nouvelles solutions d'authentification a dû être suspendu par les banques émettrices, qui estimaient i) ne pas vouloir prendre le risque d'affecter la capacité de leur clientèle à payer sur Internet durant le confinement, alors que ce mode d'achat était devenu essentiel, et ii) ne pas disposer d'un support client adéquat pour une telle migration.
- La migration des e-commerçants vers la nouvelle plateforme 3D-Secure v2 a également été ralentie, devant le besoin de sécuriser les activités opérationnelles et logistiques dans un contexte de confinement particulièrement défavorable. Ainsi, seuls quelques grands e-commerçants ont pu se connecter à la nouvelle plateforme et contribuer à sa montée en charge. Par ailleurs, quelques milliers de petits e-commerçants (non gestionnaires de leur page de paiement) ont été migrés de façon transparente à l'initiative de leur prestataire d'acquisition technique (PAT). Les flux 3D-Secure v2 ont ainsi augmenté à un rythme réduit, bien qu'en forte progression depuis le début de l'année 2020 (multiplication par dix entre janvier et mai).

Cette temporisation des deux volets de la migration s'est répercutée sur les indicateurs de suivi du plan, qui ont globalement stagné depuis le début de la crise sanitaire, en mars 2020 :

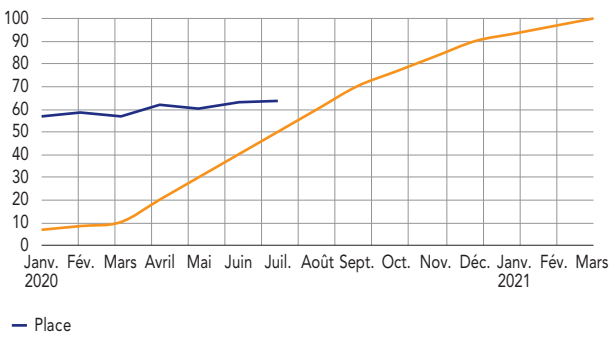
- Après une progression du niveau d'équipement des porteurs globalement conforme à la trajectoire attendue au premier trimestre 2020, la temporisation des actions d'enrôlement par les banques a conduit à un décrochage par rapport aux cibles fixées au deuxième trimestre 2020, même si la trajectoire s'est redressée par la suite au début de l'été (*cf. graphique 4a*).
- L'indicateur de conformité des flux par rapport à la cible DSP 2 a très peu évolué depuis le début de l'année à environ 62 % en valeur. Il reste cependant bien au-dessus de la trajectoire cible (40 % en valeur à fin juin) dans la mesure où le protocole 3D-Secure était déjà largement utilisé par les e-commerçants français et avait connu une progression sensible en 2019 (*cf. graphique 4b*). Cet écart tend toutefois à se réduire rapidement. Ce taux reste très largement dominé par le protocole 3D-Secure en version 1 qui, s'il est bien conforme à la DSP 2 car il appelle en règle générale une authentification du porteur, n'est pas optimal dans la mesure où il ne permet pas le recours aux exemptions prévues par les textes européens.

G4 Indicateurs de conformité par rapport à l'objectif cible de la DSP 2 (en %)

a) Volet consommateurs : taux d'équipement des porteurs effectuant des achats sur Internet



b) Volet commerçants : part des flux 3D-Secure versions 1 et 2 en valeur



Source : Observatoire de la sécurité des moyens de paiement.

En complément de ces indicateurs quantitatifs, l'Observatoire note que certaines actions techniques de maintenance et d'évolution des nouvelles infrastructures ont pu se poursuivre conformément au plan de migration durant la crise (*cf. tableau 1*), et ont pu permettre de préparer et fiabiliser leur fonctionnement cible.

- Le chargement des numéros de carte dans les nouvelles infrastructures d'authentification bancaires (*directory servers*) a pu se poursuivre durant le confinement et permet désormais d'utiliser le protocole 3D-Secure v2 pour la quasi-totalité du parc de cartes.
- La poursuite des actions de remontée et de traitement des incidents rencontrés par les e-commerçants pilotes a par exemple permis d'identifier divers problèmes techniques portant sur la compatibilité de l'authentification par redirection avec certaines configurations, ainsi qu'un niveau de performance ne permettant pas d'assurer la bonne fluidité des parcours d'achat. Une action correctrice a été engagée pour adapter le paramétrage des nouveaux serveurs d'authentification des banques, avec une mise en production effective au début de l'été 2020.
- Le mécanisme de *soft decline* (rejet par l'émetteur de la carte d'une transaction non conforme DSP 2 avec possibilité pour le e-commerçant de soumettre une nouvelle fois la transaction via 3D-Secure) a été introduit comme attendu au 1er avril 2020, sur une base réduite visant à éviter tout impact négatif pour les e-commerçants (émission en réponse à des transactions jusqu'alors rejetées ou *hard decline*). Le dispositif a connu une montée en régime rapide d'avril à juin, et est désormais opérationnel pour la quasi-totalité des émetteurs. Toutefois, les volumes émis restant relativement faibles et concentrés sur des transactions à niveau de risque élevé, l'incitation économique pour les marchands et pour les acteurs de la chaîne des paiements à y répondre est restée très faible. Ainsi, les e-commerçants ne sont pas encore tous en mesure de traiter opérationnellement ces messages, et leur taux de réponse (ou *retry*) reste de fait quasi-nul. En réponse à cette situation, l'Observatoire s'est attaché à développer une approche de montée en charge du *soft decline* progressive et mesurée (*cf. encadré 3 infra*), à même d'accompagner l'appropriation de ce mécanisme par les acteurs du marché.

Enfin, l'Observatoire a élaboré des supports de communication à l'attention respectivement des consommateurs et des e-commerçants, visant à expliquer la nouvelle règlementation et les conditions de la migration (*cf. encadré 2 infra*).

1.2.3 Recommandations de l'Observatoire pour le pilotage du plan de migration

L'Observatoire confirme l'attention portée à l'achèvement du déploiement de l'authentification forte pour les paiements sur Internet. Si les perturbations ayant affecté l'ensemble des acteurs de la chaîne des paiements pendant la période de confinement ont conduit à temporiser certaines actions de ce déploiement, les acteurs de marché ont été invités à reprendre activement dès juin 2020 les actions de migration dans les meilleures conditions. L'objectif est d'assurer le plus haut niveau de sécurité des paiements sur Internet au bénéfice des consommateurs et des commerçants.

T1 État d'avancement des actions inscrites au plan de migration

Action	Échéance	État
Actions inscrites au plan de migration initial		
Livraison de l'infrastructure communautaire 3D-Secure v2 sans gestion des exemptions	4e trimestre 2020	Terminé fin 2019
Réalisation de supports de communication consommateurs et commerçants	1er trimestre 2020	Terminé en juillet 2020
Chargement des bases de carte sur les nouveaux serveurs d'autorisation des émetteurs	1er trimestre 2020	Terminé en avril 2020
Introduction du mécanisme de *soft decline* par les émetteurs	31 mars 2020	Terminé en avril 2020
Déploiement de la gestion de l'exemption pour faible niveau de risque par les émetteurs	31 mars 2020	Terminé en mai 2020
Actions complémentaires décidées par l'Observatoire		
Disponibilité de l'acceptation en mode 3D-Secure v2 par l'ensemble des couples « prestataire technique d'acceptation / banque » actifs en e-commerce	Octobre 2020	En cours
Définition d'un dispositif de Place assurant la continuité des encaissements en e-commerce en cas d'incident sur les infrastructures d'authentification	Novembre 2020	En cours

Source : Observatoire de la sécurité des moyens de paiement.

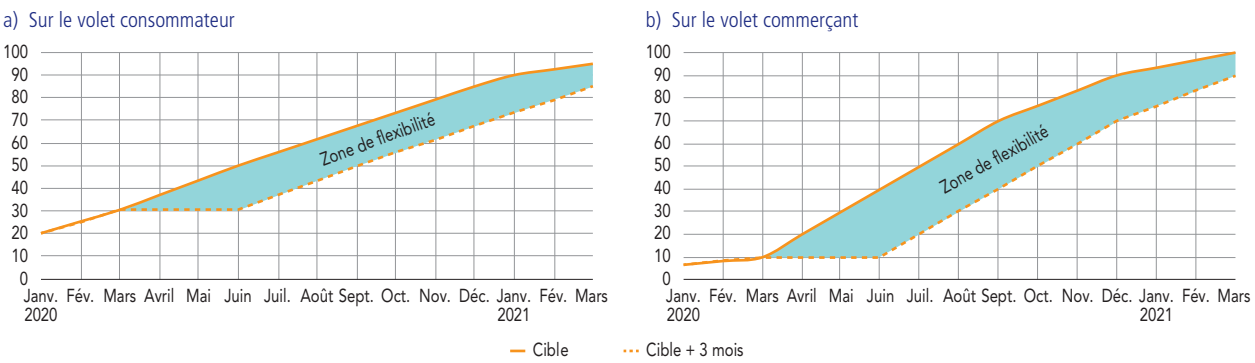
Toutefois, afin de tenir compte des répercussions de la crise sanitaire tout en les encadrant strictement, l'Observatoire a décidé d'assortir ses outils de pilotage du plan de migration d'une marge de flexibilité : les trajectoires cibles sont maintenues à l'identique, mais doublées d'une trajectoire parallèle retardée de trois mois à compter d'avril 2020 (*cf. graphique 5*). Tant que les acteurs se situeront à un niveau intermédiaire entre les deux trajectoires, leur migration pourra être considérée comme satisfaisante. En cas de retard, des actions correctives visant à assurer le retour vers la trajectoire cible seront activées :

- d'une part, des mesures individuelles : suivi renforcé par la Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR) des acteurs en retard sur la trajectoire cible ;
- d'autre part, des mesures collectives : notamment l'intensification des émissions de *soft decline* par l'ensemble des banques émettrices dans une proportion équivalente à celle du retard constaté sur le recours aux infrastructures d'authentification (*cf. encadré 3 infra*).

Par ailleurs, l'Observatoire a confié au groupe de travail en charge du pilotage de la migration deux actions complémentaires à conduire au second semestre 2020 et visant à renforcer l'accompagnement du marché :

- Un suivi de la mise à niveau des protocoles d'autorisation et d'authentification, notamment concernant les prestataires d'acceptation techniques (PAT) des marchands et les banques avec lesquelles ils opèrent ; il s'agit en effet d'assurer que l'ensemble des couples PAT/banques traitant des flux en e-commerce sera bien en mesure de proposer une solution d'encaissement conforme à la règlementation au plus tard en octobre 2020, afin de ne pas faire obstacle à la migration de leur clientèle de marchands.
- L'identification de dispositifs de continuité permettant aux commerçants de disposer d'une solution de contournement en cas d'incident affectant les nouvelles infrastructures d'authentification. Ces dispositifs devront permettre d'assurer l'identification des incidents, le partage d'information au niveau de la Place et l'activation de modes de traitement alternatifs dans un cadre normé.

G5 Matérialisation de la zone de flexibilité (en %)



Source : Observatoire de la sécurité des moyens de paiement.

ENCADRÉS

❶

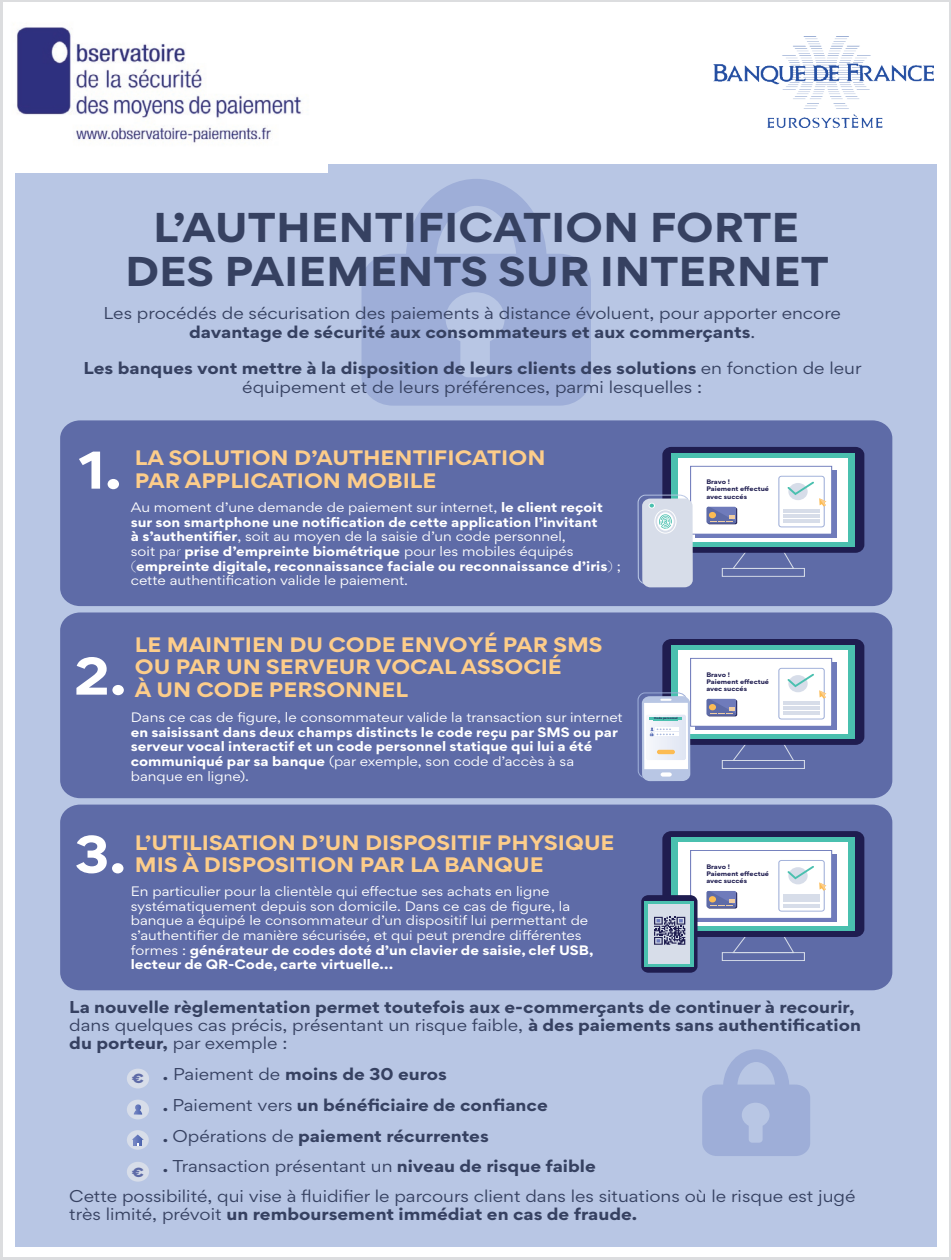
Les mesures de prévention de la fraude associées à l'élévation du plafond de paiement sans contact

Au-delà des enjeux sanitaires associés à l'élévation du plafond unitaire des paiements en mode sans contact, il convient de souligner que les aspects sécuritaires ont été un paramètre clé dans la prise de décision et dans sa mise en œuvre opérationnelle :

- Le taux de fraude sur les paiements sans contact est particulièrement stable depuis plusieurs années (à 0,020 % environ, soit un euro de fraude pour cinq mille euros de paiement), et ce en dépit de la croissance forte des volumes et de l'augmentation du plafond de vingt à trente euros. Il n'y avait ainsi pas d'alerte évidente s'opposant à l'élévation du plafond.
- La deuxième directive européenne sur les services de paiement (ou DSP 2, *cf. section 1.2*) donne aux prestataires de services de paiement la possibilité d'exempter d'authentification forte les paiements de proximité sans contact de moins de cinquante euros. L'élévation du plafond en sans contact de trente à cinquante euros est donc cohérente avec la limite fixée par la règlementation européenne.
- Afin d'assurer un pilotage renforcé de la sécurité des paiements sans contact entre trente et cinquante euros, les acteurs bancaires et les systèmes de paiement par carte ont choisi d'implémenter un appel systématique aux serveurs d'autorisation de la banque émettrice (contrairement au sans contact classique, où l'interaction se fait uniquement au niveau du terminal par la vérification du respect des plafonds paramétrés dans la puce de la carte). Si cette implémentation affecte marginalement la fluidité du paiement, elle permet à l'émetteur d'utiliser ses dispositifs de *scoring*, et donc d'identifier un risque d'utilisation frauduleuse.

Le développement de la fraude sur les paiements sans contact fait l'objet d'un suivi détaillé par l'Observatoire, qui en rend compte au chapitre 2 de son rapport annuel.

❷ Exemple de support d'information à l'attention des consommateurs



❸

Conditions de montée en charge de l'émission de messages de *soft decline*

La stratégie retenue par le Groupe de pilotage de la migration (GT Migration) s'appuie sur trois approches complémentaires, assorties d'un mécanisme spécifique d'exemption pour certains secteurs d'activité.

Approche A : montée en régime limitée et maîtrisée pour favoriser une capacité de réponse

Cette première approche à court terme vise à favoriser et à entretenir la capacité des e-commerçants et de leurs prestataires à traiter les messages de *soft decline* et à effectuer des opérations de *retry* via 3D-Secure. Il s'agit donc d'augmenter sensiblement la part de *soft declines* émis pour créer une incitation commerciale à leur traitement, tout en veillant à limiter l'impact sur l'activité des e-commerçants.

Cette approche repose sur les principes suivants :

- sélection des transactions sur la base des dispositifs d'analyse des risques des émetteurs, afin de cibler les transactions présentant le niveau de risque le plus élevé parmi les transactions acceptées en autorisation directe ;
- encadrement du niveau des émissions par le GT Migration ;
- suivi mensuel par le GT Migration des impacts des émissions de *soft decline* et ajustement le cas échéant des volumes cibles.

En première étape, le volume d'émission attendu pour la période août/septembre 2020 est fixé à la fourchette [0,1 % – 0,5 %] du nombre de transactions non conformes (c'est-à-dire non authentifiées et ne relevant pas d'un motif justifiant l'absence d'authentification forte) reçues par les émetteurs.

Approche B : émissions conditionnées par tranches de montants

Cette approche vise à systématiser l'envoi de messages de *soft decline* pour les transactions excédant certains seuils prédéfinis, afin de rapprocher progressivement cette pratique des seuils définis dans les RTS (*Regulatory Technical Standard*, norme technique de réglementation) :

1. d'octobre à décembre 2020 : transactions non conformes de plus de 2 000 euros,
2. à compter de janvier 2021 : transactions non conformes de plus de 1 000 euros,
3. à compter de mi-février 2021 : transactions non conformes de plus de 500 euros,
4. à compter d'avril 2021 : extension progressive aux transactions non conformes de moins de 500 euros.

Approche C : émissions correctives visant à redresser les écarts à la trajectoire de migration

Conformément à sa conception initiale, le *soft decline* est appelé à être utilisé plus massivement en cas de retard de l'ensemble du marché sur la mise en conformité des flux :

- dans l'hypothèse où la trajectoire du marché viendrait à se positionner en dehors de la zone de flexibilité, une cible d'émission correspondant à une proportion équivalente à celle du retard constaté ; par exemple, si le niveau de conformité des flux s'établit à 75 % des flux en valeur contre un niveau attendu d'au moins 85 % (borne basse de la zone de tolérance), alors il sera demandé aux émetteurs d'émettre des messages de *soft decline* à hauteur de 10 % de leurs flux ;
- afin de limiter le risque de choc majeur pour le marché du e-commerce, ce volume d'émission supplémentaire pourra être échelonné sur quatre semaines (dans l'exemple : 2,5 % en première semaine ; 5,0 % en deuxième semaine ; 7,5 % en troisième semaine ; 10,0 % en quatrième semaine).

Mécanisme d'exemption sectoriel à l'émission de messages de *soft decline*

Conformément à la stratégie présentée au Plénier de juin 2020, la stratégie d'émission de *soft decline* devrait s'attacher à préserver les secteurs les plus affectés par la crise sanitaire, notamment dans les secteurs du voyage, de l'hôtellerie et de l'événementiel.

Les émetteurs sont invités à ne pas émettre de messages de *soft decline* en réponse aux transactions associées aux codes marchands listés ci-après, sauf en substitution de messages de *hard decline*. Cette exemption restera applicable au moins jusqu'au 31 mars 2021.

❸

Conditions de montée en charge de l'émission de messages de *soft decline*

Liste des codes marchands bénéficiant de l'exemption

Code(s) MCC	Libellé	Code(s) MCC	Libellé
3000 à 3350	Airlines & Air Carriers	7011	Lodging – Hotels, Motels
3351 à 3500	Car Rentals	7033	Trailer Parks & Camp
3501 à 3999	Lodging	7512	Automobile Rental Agency
4011	Railroads	7519	Motor Home & Vehicle Rent
4111	Ferries	7523	Parking Lots & Garages
4112	Passenger Railways	7991	Tourist Attract. & Exhibits
4121	Taxi Cabs & Limousine	7998	Aquarium, Sea & Dolphin
4131	Bus Lines	9399	Government Services
4411	Cruise Lines	7999	Recreation Services
4511	Airline	7996	Amusement Parks, Circuses, Carnivals (…)
4722	Travel Agencies	7997	Membership Clubs (Sports, Recreation (…)
4789	Transportation Services	7922	Theatrical Producers and Ticket Agencies
6513	Vacation Rental		

Note : Le code MCC (*Merchant Category Code*) est un nombre composé de quatre chiffres associé aux paiements réalisés avec une carte bancaire. Il s'agit d'un standard international qui permet d'identifier le type d'activité du commerçant bénéficiaire de la transaction.

Source : Systèmes de paiement par carte internationaux.

2

ÉTAT DE LA FRAUDE EN 2019

2.1 Vue d'ensemble

2.1.1 Cartographie des moyens de paiement

Les opérations de paiement scripturales réalisées par les particuliers, les entreprises et les administrations représentent en 2019 un volume de 26 milliards de transactions pour un montant total de 28 658 milliards d'euros. Ces données sont en progression régulière depuis plusieurs années, avec pour 2019 une croissance de 6 % en volume et de 3 % en valeur. Entre 2018 et 2019, la répartition de l'usage des différents moyens de paiement est restée relativement stable, tant en volume qu'en valeur, avec une augmentation des paiements électroniques (carte, virement et prélèvement) et un recul des paiements non dématérialisés (chèque et effets de commerce).

Comme les années précédentes, **la carte** continue d'avoir la préférence des français qui l'utilisent dans plus de la moitié des transactions scripturales en volume (55 %, contre 53 % en 2018) pour un montant total de 599 milliards d'euros en 2019. Son usage progresse sous l'effet notamment de la poursuite du développement des paiements sans contact qui ont représenté en 2019, 3,8 milliards d'opérations (+ 59 % par rapport à 2018) pour un montant total de 42,9 milliards d'euros (+ 70 % par rapport à 2018). En complément, les retraits par carte ont représenté un peu moins de 1,4 milliard d'opérations en 2019 (– 3 % par rapport à 2018), pour un montant stable par rapport à 2018 de près de 137 milliards d'euros.

Le virement reste l'instrument de paiement privilégié pour les règlements de montant élevé (paiements des salaires et pensions, paiements interentreprises, etc.) puisqu'il représente à lui seul 87 % du montant total des paiements scripturaux, soit une part stable par rapport à 2018. Il reste le troisième moyen de paiement le plus utilisé en France (16 %) en nombre de transactions, juste après la carte et le prélèvement. Les virements sont principalement nationaux (79 % de la valeur totale des virements émis), contre 21 % à destination de l'étranger (espace SEPA – *Single Euro Payments Area* – et en-dehors). Les virements de gros montant (VGM) échangés au travers d'infrastructures de paiement dédiées et les virements SEPA classiques représentent respectivement 46 % et 47 % du montant total des virements émis. Le solde comprend d'autres formes de virement, notamment les virements SEPA instantanés et les virements internationaux hors Union européenne. Concernant les virements SEPA instantanés, disponibles en France depuis fin 2018, on observe un développement de leur usage avec un nombre de transactions multiplié sur un an par quatre-vingts (soit 14 millions d'opérations en 2019) et par soixante-quinze en valeur de transactions (soit un montant total de 7 milliards d'euros en 2019), ce qui néanmoins représente une part très marginale à l'échelle de l'ensemble des flux de virements émis (0,3 % en volume et 0,03 % en valeur).

Le prélèvement conserve le deuxième rang des instruments de paiement scripturaux les plus utilisés en volume. Il représente ainsi 17 % des transactions en nombre et atteint 6 % du montant total des transactions en 2019, soit une progression sur un an de 4 % tant en volume qu'en valeur. Son utilisation est presque exclusivement nationale (99 %), les prélèvements SEPA transfrontaliers ne représentant que 1 % de l'ensemble des flux émis.

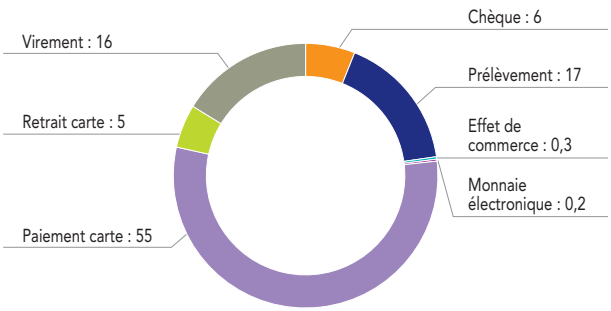
Le déclin continu du **chèque**, observé depuis les années 2000, s'est encore poursuivi en 2019, tant en nombre qu'en valeur d'opérations (– 9 % dans les deux cas), avec une émission de près de 1,6 milliard de chèques en 2019, pour un montant global de 814 milliards d'euros. Néanmoins, le chèque reste ancré dans les habitudes de paiement en particulier pour les règlements de montants élevés puisqu'il conserve son rang de troisième moyen de paiement le plus utilisé en valeur de transactions.

Les effets de commerce (lettres de change relevé et billets à ordre relevé), qui représentent moins de 1 % des transactions scripturales tant en nombre d'opérations (0,3 %) qu'en valeur (0,8 %), poursuivent leur déclin (– 8 % par rapport à 2018 en montant).

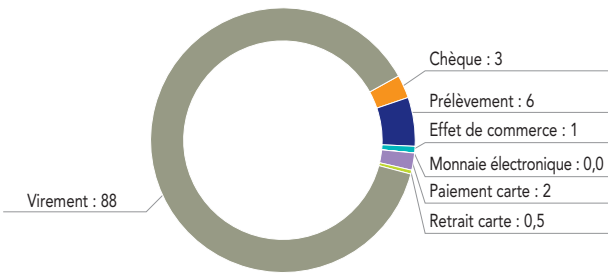
Enfin, **la monnaie électronique** représente une part marginale des transactions scripturales (moins de 1 % tant en volume qu'en valeur) et enregistre une baisse significative en 2019 (– 47 % par rapport à 2018) de son encours total qui s'établit à 561 millions d'euros.

G1 Usage des moyens de paiement scripturaux en France en 2019 (en %)

a) En volume

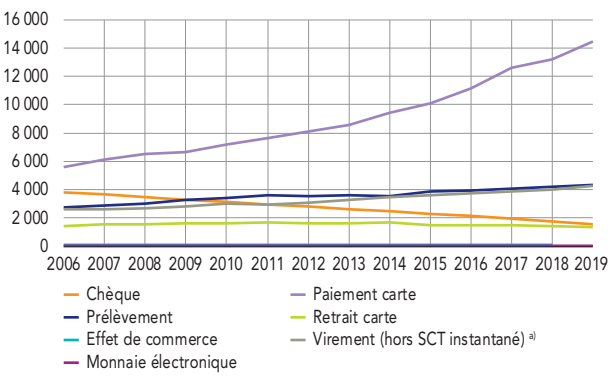


b) En montant



Source : Observatoire de la sécurité des moyens de paiement.

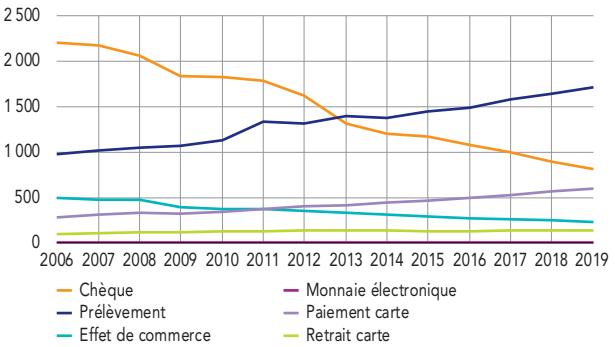
G2 Usage des moyens de paiement en France depuis 2006
(en millions d'opérations)



a) SCT instantané (*SEPA instant credit transfer*) : virement instantané.

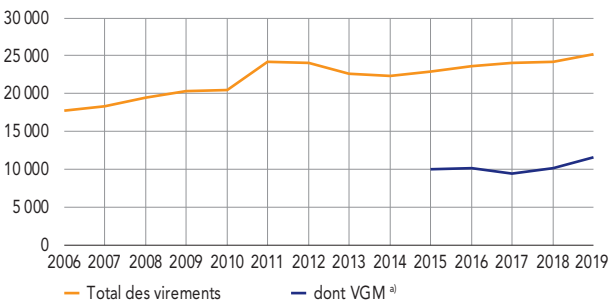
Source : Observatoire de la sécurité des moyens de paiement.

G3 Montant des transactions hors virements en France depuis 2006
(en milliards d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G4 Montant des virements en France depuis 2006 (en milliards d'euros)



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

Source : Observatoire de la sécurité des moyens de paiement.

2.1.2 Fraude aux moyens de paiement

En 2019, la fraude aux transactions scripturales représente un montant global de 1,182 milliard d'euros pour près de 7,5 millions de transactions frauduleuses, soit une hausse sur un an de 13 % en montant et de 11 % en nombre.

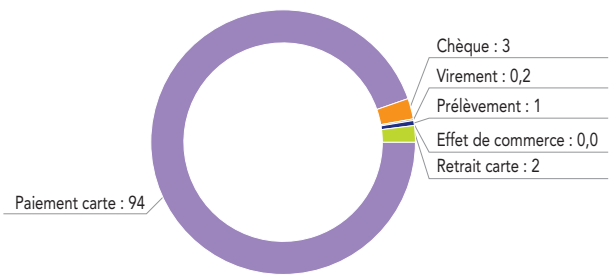
Cette progression de la fraude est portée principalement par le chèque, le virement et dans une moindre mesure par la carte. À l'inverse, le prélèvement est le seul moyen de paiement pour lequel la fraude diminue. Ainsi :

- Le **chèque** reste le moyen de paiement le plus fraudé en France, et ce pour la deuxième année consécutive, avec un montant de fraude qui atteint 539 millions d'euros (contre 450 millions en 2018, soit + 20 % sur un an). La part du chèque dans la fraude totale progresse (à 46 %, contre 43 % en 2018) alors que son usage continue de décroître, ce qui a pour effet une augmentation de son taux de fraude (0,066 % soit un euro de fraude pour 1 510 euros de paiement) qui dépasse, pour la première fois depuis la création de l'Observatoire, celui de la carte (0,064 %) ;

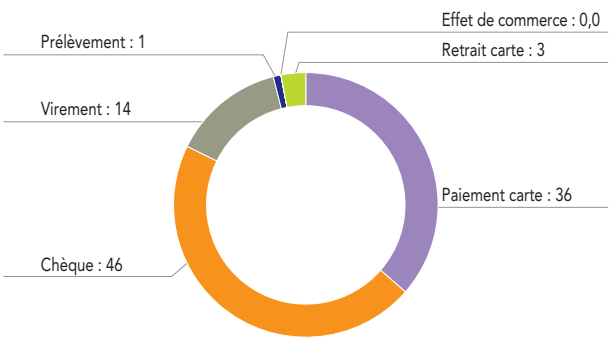
- En cumulant les transactions de paiement et de retrait, la **carte** enregistre également une hausse de ses montants de fraude en 2019 (470, contre 439 millions d'euros en 2018, soit + 7 % sur un an), et représente toujours une écrasante majorité (97 %) du nombre de transactions frauduleuses. Elle ne concentre toutefois que 39 % de la fraude globale en montant (à hauteur de 36 % pour les paiements et de 3 % pour les retraits). Le taux de fraude sur les opérations par carte progresse légèrement en 2019 pour s'établir à 0,064 % (contre 0,062 % en 2018), soit un euro de fraude pour 1 560 euros de paiement. Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,010 %, soit un euro de fraude pour 10 000 euros de paiement) mais plus significative sur les paiements à distance (0,170 %, soit un euro de fraude pour 588 euros de paiement) ;
- La fraude touchant le **virement** enregistre une forte hausse (+ 67 %) en 2019 avec un montant annuel passant de 97 à 162 millions d'euros. Toutefois, sous l'effet de la croissance des flux de paiement (+ 4 % en montant), le taux de fraude reste maîtrisé à un niveau extrêmement bas à 0,0006 % (contre 0,0004 % en 2018) ce qui représente un euro de fraude pour 160 000 euros de paiement ;
- La fraude au **prélèvement** est ramenée de 58 à 11 millions d'euros (– 81 %) sur un an de sorte que ce moyen de paiement représente le montant annuel de fraude le plus limité parmi les moyens de paiement scripturaux accessibles aux particuliers. Son taux de fraude s'établit à un niveau très bas, identique à celui du virement, à 0,0006 % ;
- Enfin, les **effets de commerce** restent relativement épargnés par la fraude, avec un montant de l'ordre de 75 000 euros en 2019 pour un seul cas de fraude, et un taux de fraude de 0,00003 % équivalent à un euro de fraude pour plus de 3 millions d'euros de paiement.

G5 Répartition de la fraude sur les moyens de paiement scripturaux en 2019 (en %)

a) En volume

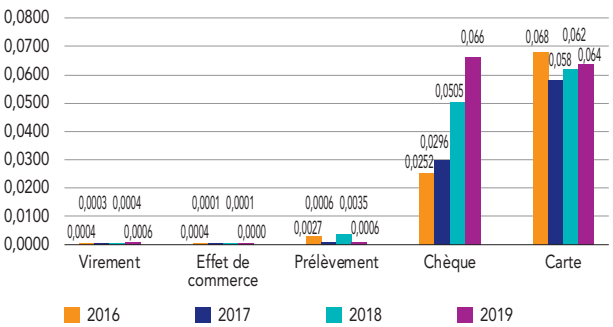


b) En montant



Source : Observatoire de la sécurité des moyens de paiement.

G6 Évolution du taux de fraude par moyen de paiement, de 2016 à 2019 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.2 État de la fraude sur le paiement et le retrait par carte

2.2.1 Vue d'ensemble

Les statistiques de fraude sur les cartes sont issues d'une collecte auprès de nombreux contributeurs (*cf. encadré 1 infra*).

La fraude sur les transactions de paiement et de retrait effectuées en France et à l'étranger avec des cartes françaises est en progression en 2019 (+ 7,1 % par rapport à 2018) et s'élève à 470 millions d'euros pour un montant total de transactions de 736 milliards d'euros, en augmentation de 4,5 % par rapport à 2018.

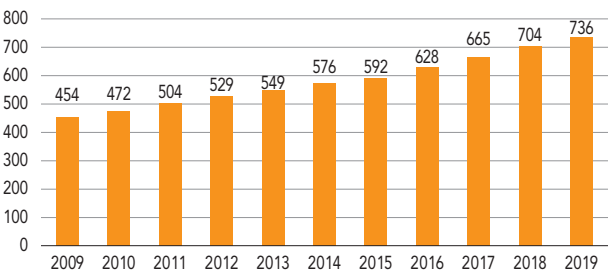
Le taux de fraude sur les cartes de paiement françaises est quasi-stable à 0,064 %, contre 0,062 % en 2018, ce qui représente l'équivalent d'un euro de fraude pour 1 560 d'euros de transactions. En tenant compte de la fraude enregistrée sur les transactions réalisées en France avec des cartes émises dans d'autres pays, une tendance à la hausse est également observée (+ 3,5 % par rapport à 2018) avec un montant total de la fraude de 557 millions d'euros en 2019, pour un montant total de transactions

atteignant 789 milliards d'euros, en progression de 3,8 % sur un an.

Sur la base de ces éléments, le taux de fraude global sur les transactions par carte traitées dans les systèmes monétiques français, incluant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises ainsi que ceux effectués en France avec des cartes étrangères reste stable à 0,071 %. Ce qui représente l'équivalent d'un euro de fraude pour 1 410 euros de transactions.

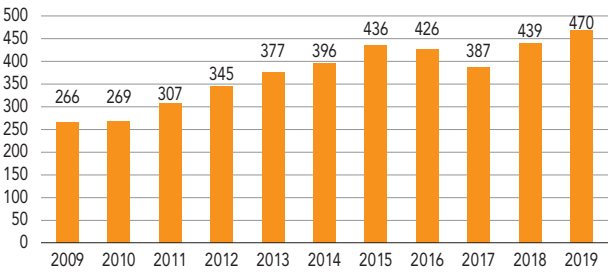
Enfin, le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2019 s'élève à 1 405 624, ce qui représente une progression de 3,4 % par rapport à 2018. Toutefois, cette hausse ne s'est pas accompagnée d'une augmentation du montant unitaire des transactions frauduleuses puisque celui-ci est au contraire en baisse à 64,9 euros, contre 70,5 euros en 2018. Ce phénomène s'explique par le renforcement des mesures pour sécuriser les paiements par carte (authentification renforcée des paiements en ligne, systèmes d'analyse du risque et de *scoring* des transactions, alertes SMS aux porteurs, etc.). Elles permettent de détecter et désactiver plus rapidement des cartes compromises. Les fraudeurs sont ainsi contraints de multiplier les tentatives de fraude, tout en réduisant leur montant unitaire pour échapper aux mécanismes de détection des opérations frauduleuses.

G7 Montant total des transactions des cartes françaises (en milliards d'euros)



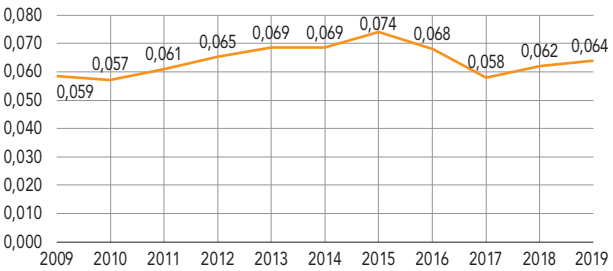
Source : Observatoire de la sécurité des moyens de paiement.

G8 Montant total de la fraude des cartes françaises (en millions d'euros)



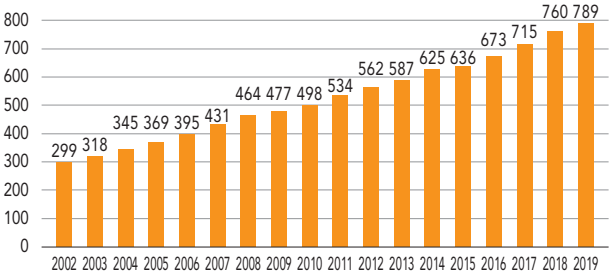
Source : Observatoire de la sécurité des moyens de paiement.

G9 Taux de fraude des cartes françaises (en %)



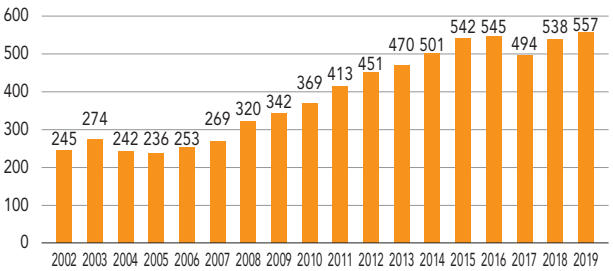
Source : Observatoire de la sécurité des moyens de paiement.

G10 Montant des transactions traitées dans les systèmes français, cartes françaises et étrangères (en milliards d'euros)



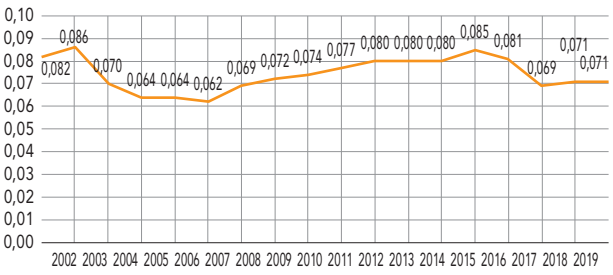
Source : Observatoire de la sécurité des moyens de paiement.

G11 Montant de la fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères (en millions d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

G12 Taux de fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.2.2 Répartition de la fraude par zone géographique

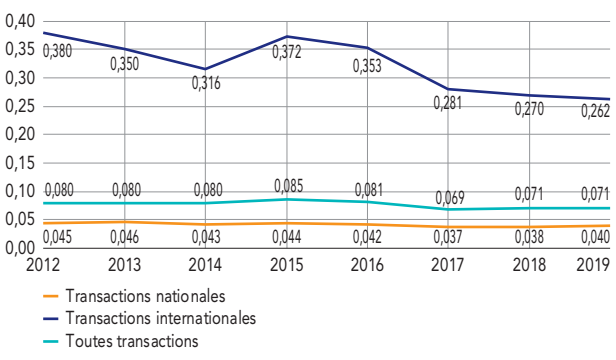
La fraude sur les transactions nationales s'est accrue de 10,2 % en 2019. Le montant de la fraude sur les transactions de paiement et de retrait effectuées en France avec des cartes françaises s'établit à 270,7 millions d'euros en 2019, contre 245,6 millions d'euros en 2018. Toutefois, sous l'effet de la croissance des transactions nationales (+ 4,2 % en valeur par rapport à 2018), le taux de fraude reste à un niveau relativement bas, quasi-stable par rapport à 2018, soit à 0,040 % (contre 0,038 % en 2018), ce qui représente l'équivalent d'un euro de fraude pour environ 2 500 euros de transactions.

En ce qui concerne les transactions internationales [1], la fraude diminue en valeur de 1,9 % en 2019, avec un montant total de fraude s'élevant à 286,3 millions d'euros. La baisse des montants fraudés, conjuguée à la progression des transactions internationales (+ 1,1 % en valeur par rapport à 2018), permet une nouvelle amélioration du taux de fraude à 0,262 %, contre 0,270 % en 2018. Il s'établit à un niveau historiquement bas mais qui reste bien supérieur au taux national (0,040 %). Ce taux de fraude demeure toujours élevé en proportion des flux puisque les transactions internationales représentent 51 % du montant total de la fraude alors qu'elles ne comptent que pour 14 % de la valeur totale des transactions.

Par ailleurs, on observe :

- pour les porteurs français, une légère baisse du taux de fraude sur les opérations qu'ils réalisent au sein de la zone SEPA [2] qui passe de 0,352 % en 2018 à 0,333 % en 2019 ; à l'inverse le taux de fraude sur les transactions qu'ils effectuent hors de l'espace européen SEPA progresse légèrement à 0,441 % (contre 0,438 % en 2018) ;

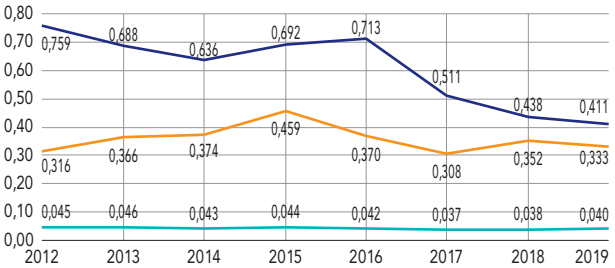
G13 Taux de fraude par zone géographique (en %)



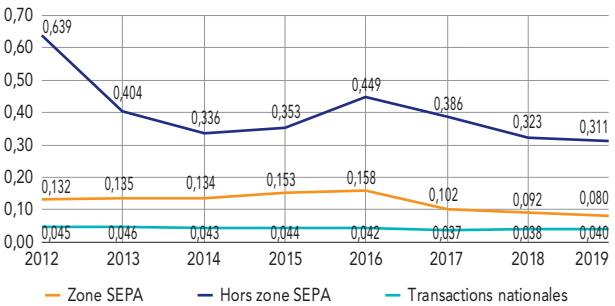
Source : Observatoire de la sécurité des moyens de paiement.

G14 Taux de fraude par zone géographique (en %)

a) Porteurs français



b) Commerçants français



Note : SEPA : *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

- pour les commerçants français, une baisse des taux de fraude sur les transactions qu'ils acceptent et qui sont réalisées avec des cartes étrangères. Toutefois, le taux de fraude sur les cartes émises en-dehors de la zone SEPA (0,311 %, contre 0,323 % en 2018) demeure près de quatre fois supérieur à celui sur les cartes émises dans l'espace européen SEPA (0,080 %, contre 0,092 % en 2018).

2.2.3 Répartition de la fraude par type de transaction

Fraude sur les transactions nationales

Bien que le montant de la fraude sur les transactions nationales ait progressé en 2019, les taux de fraude sur l'ensemble des canaux d'initiation se sont améliorés, à l'exception de celui des retraits aux distributeurs automatiques, en légère dégradation.

1 Transactions de paiement et de retrait effectuées à l'étranger avec des cartes françaises ainsi que les transactions de paiement et de retrait effectuées en France avec des cartes étrangères.

2 La zone SEPA comprend les vingt-sept pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande, le Royaume-Uni et Saint-Martin.

En effet, selon les différents types de transaction, on observe que :

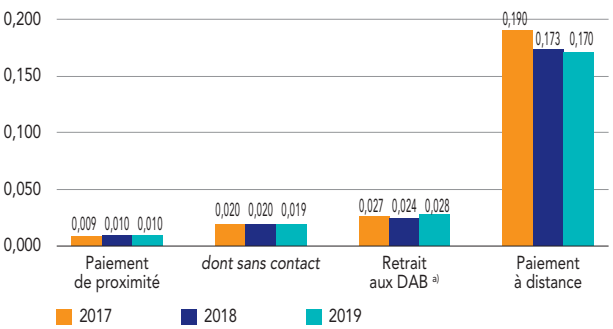
- Pour les paiements de proximité et sur automate, en dépit de l'augmentation de la fraude en 2019 (+ 7 % en valeur), le taux de fraude reste à un niveau très faible, identique à celui de 2018, soit à 0,010 %. La hausse observée sur les montants fraudés est en partie imputable à la croissance des paiements sans contact, dont le taux de fraude est sensiblement plus élevé (*cf. encadré 2 infra*). Bien que les paiements de proximité et sur automate représentent toujours une part prépondérante des transactions nationales en valeur, (près des deux tiers), ils ne comptent que pour 16 % du montant de la fraude.
- Pour les paiements à distance, malgré l'augmentation du montant de la fraude en 2019 (+ 10 % en valeur), le taux de fraude s'inscrit à nouveau en baisse, pour la huitième année consécutive à 0,170 %, contre 0,173 % en 2018 sous l'effet de la croissance des transactions à distance (+ 12 % en valeur par rapport à 2018). Cette amélioration résulte des efforts de sécurisation des émetteurs de moyens de paiement, des commerçants et des entreprises pour déployer des dispositifs d'authentification du porteur, ainsi que des outils d'analyse de risque et de *scoring* des transactions. Ces systèmes experts sont capables d'évaluer le niveau de risque d'une transaction donnée sur la base de certaines caractéristiques, comme par exemple les habitudes du client, sa localisation ou encore le matériel utilisé. Néanmoins, si la fraude sur les paiements à distance diminue, elle représente toujours la majeure partie de la fraude nationale (70,4 % en valeur), avec un taux de fraude qui reste supérieur de dix-sept fois à celui sur les paiements de proximité et sur automate. La mise en œuvre des exigences de sécurité relatives à l'authentification forte du payeur prévues par la deuxième directive sur les services de paiement (DSP 2), avec notamment l'application progressive des dispositions généralisant l'authentification renforcée et l'analyse des transactions à risque (*cf. chapitre 1.2*), devrait permettre une réduction de la fraude sur les paiements en ligne.
- Pour les retraits aux distributeurs, le montant de la fraude a progressé en 2019 (+ 16 % par rapport à 2018). Le taux de fraude s'établit à 0,028 %, contre un plus bas historique de 0,024 % en 2018, soit un niveau qui reste maîtrisé et proche de celui observé en 2016 et 2017.

Fraude sur les transactions internationales

Si les montants fraudés sur les transactions internationales ont baissé en 2019, les évolutions sont contrastées selon le canal de paiement et les zones géographiques. En règle générale, on continue à observer une meilleure maîtrise de la fraude sur les transactions réalisées avec la zone SEPA que sur celles effectuées avec des pays situés en-dehors de cette zone. Cela résulte des efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et terminaux de paiement vers le standard EMV (Europay Mastercard VISA) [3] et pour renforcer la sécurité des paiements sur Internet [4].

- Pour les cartes françaises, la fraude reste largement concentrée sur les paiements à distance dont la part dans les montants fraudés représente 92 % du total de la fraude au sein de l'espace européen SEPA (136,6 millions d'euros et un taux de fraude à 0,552 % en 2019) et 70 % du total de la fraude en dehors de la zone SEPA (36,1 millions d'euros et un taux de fraude à 1,175 % en 2019). En 2019, les taux de fraude sur les paiements à distance réalisés par courrier ou par téléphone/fax augmentent fortement et se situent à des niveaux très élevés soit 1,159 % pour ceux effectués auprès de commerçants de la zone SEPA et 1,263 % pour ceux réalisés auprès de commerçants établis en-dehors de la zone SEPA. Enfin, le taux de fraude sur les retraits effectués

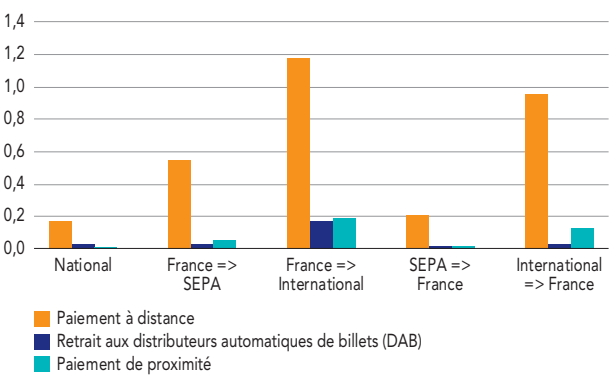
G15 Comparaison des taux de fraude sur les transactions nationales, par type de transaction (en %)



a) DAB : distributeurs automatiques de billets.

Source : Observatoire de la sécurité des moyens de paiement.

G16 Taux de fraude par type de transaction et origine géographique (en %)



Note de lecture : *Cf. annexe 5.*
Note : SEPA : *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

en-dehors de la zone SEPA demeure à un niveau élevé : 0,168 % soit près de six fois plus élevé que celui des retraits effectués en France (0,028 %). Cette situation s'explique du fait que les automates bancaires de certains pays continuent de recourir à la lecture de la piste magnétique de la carte, vulnérable à la contrefaçon.

- Pour les cartes étrangères, on continue également à observer des niveaux de fraude beaucoup plus élevés sur les transactions à distance avec des taux se situant à 0,207 % pour les cartes émises au sein de l'espace européen SEPA et à 0,956 % pour celles émises en-dehors de la zone SEPA.

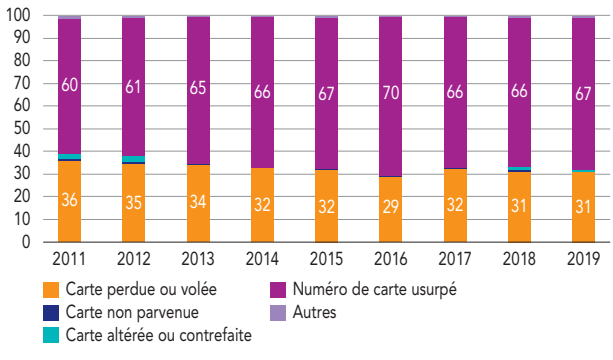
2.2.4 Répartition de la fraude par typologie

La fraude sur les transactions par carte continue d'avoir principalement pour origine l'usurpation des numéros de carte qui permet la réalisation de paiements frauduleux à distance (67 % des montants fraudés ; *cf. encadré 3 infra*). Les techniques de fraude les plus utilisées en 2019 pour usurper les numéros de cartes demeurent celles de l'hameçonnage (*phishing*) [5] et des logiciels malveillants (*malwares*) [6]. Les pertes et vols de cartes représentent la deuxième source de fraude, soit près du tiers de la fraude sur les transactions nationales (31 % des montants fraudés), une part stable par rapport à 2018.

La contrefaçon de cartes n'est à l'origine que de 1 % des paiements nationaux frauduleux. Ce niveau très bas s'explique principalement par l'adoption de technologies de cartes à puce par le plus grand nombre de systèmes de cartes privatives et par le renforcement continu de la sécurité des cartes à puce EMV existantes.

Enfin, le suivi des points physiques de compromission montre que le nombre d'attaques de distributeurs automatiques de billets et d'automates de carburant continue à diminuer en 2019 (*cf. encadré 4 infra*).

G17 Répartition de la fraude aux paiements par carte selon la typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.3 État de la fraude sur le chèque

2.3.1 Vue d'ensemble

En hausse pour la quatrième année consécutive, la fraude sur le chèque s'élève à 539 millions d'euros en 2019, soit un niveau supérieur de 20 % par rapport à 2018. Cette hausse des montants fraudés conjuguée à la décroissance des flux de paiement par chèque (– 9 % tant en nombre qu'en valeur en 2019) entraîne une hausse sensible du taux de fraude qui s'établit en 2019 à 0,066 % (contre 0,051 % en 2018) soit à un niveau supérieur à celui de la carte de paiement (0,064 % en 2019). Cela représente un euro de fraude pour 1 510 euros de paiement. Ces chiffres placent le chèque comme le premier moyen de paiement le plus fraudé en France. La part du chèque dans la fraude totale aux moyens de paiement atteint 46 %, contre 40 % pour la carte, alors même que le chèque est utilisé dix fois moins souvent que celle-ci. Le nombre de chèques fraudés progresse de 10 % en 2019 (183 488, contre 166 421 en 2018).

2.3.2 Répartition de la fraude par typologie

Les principales origines de la fraude sur le chèque restent quasiment identiques à celles de 2018. Il s'agit principalement de l'utilisation frauduleuse de chèques perdus ou volés qui représente 55 % des montants fraudés en 2019 (contre 56 % en 2018). Cette typologie de fraude recouvre principalement les chèques perdus ou volés (notamment dans les circuits de distribution des chéquiers). Ils sont utilisés par un fraudeur soit pour régler l'achat de biens ou de services, ou soit à l'encaissement sur un compte ouvert frauduleusement sur la base de fausses pièces d'identité ou par usurpation

3 EMV est un standard international de sécurité des cartes de paiement à puce, dont les spécifications ont été développées par le consortium EMVCo regroupant American Express, JCB Cards, MasterCard et Visa. Le standard EMV pour les paiements de proximité et les retraits prévoit notamment le recours à la combinaison d'une puce sécurisée sur la carte, associée à la saisie d'un code confidentiel, communément dénommée « *chip and PIN* » (puce et code PIN).

4 Le renforcement de la sécurité des paiements sur Internet s'appuie sur le déploiement de l'authentification forte du payeur, dans les conditions prévues par la deuxième directive européenne sur les services de paiement (*cf. partie 1.2 du rapport*).

5 L'hameçonnage ou *phishing* repose généralement sur l'envoi de courriels usurpant des chartes visuelles et logos connus de leurs destinataires (par exemple un établissement de crédit) et invitant les victimes à se connecter à un site qui s'avère frauduleux. L'objectif est de collecter des données de la carte.

6 Les logiciels malveillants visent tant les serveurs des grandes entreprises que les ordinateurs personnels des particuliers, et, de manière croissante, les téléphones mobiles qui sont de plus en plus utilisés dans le cadre de transactions de paiement. L'un des « *malwares* » les plus répandus, connu sous le nom de « *keylogger* » (enregistreur de frappe), permet ainsi d'enregistrer les touches frappées au clavier par la victime. Ces logiciels malveillants son généralement inoculés, à l'insu de l'utilisateur, au travers de sources apparemment de confiance.

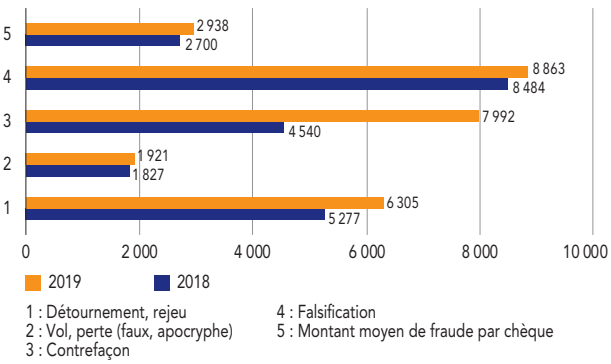
d'identité ou sur celui d'une tierce personne. Concernant ce dernier mode opératoire, qui est en fort développement, le fraudeur a recours à des « mules » recrutées via les réseaux sociaux. Il les charge, en contrepartie d'une promesse de rémunération, d'encaisser les chèques frauduleux sur leurs propres comptes bancaires, puis de lui reverser les fonds. L'Observatoire précise que les « mules » qui participent à ce type de fraude encourent le risque d'être reconnues complices de fraude, un délit passible de poursuites judiciaires. Il appelle par ailleurs les utilisateurs à être particulièrement attentifs à la bonne réception de leur commande de chéquiers et aux modalités de conservation de ceux-ci (comme rappelé parmi les bonnes pratiques en matière de vigilance présentées en annexe 1 de ce rapport). L'autre grande typologie de fraude rencontrée est la falsification de chèques régulièrement émis. Ce mode opératoire, qui consiste à modifier frauduleusement le montant ou le bénéficiaire d'un chèque valide, représente 27 % des montants fraudés, contre 33 % en 2018. Enfin, la contrefaçon de chèque, c'est-à-dire l'encaissement de chèques fabriqués de toutes pièces par le fraudeur, augmente en 2019 et représente 14 % des montants fraudés, contre 8 % en 2018.

G18 Répartition de la fraude par chèque en montant par typologie de fraude (en %)



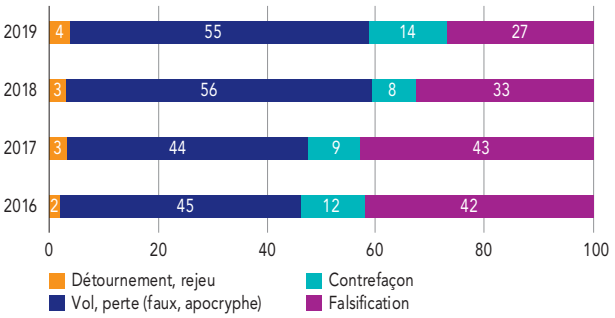
Source : Observatoire de la sécurité des moyens de paiement.

G19 Montant unitaire de fraude par chèque par typologie de fraude, 2018–2019 (en euros)



Source : Observatoire de la sécurité des moyens de paiement.

G20 Répartition de la fraude par chèque en montant, par typologie de fraude, 2016–2019 (en %)



Source : Observatoire de la sécurité des moyens de paiement.

Le montant moyen d'un chèque frauduleux progresse à 2 938 euros, contre 2 700 en 2018. Cette augmentation concerne toute typologie de fraude, avec des montants unitaires particulièrement élevés pour la falsification de chèque (8 863 euros, contre 8 484 euros en 2018) et la contrefaçon (7 992 euros, contre 4 540 euros en 2018).

Devant la progression continue de la fraude au chèque constatée au cours des quatre dernières années, l'Observatoire a décidé de conduire une étude sur les pistes de renforcement de la sécurité du chèque, en y associant l'ensemble des parties prenantes concernées (banques, autorités publiques, associations de consommateurs, d'entreprises et de commerçants, et prestataires techniques intervenant dans le cycle de traitement de ce moyen de paiement). Ces travaux seront présentés dans le rapport annuel 2020 de l'Observatoire, assortis de recommandations à l'attention des différentes catégories d'acteurs impliqués.

2.4 État de la fraude sur le virement

2.4.1 Vue d'ensemble

En 2019, la fraude sur les virements émis depuis un compte tenu en France a de nouveau progressé pour s'établir à près de 162 millions d'euros. Il s'agit d'une hausse significative : 66 % par rapport à 2018, pour un nombre de cas qui a plus que doublé, soit près de 16 000 opérations frauduleuses en 2019. Le montant moyen d'un virement frauduleux diminue à 10 144 euros, contre 12 586 euros en 2018.

Sous l'effet de la croissance des flux de virement (+ 4 % en valeur par rapport à 2018) et de leur importance (87 % du montant total des paiements scripturaux émis en 2019), le taux de fraude reste à un niveau extrêmement bas, à

0,0006 % (contre 0,0004 % en 2018), soit un euro de fraude pour 160 000 euros de paiement. Le virement reste le moyen de paiement le moins fraudé en proportion, alors qu'il est celui qui véhicule les montants globaux les plus importants. Toutefois, ce taux de fraude revêt des disparités selon le canal d'initiation de l'ordre de virement, le type de virement émis ou encore la destination géographique des fonds.

2.4.2 Répartition de la fraude par canal d'initiation

En 2019, l'initiation de virement depuis les espaces de banque en ligne (sur Internet ou via application mobile) reste le canal le plus touché puisqu'il représente à lui seul 55 % des montants fraudés, contre 42 % en 2018. Cette part est proportionnellement élevée dans la mesure où les virements émis depuis ce canal ne représentent que 15 % de l'ensemble des flux de virement. Le taux de fraude sur ce canal d'initiation progresse de façon significative à 0,0023 % (contre 0,0005 % en 2018), soit à un niveau quatre fois supérieur à celui de ce moyen de paiement. Cela correspond à un euro de fraude pour 43 500 euros de paiement. Cette progression résulte d'une recrudescence de faux ordres de virement initiés par des fraudeurs à partir de l'usurpation des données personnelles de connexion aux espaces de banque en ligne ou mobile du client légitime.

Les virements émis sur support papier (courrier, appel téléphonique, etc.) représentent 21 % des montants fraudés, contre 22 % en 2018. Cette part est importante en proportion des flux de virements émis sur support papier qui constituent seulement 8 % du total des émissions de virement. Le taux de fraude sur les ordres de virement papier est en hausse à 0,0017 % (contre 0,0010 % en 2018), soit un niveau près de trois fois supérieur à celui de ce moyen de paiement. La fraude aux virements émis sur support papier résulte soit de l'émission de faux ordres par le fraudeur, qui usurpe alors l'identité du titulaire du compte débité, soit de techniques de manipulation par ingénierie sociale[7] visant à conduire le titulaire du compte à émettre un ordre de virement illégitime. Ce canal est particulièrement exposé à la fraude compte tenu de ses caractéristiques propres qui ne permettent pas la mise en place des dispositifs avancés de sécurisation.

Enfin, le canal télématique (utilisé principalement par la clientèle professionnelle) demeure le mode d'initiation des ordres de virement le plus sécurisé avec une part dans les montants fraudés en baisse (24 %, contre 37 % en 2018) et un taux de fraude extrêmement bas à 0,0002 % (stable par rapport à 2018).

2.4.3 Répartition de la fraude par type de virement

La quasi-totalité des virements (98,5 % des volumes) étant émis sous la forme du virement SEPA classique, ceux-ci concentrent logiquement une part très importante des montants fraudés, soit 81 % en 2019. Toutefois, dans la mesure où le virement SEPA classique ne véhicule que 47 % des flux en valeur, son taux de fraude s'établit à un niveau relativement faible de 0,0011 %, soit l'équivalent d'un euro de fraude pour environ 91 000 euros de paiement.

En ce qui concerne le virement SEPA instantané, si sa part dans les montants fraudés est faible à 1 % compte tenu de son usage encore très modeste (0,3 % en volume et 0,03 % en valeur des virements émis), en revanche son taux de fraude s'établit à 0,0311 %, soit à un niveau supérieur de près de cinquante fois au taux global de ce moyen de paiement.

Enfin, les virements de gros montants (VGM), échangés au travers d'infrastructures de paiement dédiées et correspondant exclusivement à des paiements de clientèle entreprise de montant unitaire élevé ou urgents, sont relativement épargnés par la fraude. Le montant moyen fraudé est de l'ordre de 15,4 millions d'euros en 2019. Cependant, le taux de fraude est extrêmement bas à 0,0001 %, ce qui équivaut à un euro de fraude pour plus d'un million d'euros de paiement.

2.4.4 Répartition de la fraude par zone géographique

Si toutes les zones géographiques enregistrent une progression de la fraude au virement, cette augmentation est toutefois particulièrement importante pour les virements nationaux (+ 168 % en valeur par rapport à 2018). En conséquence, la part des virements nationaux dans les montants fraudés progresse à 52 %, contre 32 % en 2018. Néanmoins, compte tenu de la croissance des flux de paiement (+ 6 % en valeur), le taux de fraude sur ces transactions reste particulièrement contenu, à 0,0004 % (soit un euro de fraude pour 250 000 euros de paiement).

En ce qui concerne les virements transfrontaliers, qui ne constituent que 21 % des virements émis en valeur, la hausse de la fraude est plus mesurée (+ 18 % en valeur par rapport à 2018). Mais leurs taux de fraude restent structurellement plus élevés que celui des virements nationaux, à 0,0016 % pour ceux émis vers un pays de la zone SEPA (hors France) et à 0,0011 % pour ceux émis en dehors.

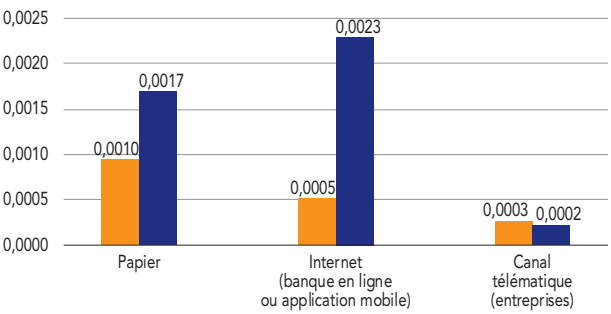
7 L'ingénierie sociale se définit comme « l'art de manipuler son interlocuteur » pour qu'il réalise une action ou divulgue une information confidentielle.

2.4.5 Répartition de la fraude par typologie de fraude

Comme en 2018, le faux virement, c'est-à-dire l'émission d'un ordre de virement par le fraudeur au moyen d'attaques informatiques par *malware* et *phishing*, reste le type de fraude prédominant puisqu'il représente à lui seul 61 % des montants fraudés (contre 52 % en 2018). Ce procédé a été particulièrement actif en fin d'année 2019, avec une multiplication des attaques opportunistes s'appuyant sur la mise en place des solutions d'authentification forte par les banques et l'exploitation des actions de communication associées, en envoyant de faux messages visant à collecter les données personnelles de connexion aux espaces de banque en ligne ou mobile pour ensuite initier des virements frauduleux.

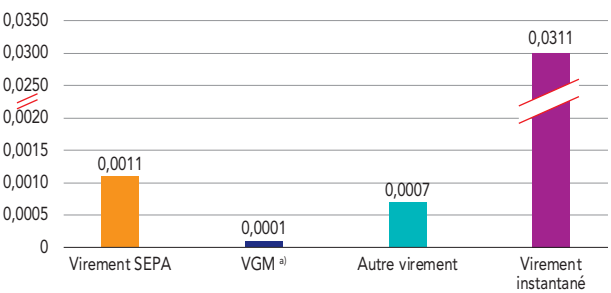
Le détournement demeure le deuxième type de fraude sur le virement avec une part dans les montants fraudés à 35 % (contre 41 % en 2018). Cette typologie de fraude recense les fraudes de type ingénierie sociale, comme par exemple « la fraude au président » (*cf. tableau 2 infra*) ou celle « au changement de coordonnées bancaires », qui touchent particulièrement les entreprises.

G21 Taux de fraude sur les virements par canal d'initiation (en %)



Source : Observatoire de la sécurité des moyens de paiement.

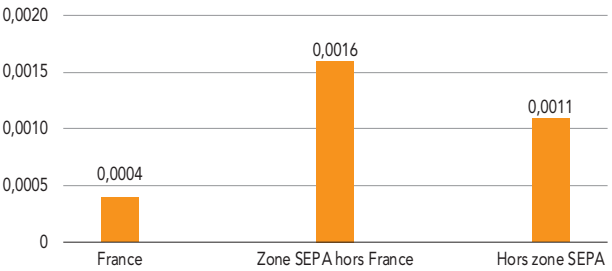
G22 Taux de fraude sur les virements par type de virement (en %)



a) VGM : virement de gros montant.

Source : Observatoire de la sécurité des moyens de paiement.

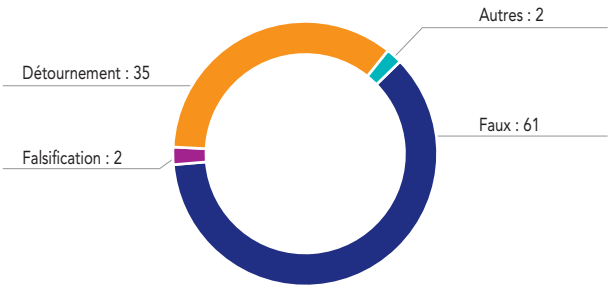
G23 Taux de fraude sur les virements par zone géographique (en %)



Note : SEPA : *Single Euro Payments Area.*

Source : Observatoire de la sécurité des moyens de paiement.

G24 Répartition de la fraude au virement en montant, par typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.5 État de la fraude sur le prélèvement

2.5.1 Vue d'ensemble

En 2019, les prélèvements frauduleux émis au débit d'un compte tenu en France s'élèvent à 11 millions d'euros, contre près de 58 millions d'euros en 2018, soit une baisse significative de 81 %. **Le prélèvement est le moyen de paiement qui présente le montant annuel de fraude le plus limité parmi les instruments de paiement accessibles aux particuliers.** Le taux de fraude sur le prélèvement enregistre une baisse significative à 0,0006 %, contre 0,0035 % en 2018, soit à un niveau équivalent à celui du virement. Le montant moyen d'un prélèvement frauduleux s'établit toutefois en progression, à 253 euros, contre 188 euros en 2018.

2.5.2 Répartition de la fraude par typologie

Alors qu'en 2018, la fraude au prélèvement avait pour unique origine le faux prélèvement, c'est-à-dire l'émission d'ordres de prélèvement par un créancier fraudeur sans

aucune autorisation ou réalité économique, cette typologie a fortement diminué en 2019 (– 93 % en valeur). Elle ne constitue plus que 34 % des montants fraudés, contre 99 % en 2018.

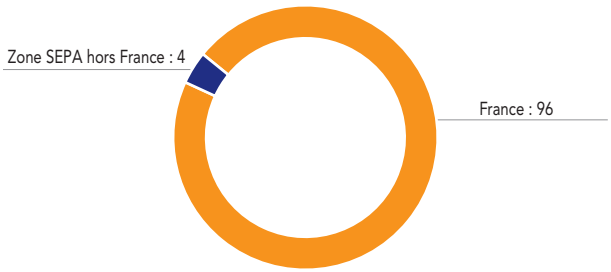
À l'inverse, la typologie de fraude « Détournement » qui correspond à l'usurpation par un fraudeur de l'IBAN [8] aux fins de souscrire des services (de téléphonie par exemple) réapparaît en 2019 avec une part dans les montants fraudés à 61 % alors qu'elle avait quasiment disparu en 2018.

2.5.3 Répartition de la fraude par zone géographique

Le prélèvement étant utilisé presque exclusivement au niveau domestique (99 % des flux en valeur), la fraude reste concentrée sur les transactions nationales. Celle-ci s'élève à 96 % des montants fraudés, contre 76 % en 2018, avec néanmoins un taux de fraude extrêmement bas à 0,0006 %.

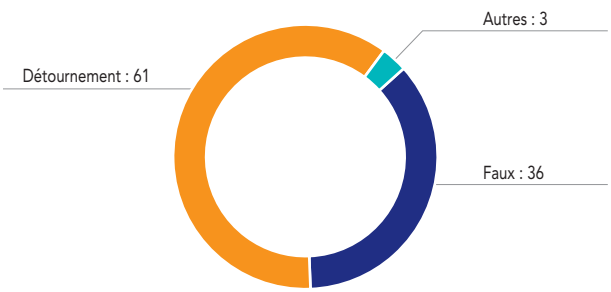
En ce qui concerne les prélèvements transfrontaliers, c'est-à-dire émis vers des comptes tenus par des établissements de la zone SEPA, même s''ils enregistrent une progression de 49 % en valeur sur un an, leur part dans les montants fraudés diminue à 4 % (contre 24 % en 2018). Leur taux de fraude s'établit à 0,0020 %, soit un niveau trois fois plus élevé que celui du taux de fraude global sur ce moyen de paiement.

G25 Répartition de la fraude au prélèvement en montant, par zone géographique (en %)



Note : SEPA : *Single Euro Payments Area.*
Source : Observatoire de la sécurité des moyens de paiement.

G26 Répartition de la fraude au prélèvement en montant, par typologie de fraude (en %)



Source : Observatoire de la sécurité des moyens de paiement.

8 *International bank account number.*

Typologie de la fraude au chèque en 2019

Principaux cas de fraude	Mesures de prévention
Vol de chéquiers dans les circuits de distribution : les circuits de distribution font intervenir de nombreux prestataires extérieurs aux banques, notamment pendant le transport ou lors de la remise au client. Le vol de chéquiers ou de formules de chèques vierges peut se produire à deux niveaux : • en amont de la délivrance au client : chez les prestataires fabricants et/ou expéditeurs, chez les prestataires transporteurs ou distributeurs vers les agences bancaires, dans les boîtes à lettres des clients bénéficiaires, • lors de la remise en agences bancaires, les fraudeurs utilisent des pièces d'identité volées ou falsifiées pour se faire remettre un chéquier. **Vol de chéquiers lors de la détention par le client lui-même** faisant suite à un cambriolage, au vol ou à la perte de son chéquier.	**Traçabilité des envois** de chéquiers et lettres chèques durant les phases de transport. **Information par la banque de la mise à disposition d'un chéquier**, soit en agence bancaire, soit par pli postal selon l'option définie par le client lors de la souscription au moyen de paiement, et indication d'un délai attendu de mise à disposition, permettant au client d'informer sa banque en cas de retard constaté. **Rappel régulier par les banques des obligations de vigilance** des détenteurs de chéquiers et lettres chèques et de l'obligation de déclaration en cas de perte ou de vol, même en cas de souscription d'une assurance couvrant ces événements.
Falsification d'un chèque régulier intercepté par les fraudeurs, consistant à altérer le chèque subtilisé par grattage, gommage ou effacement, se manifeste par le fait que, concrètement, les fraudeurs tirent profit des vulnérabilités présentes sur le chèque subtilisé pour le modifier, par exemple : • en substituant, par grattage ou gommage, le nom du bénéficiaire légitime inscrit avec une encre faible, • en réécrivant un nom de bénéficiaire sur celui du bénéficiaire légitime, • en ajoutant une mention (par exemple nom ou sigle, tampon de société, etc.) après celui du bénéficiaire légitime sur l'espace libre de la ligne non remplie, • en ajoutant un montant en lettres et/ou en chiffres sur l'espace libre laissé avant ou après la mention manuscrite.	**Examen systématique du chèque et des mentions portées, ainsi que de leur cohérence avec l'identité du payeur.** Il s'agit de réaliser un examen physique du chèque afin d'identifier les éventuelles altérations avant son acceptation, ainsi que de contrôler l'identité du payeur, via la demande par exemple d'une pièce d'identité ou d'un justificatif de domicile. **Les commerçants peuvent se prémunir des chèques irréguliers en accédant au fichier national des chèques irréguliers (FNCI)** de la Banque de France, service officiel de prévention des impayés chèques [1].
Contrefaçon de chèque, en créant un faux chèque de toutes pièces, émis sur une banque existante ou une fausse banque.	**Examen physique approfondi du chèque et des documents d'identité du payeur** (*cf. ci-dessus*).
Techniques de fraude dérivées du processus dit de « **cavalerie** » consistant en une remise à l'encaissement de plusieurs chèques frauduleux, suivie immédiatement de virements des fonds crédités, et visant principalement les comptes de professionnels et d'entrepreneurs bénéficiant de mécanismes de crédit en compte immédiat des chèques remis à l'encaissement.	**Identification des flux d'encaissement atypiques** au regard du profil du client afin de suspendre, le cas échéant, les opérations de retrait ou de transfert des fonds vers un autre établissement, immédiatement consécutives à une remise de chèques.

1 Cf. *https://www.verifiance-fnci.fr*

Source : Observatoire de la sécurité des moyens de paiement.

Typologie de la fraude au virement en 2019

Cas de fraude rencontrés	Mesures de prévention
En 2019, la fraude de type **détournement au moyen de techniques d'ingénierie sociale** a revêtu essentiellement les formes exposées ci-après. • **La fraude au président** : le fraudeur usurpe l'identité d'un haut responsable de l'entreprise pour obtenir d'un collaborateur la réalisation d'un virement urgent et confidentiel à destination de l'étranger. Pour ce faire, le fraudeur utilise des informations recueillies sur l'entreprise et ses dirigeants sur Internet ou directement auprès des services de l'entreprise. • **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 avec un courrier en bonne et due forme du créancier. • **La fraude au faux technicien** : le fraudeur usurpe l'identité d'un technicien informatique (de la banque, par exemple) pour effectuer des faux tests dans le but de récupérer des identifiants de connexion, provoquer des virements frauduleux ou encore procéder à l'installation de logiciels malveillants. • **La fraude au faux conseiller bancaire** : le fraudeur usurpe le numéro de téléphone du conseiller bancaire, généralement en période d'absence de ce dernier, et contacte le client pour obtenir des informations.	**Outils de surveillance et de détection des transactions à caractère inhabituel** qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison par exemple de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Un contre-appel auprès du client peut alors être fait afin de vérifier le bien-fondé de l'ordre de virement. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des entreprises et des particuliers.
Les **attaques informatiques** ont principalement visé en 2017 les sites de banque en ligne et les canaux télématiques, tels que par exemple 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) et ont été réalisées essentiellement par deux moyens. • ***Malwares*** : des 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). Ces *malwares* permettent à des fraudeurs d'analyser et de collecter les données transitant par l'ordinateur ou le système d'information du client. Ainsi, lors de la connexion au site de banque en ligne d'un client, le *malware* récupère les identifiant et mot de passe que le client a saisis puis les réutilise pour s'y connecter lui-même, faire une demande d'ajout de bénéficiaire et initier un ordre de virement frauduleux. • ***Phishing* ou hameçonnage** : technique permettant de collecter des données personnelles et bancaires à partir de courriels non sollicités invitant leurs destinataires à cliquer sur un lien renvoyant vers un faux site (celui d'une banque en ligne ou d'un marchand en ligne) lequel le plus souvent demande à l'internaute de communiquer ses coordonnées bancaires. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide (facture à régler sous peine de la suspension d'un service, régularisation d'une interdiction bancaire ou encore une mise à jour sécuritaire). Des variantes du *phishing* sur d'autres canaux sont également mises en œuvre, comme le *smishing* par SMS.	**Déploiement d'un dispositif d'authentification forte pour la validation des ordres de virement** saisis en ligne. **Mise en place d'une temporisation ou d'une authentification forte du client pour l'ajout de nouveaux bénéficiaires** de virement depuis le site de banque en ligne. **Fixation de plafonds maximaux de virements** sur le site de banque en ligne. **Mise à disposition aux clients de solutions informatiques de sécurisation** permettant la recherche d'infections de type *malware* sur les postes de la clientèle. **Outils de surveillance et de détection** des transactions à caractère inhabituel qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison, par exemple, de son montant ou du pays destinataire des fonds, eu égard à l'activité habituelle du client. Une alerte peut être adressée au client pour lui permettre de faire opposition à la transaction, le cas échéant, pendant la durée de temporisation. **Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des particuliers.

Source : Observatoire de la sécurité des moyens de paiement.

Typologie de la fraude au prélèvement en 2019

Cas de fraude rencontrés	Mesures de prévention
Émission illégitime d'ordres de prélèvement (faux prélèvement) : le créancier fraudeur s'enregistre en tant qu'émetteur de prélèvement auprès d'un prestataire de services de paiement et émet massivement des prélèvements vers des IBAN (*international bank account number*) qu'il a obtenus illégalement et sans aucune autorisation.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire. **Envoi d'une alerte aux clients débiteurs** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »).
Usurpation d'IBAN pour la souscription de service (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.	**Envoi d'une alerte aux clients débiteurs** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays, ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelées aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelées aussi « listes noires »).
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 rétraction légale (de 13 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 transférés vers un compte tenu à l'étranger.	**Outils de surveillance de l'activité des créanciers émetteurs de prélèvement** qui permettent de déceler d'éventuels flux anormaux au regard des éléments de connaissance du client. Il est à préciser que pour émettre des prélèvements, un créancier doit disposer d'un identifiant créancier SEPA (ICS) qui lui est attribué après que son prestataire de services de paiement se soit assuré de son aptitude à pouvoir le faire.

Source : Observatoire de la sécurité des moyens de paiement.

ENCADRÉS

❹ Statistiques de fraude sur les cartes : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire recueille les données de l'ensemble des émetteurs de cartes de type « interbancaire » ou « privatif » [1].

Les statistiques calculées par l'Observatoire pour l'année 2019 portent ainsi sur :

- 716,6 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 84 millions de cartes de type « interbancaire » émises en France (dont 73 millions de cartes avec la fonction sans contact) ;
- 19,2 milliards d'euros de transactions réalisées (principalement en France) avec 8,7 millions de cartes de type « privatif » émises en France ;
- 53,3 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».

Les données recueillies proviennent :

- Des cent vingt membres du Groupement des cartes bancaires CB. Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et de Visa Europe France ;
- De huit émetteurs de cartes privatives : American Express, Oney Bank, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance, Cofidis, Franfinance, JCB et UnionPay International.

1 Les systèmes de paiement par carte dits « interbancaires » correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. À l'inverse, les systèmes privatifs sont ceux pour lesquels il existe un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs.

5
Fraude aux paiements sans contact

Les paiements nationaux en mode sans contact ont poursuivi leur croissance à un rythme soutenu avec une augmentation de 59 % en volume et de 70 % en valeur par rapport à 2018. Ainsi, sur l'ensemble de l'année 2019, ce sont 3,7 milliards de paiement sans contact qui ont été réalisés (contre 2,3 milliards en 2018) pour un montant total de 41,6 milliards d'euros (contre 24,4 milliards d'euros en 2018). Les paiements sans contact représentent ainsi 10 % de la valeur et 31 % des volumes des paiements en proximité, de sorte qu'en 2019, près d'un paiement par carte sur trois en situation de proximité a été effectué en mode sans contact. Le montant moyen d'un paiement sans contact s'établit à 11,3 euros, contre 10,5 euros en 2018. Si l'on ajoute aux paiements nationaux sans contact ceux réalisés en France au moyen de cartes étrangères et ceux effectués avec des cartes françaises à l'étranger, ce sont 3,9 milliards d'opérations qui ont été réalisées pour un montant total de 44,3 milliards d'euros. Cela correspond à une progression sur un an de 135 % en valeur et de 126 % en volume.

En dépit de la croissance forte des flux de paiement et du relèvement du plafond de vingt à trente euros, le taux de fraude sur les transactions nationales en mode sans contact s'améliore très légèrement à 0,019 % (contre 0,020 % en 2019), avec un montant total de fraude de près de 7,9 millions d'euros. Le taux de fraude sur les paiements sans contact se situe toujours à un niveau intermédiaire entre celui des paiements de proximité (0,010 %) et celui des retraits (0,028 %), et bien en deçà de celui des paiements à distance (0,170 %). Si l'on ajoute à cette fraude nationale celle engendrée sur les paiements sans contact effectués au moyen de cartes étrangères en France et ceux réalisés par des cartes françaises à l'étranger, le taux de fraude ressort à un niveau quasi-stable à 0,020 %, contre 0,021 % en 2018.

En 2019 et comme les années précédentes, la fraude sur les paiements sans contact résulte seulement du vol ou de la perte de la carte. En effet, les émetteurs de carte fixent des plafonds sur le montant d'une transaction unitaire (montant fixé au maximum à cinquante euros [1]) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (cumul fixé au plus à 250 euros). Ces mesures permettent de limiter le préjudice subi en cas de perte ou de vol d'une carte. Il est d'ailleurs rappelé que le porteur est protégé par la loi en cas de fraude et ne supporte aucune perte (*cf. annexe 2*).

Ces données intègrent les paiements initiés avec des équipements de téléphonie mobile, dont l'usage progresse également en 2019, bien que leur part dans les transactions de proximité demeure encore très marginale (0,18 % en valeur et 0,38 % en volume). En 2019, les transactions nationales par équipements de téléphonie mobile représentent 45,2 millions d'opérations, soit un peu plus de quatre fois plus qu'en 2018, et un montant total de près de 794,2 millions d'euros, contre 190,9 millions d'euros en 2018. Avec les transactions effectuées en France par des équipements de téléphonie mobile étrangers et celles réalisées à l'étranger par des équipements de téléphonie mobile français, le montant total des transactions s'élève à un peu plus d'un milliard d'euros pour 58,8 millions d'opérations.

En 2019, des cas de fraude ont été enregistrés sur des transactions nationales par équipements de téléphonie mobile, pour un montant total toutefois peu significatif (environ 197 000 euros) et un taux de fraude à 0,02 % (contre 0,03 % en 2018). La fraude sur le paiement mobile, toutes zones confondues, s'établit à 0,03 %, contre 0,04 % en 2018 pour un montant total de fraude d'un peu plus de 326 000 euros.

1 Mesure effective à compter du 11 mai 2020.

❻
Fraude nationale sur les paiements à distance selon le secteur d'activité

L'Observatoire a collecté des données permettant de fournir des indications sur la répartition de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions nationales (*cf. tableau*).

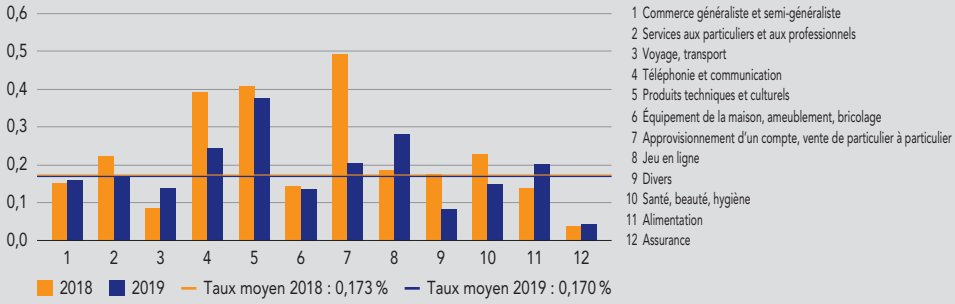
Les secteurs « Commerce généraliste et semi-généraliste », « Services aux particuliers et aux professionnels », « Voyage et transport » et « Téléphonie et communication » demeurent toujours les plus exposés, concentrant à eux seuls 72 % du montant total de la fraude en vente à distance. La comparaison des taux moyens de fraude de chacun des secteurs d'activité permet de constater que les secteurs « Produits techniques et culturels », « Jeu en ligne » et « Vente de particulier à particulier » et « Alimentation », qui comptent pour une plus faible part du total de la fraude, subissent néanmoins des taux de fraude largement supérieurs à la moyenne (*cf. graphique*). À l'inverse, le secteur « vente de particulier à particulier » enregistre une baisse notable de son taux de fraude à 0,206 %, contre 0,494 % en 2018.

Répartition de la fraude par secteur d'activité (montant en millions d'euros, part en pourcentage)

		Montant	Part
1	Commerce généraliste et semi-généraliste	44,3	23,2
2	Services aux particuliers et aux professionnels	42,1	22,1
3	Voyage, transport	24,6	12,9
4	Téléphonie et communication	25,7	13,5
5	Produits techniques et culturels	14,9	7,8
6	Équipement de la maison, ameublement, bricolage	10,1	5,3
7	Approvisionnement d'un compte, vente de particulier à particulier	11,7	6,1
8	Jeu en ligne	6,0	3,2
9	Divers	5,9	3,1
10	Santé, beauté, hygiène	2,0	1,0
11	Alimentation	2,6	1,4
12	Assurance	0,7	0,4
Total		**190,6**	**100,0**

Source : Systèmes de paiement par carte internationaux.

Taux de fraude en vente à distance par secteur d'activité, transactions nationales (en %)



Source : Observatoire de la sécurité des moyens de paiement.

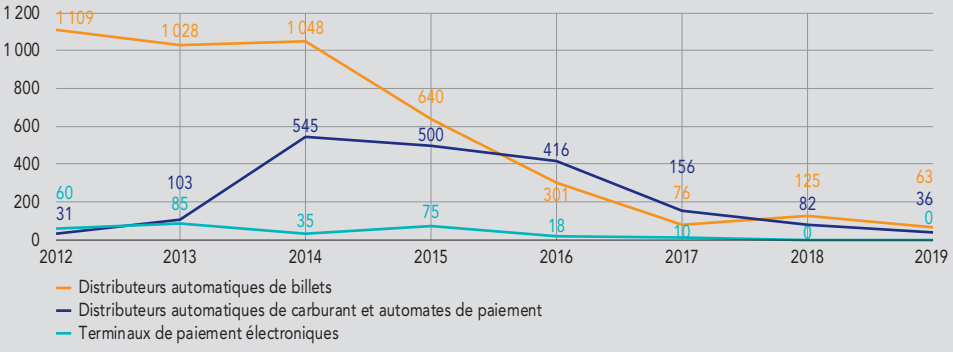
7
Indicateurs des services de police et de gendarmerie

Le nombre de piratages de distributeurs automatiques de billets (DAB) a à nouveau diminué en 2019 avec 63 cas recensés, contre 125 un an plus tôt. Les compromissions de DAB par la technique du « *jackpotting* », apparue depuis 2016, se sont poursuivies en 2019 avec des vagues d'attaques à grande échelle qui montrent des évolutions notables dans les modes opératoires utilisés. Le *jackpotting* consiste à prendre le contrôle d'un distributeur en y connectant un ordinateur portable soit pour accéder aux données du calculateur du DAB, soit pour lui injecter un *malware*.

Les attaques de distributeurs automatiques de carburant (DAC) sont également en nette baisse avec 26 cas recensés en 2019 (contre 64 cas en 2018) ; il en est de même pour les automates de paiement (tels les bornes de parking) dont le nombre de piratages s'élève à 10 (contre 18 cas en 2018). Enfin, aucune compromission de terminaux de paiement chez les commerçants n'a été constatée au cours des deux dernières années.

Quel que soit le type d'automates de paiement ou de retrait compromis, les données de carte de paiement ainsi obtenues par les réseaux criminels sont ensuite exploitées, soit pour contrefaire des cartes à piste magnétique qui seront utilisées pour des paiements et des retraits à l'étranger, principalement dans les pays où la technologie de carte à puce EMV (Europay Mastercard VISA) est peu déployée (pays d'Amérique ou d'Asie du Sud-Est notamment), soit pour usurper des numéros de carte en paiement à distance, qui sont réutilisés principalement sur les sites de e-commerce qui n'ont pas mis en œuvre l'authentification du porteur de la carte.

Nombre d'infractions constatées sur les distributeurs et terminaux (en unités)



Source : Observatoire de la sécurité des moyens de paiement.

3

ÉTUDE DE VEILLE TECHNOLOGIQUE SUR LA SÉCURITÉ DES DONNÉES DE PAIEMENT

Alors que le volume des paiements scripturaux est en constante augmentation, la multiplication des usages numériques et les promesses d'une expérience de paiement toujours plus fluide ont participé à la dissémination des données de paiement. De fait, les utilisateurs sont de plus en plus souvent invités à préenregistrer leurs données de paiement dans leur navigateur Internet, leur application mobile ou sur les sites marchands.

En parallèle, les chaînes de traitement des opérations de paiement font intervenir un nombre croissant d'intervenants. Cela est en partie dû à la numérisation des services (e-commerce, e-administration), mais c'est également lié au recours de plus en plus fréquent à l'externalisation notamment par les prestataires de services de paiement, qui délèguent tout ou partie du traitement des opérations de paiement à des prestataires techniques.

Enfin, alors que le paiement est une activité soumise à une forte concurrence, les acteurs de paiement cherchent de plus en plus à exploiter le potentiel des données de transactions pour proposer des services plus innovants et plus adaptés à leurs clients. C'est notamment le fait des nouveaux acteurs tels que les « fintech » ou les « Big Tech », qui ont placé le traitement des données de paiement au cœur de leur modèle d'affaires. Il s'agit par exemple des prestataires de service d'information sur les comptes et d'initiation de paiement, qui sont reconnus et encadrés par la deuxième directive européenne sur les services de paiement dite « DSP 2 ».

La dissémination des données de paiement auprès d'une multitude d'acteurs constitue donc une tendance structurante de l'industrie des paiements. Celle-ci concourt en retour à la recherche continue de vulnérabilités par les cyberfraudeurs. Dans ce contexte d'innovation et d'évolution rapide des modes de consommation, il s'agit d'évaluer les nouveaux risques portant sur la sécurité des données de paiement et d'identifier les bonnes pratiques permettant d'en assurer la protection tout au long de la chaîne de traitement.

3.1 De nouveaux risques pour la sécurité des données de paiement

3.1.1 Les données de paiement : de quoi parle-t-on ?

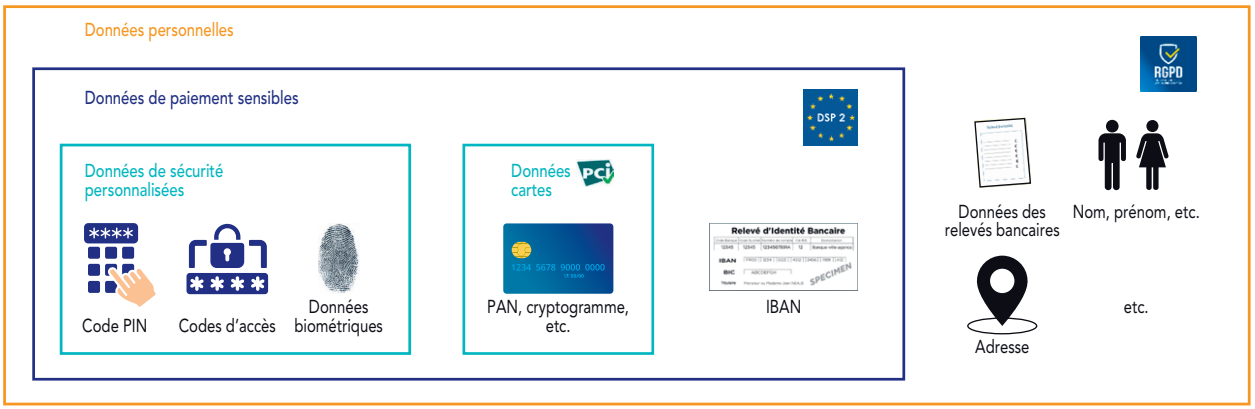
Les données de paiement peuvent répondre à plusieurs qualifications juridiques. En fonction de la nature de ces données, celles-ci peuvent être soit sensibles, soit personnelles, soit soumises au secret professionnel [1], soit protégées par le droit pénal, ou encore tout cela simultanément.

Les données de paiement sensibles sont des données « *susceptibles d'être utilisées pour commettre une fraude* » (article 4, paragraphe 32 de la DSP 2 [2]). Le numéro de compte bancaire, les données de la carte bancaire et plus généralement les données de sécurité personnalisées, c'est-à-dire « *les données fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification* » (article 4, paragraphe 31 de la DSP 2), comme les mots de passe ou le code PIN, appartiennent à cette catégorie. La protection des données de paiement sensibles est une condition nécessaire pour la sécurité des paiements et fait l'objet, via la mise en œuvre de la DSP 2, d'un ensemble d'exigences réglementaires. Il est notamment attendu du prestataire

1 Le secret professionnel, parfois appelé « secret bancaire », est applicable aux établissements de crédit au titre de l'article L. 511-33 du Code monétaire et financier.

2 Directive européenne 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

S1 Périmètre de protection des données de paiement par les textes réglementaires et les standards industriels



Note : DSP 2 : deuxième directive européenne sur les services de paiement ; RGPD : règlement général sur la protection des données ; PCI (*payment card industry*) : industrie des cartes de paiement ; PAN (*personnal account number*) : numéro de carte ; IBAN *(international bank account number)* : numéro de compte.

Source : Banque de France.

de service de paiement de prendre les mesures nécessaires pour « *protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur* » (article 1 du règlement délégué de l'Union européenne (UE) 2018/389 et articles 22 à 27).

Dès lors qu'elles peuvent être rattachées à une personne physique, les données dites « transactionnelles », par exemple celles qui figurent sur les relevés de compte ainsi que l'historique de ces données, entrent aussi dans la catégorie des données personnelles. Leur confidentialité et leur intégrité sont alors exigées par le règlement européen 2016/679, dit règlement général sur la protection des données (RGPD). Les responsables de traitement doivent en particulier assurer « *une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* » (RGPD, article 5.1, f).

Enfin, les données commerciales issues de la relation banque/client appartiennent à la catégorie des données des entreprises dont la protection peut être couverte par la loi n° 2018-670 en date du 30 juillet 2018 relative à la protection du secret des affaires, elle-même prise en transposition d'une directive européenne [3].

En conclusion, la sécurité des données de paiement est tenue par plusieurs exigences légales et réglementaires. À titre d'exemple, concrètement, les données monétiques, relatives à l'utilisation des cartes bancaires, sont successivement couvertes par les principes du RGPD, les exigences de la DSP 2 et les normes professionnelles (PCI-DSS – *payment card industry data security standard*, standard de sécurité des données pour l'industrie des cartes de paiement).

3.1.2 Quatre évolutions structurantes participent à la dissémination des données de paiement

La croissance des usages numériques couplée avec la hausse des cyber-risques

La révolution numérique suscite des changements majeurs dans les attentes des consommateurs concernant la manière et le moment où ils effectuent leurs achats (via de multiples terminaux, en déplacement, à toute heure de la journée). Ces évolutions sociologiques ont des impacts sur l'expérience de paiement chez les commerçants, dans la mesure où les consommateurs attendent davantage de simplicité et de rapidité dans l'exécution des opérations et de sécurité. Si les acteurs du e-commerce répondent à ces nouvelles attentes, leurs solutions nécessitent souvent en contrepartie de préenregistrer les données de paiement dans le navigateur, dans l'application mobile ou sur le site marchand. Le risque d'interception ou de récupération de ces données par des fraudeurs va de pair avec leur dissémination. La sécurité des données de paiement dépend ainsi de la qualité des dispositifs de protection tout au long de la chaîne de traitement des données de paiement sensibles, qui fait intervenir de plus en plus d'acteurs.

À l'augmentation du nombre de vulnérabilités potentielles correspond une augmentation des menaces. Malgré l'absence de chiffres fiables, les différentes sources existantes s'accordent sur l'augmentation du nombre des cyberattaques telles les *hacks* et les *ransomware* – faux logiciels de décodage et de protection. La diversité et la permanente évolution des techniques d'approche utilisées pour les cyberfraudeurs appellent l'attention. S'ils exploitent les vulnérabilités des systèmes d'information, les cyberfraudeurs réussissent aussi à transposer dans le monde numérique les pratiques anciennes de persuasion, voire de menaces sur les victimes pour récupérer des données sensibles.

Un nombre de plus en plus important d'acteurs dans la chaîne des paiements

Le développement de nouveaux usages de paiement (paiement *in-app*, sans contact, QR code, porte-monnaie électronique, paiement de particulier à particulier, *cash back,* etc.) a participé à l'émergence de nouveaux acteurs à tous les niveaux de la chaîne de valeur. Cette tendance a d'abord été poussée par l'essor du e-commerce et l'émergence d'acteurs proposant des porte-monnaie électroniques. Les détaillants (*retailers*) sont entrés plus récemment dans le secteur, afin d'accompagner leurs clients tout au long de leur parcours d'achat, et ce jusqu'à l'étape du paiement.

La démultiplication des prestataires de service de paiement a, en outre, été favorisée par des évolutions réglementaires. De nouveaux acteurs comme les établissements de paiement et les établissements de monnaie électronique ont été autorisés à fournir ces services aux côtés des banques à partir des années 2000. Les prestataires de service de paiement peuvent, de surcroît, mandater des acteurs tiers, les « agents » (article L. 523-1 du Code monétaire et financier). Ainsi, lorsque leur volume d'activité est encore restreint, beaucoup de nouveaux acteurs fintech préfèrent nouer un partenariat avec un prestataire de service de paiement déjà agréé plutôt que solliciter eux-mêmes un agrément.

En parallèle, les acteurs historiques des paiements font appel à un nombre important de prestataires techniques, auxquels ils délèguent des fonctions de plus en plus critiques. C'était historiquement le cas pour le développement et la maintenance des terminaux de paiement, des distributeurs automatiques ainsi que pour la fabrication et le renouvellement des cartes de paiement. Aujourd'hui, les prestataires interviennent également dans le traitement des opérations de paiement et dans les dispositifs de gestion des risques de fraude (prestataires d'acquisition techniques, serveurs d'autorisation, prestataires spécialisés dans la lutte contre la fraude).

La montée en puissance des nouveaux services et acteurs sous l'effet de la DSP 2

À partir des années 2010, des acteurs innovants ont proposé des services de consultation des comptes ou d'initiation de paiement sans être eux-mêmes teneurs de compte. Ces acteurs recueillaient les données de sécurité personnalisées des utilisateurs, avec leur consentement, pour récupérer, via des techniques dites de *screen scraping*, les informations accessibles sur leur espace de banque en ligne. Ces entreprises opéraient alors en dehors de tout cadre réglementaire. Depuis l'entrée en application de la DSP 2 en janvier 2018, ces activités sont autorisées et encadrées par les autorités de supervision du secteur financier.

Plus spécifiquement, la DSP 2 introduit deux nouveaux services de paiement : le service d'initiation de paiement et le service d'information sur les comptes. Les prestataires de services d'information sur les comptes recueillent et traitent les informations relatives aux comptes de paiement détenus par un client, particulier ou entreprise. Les prestataires de services d'initiation de paiement agissent comme un intermédiaire ayant la capacité d'initier pour le compte de l'utilisateur des paiements, le plus souvent des virements, depuis son espace de banque en ligne. Ils proposent leurs solutions de paiement aux commerçants et aux créanciers comme une alternative possible au paiement par carte ou par portefeuille électronique.

S'il est attendu que la montée en charge d'interfaces de communication sécurisées et dédiées (appelées « API », *application programming interface*, interface de programmation d'application) renforce progressivement la sécurité de ces activités, ces acteurs accèdent à de nombreuses données de paiement, y compris sensibles. Par ailleurs, ils nouent eux-mêmes des partenariats avec des acteurs tiers qui disposent déjà d'un agrément ou qu'ils mandatent comme agents, ce qui nourrit aussi la dissémination des données de paiement.

Un recours croissant à l'hébergement externe de données

Les acteurs du paiement intensifient leur recours aux services d'hébergement de type *cloud* (nuage) sur certaines parties de leurs activités. Les principaux avantages qu'ils identifient sont la flexibilité (l'architecture s'adapte plus facilement

3 Directive européenne 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

aux pics de charge), la mutualisation, la disponibilité, la réduction des coûts et la sûreté des données (application des meilleures pratiques en matière de sauvegarde). Il s'agit avant tout d'obtenir un accès relativement facile aux nouvelles technologies proposées par les fournisseurs de *cloud* et de réaliser des économies d'échelle.

Dans le but d'encadrer ces pratiques, l'Autorité bancaire européenne (ABE, *European Banking Authority* – EBA) a publié dans un premier temps des recommandations à destination des établissements financiers sur l'externalisation vers des « fournisseurs de services » en nuage en 2018 et dans un deuxième temps, une révision de ses lignes directrices (*guidelines* – GL) sur les contrats d'externalisation (EBA/GL/2019/02 applicables depuis le 30 septembre 2019), qui intègrent les premières. Celles-ci imposent la mise en place d'une véritable politique d'externalisation, y compris pour les externalisations intragroupe, avec la désignation d'une fonction dédiée. En effet, l'organe de direction de chaque institution financière reste responsable de son institution et de ses activités à tout moment. C'est-à-dire que l'organe de direction doit veiller à ce que des ressources suffisantes soient disponibles pour soutenir et assurer l'exercice de ces responsabilités en toutes circonstances. Les lignes directrices définissent aussi les critères permettant de déterminer si l'activité externalisée est critique ou importante. Au regard de ces critères, en règle générale, toute externalisation dont la défaillance viendrait mettre à mal la continuité des services de paiement, par exemple le traitement des données sensibles de paiement, doit être considérée comme une externalisation critique.

3.1.3 Des méthodes de plus en plus sophistiquées pour subtiliser les données de paiement sensibles

Les fraudeurs ont deux options principales pour récupérer les coordonnées et identifiants bancaires : ils peuvent déjouer la vigilance des systèmes de sécurité informatique ou déjouer celle des utilisateurs. Pour ce faire, le *phishing* (ou hameçonnage) et les logiciels malveillants (*malwares*) sont les techniques les plus fréquentes dans la mesure où elles permettent de cibler des milliers d'utilisateurs en même temps.

Le *phishing* est une technique de fraude qui a pour but de récupérer les données sensibles d'un agent économique (consommateur, entreprise, etc.). Celui-ci reçoit un courriel d'un émetteur se faisant passer pour un tiers de confiance (une banque, une institution publique, un prestataire de services, etc.) l'incitant fortement à cliquer sur un lien sous un faux prétexte (nouvelle campagne de mise à jour des coordonnées clientes, vérification d'informations personnelles, etc.). Le lien le conduit vers un site de *phishing* imitant le site officiel, où il est invité à entrer ses coordonnées bancaires ou autres données sensibles. En cas de *phishing* de carte bancaire, les fraudeurs s'efforcent de s'emparer directement de la carte bancaire du consommateur et du code PIN qui y est associé en prétextant le besoin de remplacer la carte actuelle *(cf. encadré 1 infra*).

Le *malware* désigne les logiciels nuisibles et dangereux, dont le but est d'être exécutés de façon quasi transparente sur les équipements connectés d'un utilisateur. Ceux-ci peuvent perturber le bon fonctionnement du système informatique (par exemple, redirection silencieuse vers un faux site qui invite soudainement à renseigner certains codes, sous le prétexte d'un contrôle de sécurité), espionner les activités de l'utilisateur à son insu et ainsi subtiliser des données.

Plusieurs millions de *malware*s sont recensés et ceux-ci peuvent être catégorisés en plusieurs familles. Celles qui permettent le vol de données proviennent principalement des virus (programmes frauduleux qui s'autoreproduisent en infectant d'autres programmes ou fichiers dont le format permet l'exécution de code), des chevaux de Troie ou *Trojan* (similaires aux virus, programmes pouvant détourner des informations à travers des accès qu'ils auront ouverts), les enregistreurs de touche ou *keyloggers* (programmes qui enregistrent toutes les frappes sur le clavier comme les identifiants et mots de passe dans un fichier) et les rançongiciels ou *ransomwares* (chevaux de Troie qui infectent l'équipement informatique, chiffrent les données de la victime et l'informent qu'elle doit payer une rançon pour récupérer ses données).

Le *phishing* et surtout les *malwares* sont des techniques en constante évolution pour déjouer les logiciels de sécurité. Le contenu des courriels de *phishing* cible plus efficacement la victime potentielle (message sans faute d'orthographe, personnalisation des messages) et les faux sites clonent à la perfection les sites originaux. Toutefois, les techniques plus « anciennes » n'ont pas disparu. C'est ainsi que la tromperie et le *skimming* reviennent en force à des fins de récupération de données de paiement sensibles :

- la tromperie où le fraudeur se fait par exemple passer pour une personne de confiance comme un représentant d'un service client bancaire ou des forces de l'ordre, et appelle le client pour obtenir ses identifiants bancaires sous de faux prétextes (contrôles de sécurité, remises tarifaires, obligations réglementaires, etc.) ;
- le *skimming* consiste à copier les données figurant sur la piste magnétique d'une carte de paiement au moment où le porteur introduit sa carte dans un distributeur automatique à l'aide d'un lecteur à mémoire appelé *skimmer* ou un terminal de paiement modifié.

3.2 Protéger les données de paiement sensibles

3.2.1 Les données de la carte

Les données associées aux cartes de paiement

La carte bancaire contient un certain nombres d'éléments de sécurité :

Au recto :

- une puce, répondant à la norme EMV (Europay Mastercard VISA) et qui permet en proximité, par un mécanisme de chiffrement, d'assurer un dialogue sécurisé avec les terminaux de paiement électroniques (TPE) ou les distributeurs et les guichets automatiques (DAB/GAB) ; en France, toutes les cartes sont équipées d'une telle puce,
- une séquence de chiffres souvent présente en relief sur la face avant,
- la date d'expiration,
- le nom du titulaire.

Au verso :

- un hologramme,
- un panneau de signature,
- une piste magnétique,
- un cryptogramme visuel, trois chiffres imprimés au dos de la carte à droite de la zone de signature ou quatre chiffres imprimés au recto de la carte.

Pour plus de précisions sur les dispositifs innovants de renforcement de la sécurité physique des cartes, *cf. encadré 2 infra*.

Les données de la carte ne doivent pas être communiquées sans raison valable et sans précaution. En effet, la carte contient des informations qui pourraient être réutilisées par un fraudeur pour réaliser des transactions, en particulier des transactions en ligne et à l'étranger. Les données strictement nécessaires à la réalisation d'un paiement et qui peuvent être légitimement demandées par un site marchand sont :

- le numéro de la carte,
- la date d'expiration,
- le cryptogramme visuel,
- les éventuelles données d'authentification forte vérifiées par l'établissement bancaire à chaque transaction.

Pour les paiements réalisés sur Internet, la protection des données échangées est assurée par des techniques de chiffrement permises par le navigateur Internet (sessions SSL *[secure sockets layer]* symbolisées par un cadenas apparaissant dans la barre d'adresse du navigateur Internet et par l'adresse du site commençant par « https » ; *cf. encadré 3 infra*).

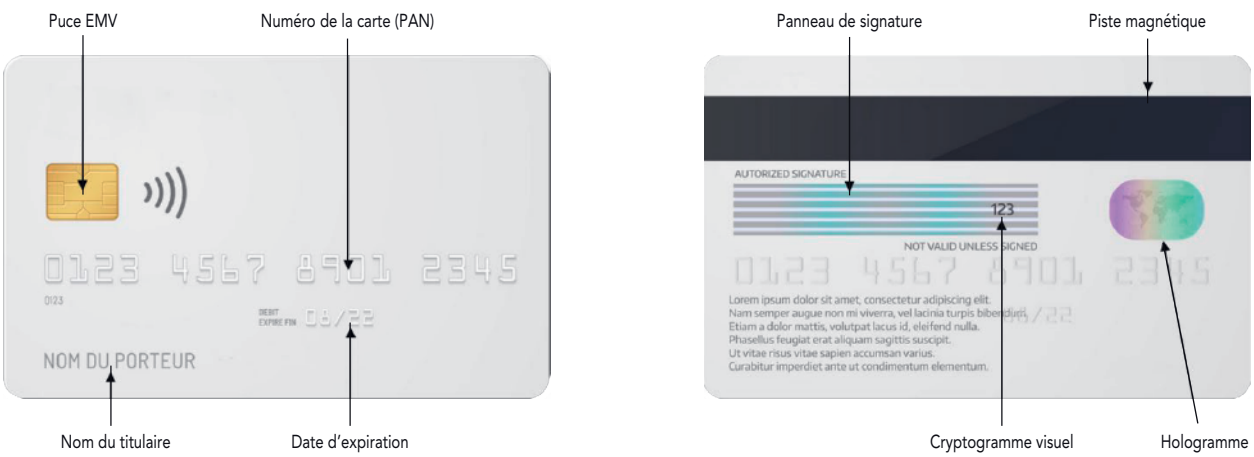
Les mesures de protection des données de carte

Pour répondre aux risques identifiés, les professionnels peuvent engager un certain nombre de mesures de sécurité.

L'application des normes de sécurité PCI-DSS *(payment card industry data security standard)*

Les normes PCI-DSS sont les normes de référence en matière de sécurité applicables aux données des cartes de paiement. Élaborées par le conseil des normes de sécurité PCI, elles visent à réduire l'utilisation frauduleuse des données des titulaires des cartes. Ce programme mondial, commun à Visa, MasterCard, American Express, Discover et JCB International, spécifie les dispositions de sécurité pour le stockage des données de cartes et les modalités d'audit.

S2 Les éléments de sécurité de la carte de paiement



Note : EMV, Europay Mastercard VISA ; PAN, *personnal account number*.

Source : Banque de France.

Les principales exigences portent sur la mise en place de pare-feux, la gestion de mots de passe, le chiffrement des données stockées, la gestion des historiques, des interdictions d'enregistrer certaines données utilisées lors de la transaction, la troncature des données spécifiques à un porteur affichées sur écran, les contrôles d'accès logiques et physiques. La dernière version des normes PCI-DSS (v3.2.1) est en vigueur depuis mai 2018.

Les données de titulaires de carte et les données d'identification sensibles sont définies dans le tableau 1.

Le programme PCI-DSS s'applique à tous les acteurs impliqués dans le traitement des cartes de paiement, et en particulier aux banques et aux autres prestataires de services de paiement. Dès lors qu'ils traitent des données « carte », il s'applique aussi aux commerçants et aux prestataires de service des banques et des commerçants, selon plusieurs niveaux d'audit.

Il existe d'autres normes de sécurité édictées par PCI, comme les exigences de sécurité relatives aux transactions par code PIN (appelées PCI PTS pour « *PIN transaction security* ») qui sont axées sur les caractéristiques et la gestion des périphériques et terminaux utilisés dans la protection des codes confidentiels. Les fabricants doivent respecter ces exigences lors de la conception, de la fabrication et du transport de l'équipement.

Les processus de « tokenisation »

La « tokenisation » est une méthode de sécurisation qui consiste à remplacer une donnée sensible par une valeur de substitution, appelé jeton ou *token*, dans la chaîne de paiement. Les *tokens* utilisés dans le domaine des paiements sont généralement des identifiants numériques uniques qui conservent le format de la donnée d'origine, telle qu'un PAN, ce qui permet de protéger une donnée sensible sans nécessiter d'adaptation particulière de la part des autres acteurs de la chaîne. Ce procédé technique s'appuie généralement sur un service centralisé qui contrôle l'utilisation restreinte de chaque *token* qui peut être unique ou propre à un canal d'initiation.

La « tokenisation » peut être mise en œuvre sur la base d'une solution propriétaire ou en suivant le standard international PCI *tokenisation security guidelines* qui définit les exigences de sécurité pour la gestion des *tokens* pour les cartes de paiement. À ce titre, plusieurs types de *tokens* sont définis pour les cartes de paiement ci-après.

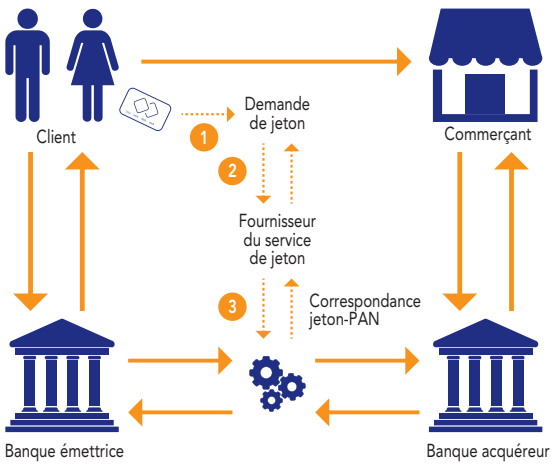
- Les *tokens* de sécurité, également appelés jetons acquéreurs sont utilisés pour protéger les PAN lorsqu'ils sont stockés dans les systèmes d'information servant à l'acquisition des flux de paiement. Ce jeton est propriétaire et ne prend pas la forme d'un PAN. Par exemple, un site de e-commerce peut détenir un jeton de sécurité qui peut servir à initier une transaction de type « paiement récurrent » relatif à un abonnement ou à un paiement fractionné.
- Les *tokens* de paiement, qui correspondent à la « tokenisation » d'un PAN, sont utilisés dans certaines solutions de paiement, en particulier les solutions de paiement mobile et les portefeuilles électroniques proposés pour le e-commerce.

T1 Données de compte

Les données du titulaire de carte comprennent :	Les données d'identification sensibles comprennent :
• Numéro de compte primaire (PAN) • Nom du titulaire de la carte • Date d'expiration • Code service	• Données de bande magnétique complètes (données de bande magnétique ou équivalent sur une puce) • CAV2/CVC2/CVV2/CID • Codes/blocs PIN

Note : CAV2 : *card authentication value 2* (par JCB International) ; CVC2 : *card validation code 2* (par MasterCard et Eurocard) ; CVV2 : *card validation value 2* (par Visa et Diners Club) ; CID : *card identification* (par Discover et American Express).
Source : Banque de France.

S3 Le fonctionnement de la « tokenisation » pour les paiements par carte



Note : PAN (*personnal account number*) : numéro de carte.
Source : Banque de France.

3.2.2 L'IBAN

Les virements et les prélèvements s'appuient sur l'utilisation du numéro d'identification des comptes bancaires, ou IBAN (*international bank account number*), qui sert à définir dans les ordres de paiement les comptes à créditer et à débiter. Avec le passage aux instruments SEPA (*Single Euro Payments Area*) en 2014, l'IBAN est devenu la donnée centrale pour l'émission de virements et de prélèvements, tant pour les opérations nationales que pour les opérations transfrontalières.

Pour les comptes tenus en France, l'IBAN est constitué de 27 caractères, commençant par le code pays FR (France) suivi de 2 caractères formant une première clé puis des 23 chiffres de l'ancien relevé bancaire français utilisé avant la migration SEPA (code de l'établissement bancaire, code du guichet, numéro de compte et clé RIB – relevé d'identité bancaire). L'IBAN est toutefois de taille variable selon les pays, et peut contenir jusqu'à 34 caractères :

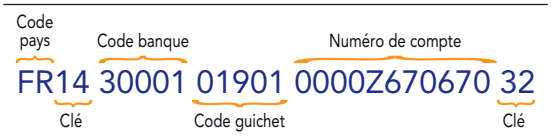
Les risques de fraude liés à la communication des IBAN

L'IBAN est considéré en France comme une donnée pouvant faire l'objet de détournements frauduleux. En particulier, deux modes opératoires s'appuient sur l'utilisation d'IBAN détournés pour réaliser des prélèvements frauduleux.

- Acheteur frauduleux : un fraudeur peut remplir un mandat de prélèvement avec un IBAN usurpé. On parle alors d'usurpation d'IBAN pour la souscription d'un service. Cette fraude s'intègre souvent dans des schémas d'usurpation d'identité.
- Créancier frauduleux : un fraudeur se fait enregistrer en tant que créancier par une banque et demande un identifiant de créancier SEPA (ICS), qui lui permet ensuite d'initier des prélèvements illégitimes sur la base d'IBAN collectés frauduleusement. Dans ce type de montage, le fraudeur transfère les fonds reçus le plus tôt possible afin d'éviter que les flux ne soient restitués à la suite de réclamations ou des plaintes des victimes. On parle alors d'émission illégitime d'ordres de prélèvement.

L'IBAN est également une donnée sensible, parce que le changement illégitime d'IBAN peut donner lieu à des virements frauduleux. En effet, un volume important de virements provient de l'activité des entreprises. Ces ordres sont principalement générés à partir d'IBAN enregistrés dans leurs bases de données et leurs logiciels. Une faiblesse dans la sécurité d'une base de données peut permettre à un fraudeur de substituer un ou plusieurs IBAN légitimes par les IBAN de comptes qu'il maîtrise (accessibles par lui ou des complices). De cette manière, les virements seront détournés au profit des comptes du fraudeur.

Composition du code IBAN



De façon plus classique, les entreprises peuvent aussi être jointes par courriel ou téléphone par des fraudeurs se faisant passer pour un de leurs fournisseurs, qui leur demandent d'enregistrer un nouvel IBAN dans leur base. C'est la « fraude au faux fournisseur ». Ainsi, les virements exécutés en règlement des factures dudit fournisseur sont détournés au profit du nouvel IBAN. La vigilance des entreprises est ainsi requise lorsqu'un changement d'IBAN est sollicité par une tierce personne. De nouveaux prestataires proposent des solutions de sécurisation des IBAN afin de vérifier qu'un IBAN est bien associé à l'entreprise qui doit être créditée.

Les mesures de protection associées à la conservation et à la communication des IBAN

Contrairement au domaine des cartes de paiement, il n'existe pas à ce jour de certification *ad hoc* visant à garantir un niveau de sécurité cible du stockage des IBAN, des ordres de virement et des données de connexion à la banque en ligne. Cependant, plusieurs mesures de sécurité peuvent être adoptées, notamment par les professionnels.

En entreprise, les ordres de paiement sont couramment gérés par des logiciels spécialisés. Il est recommandé de recourir à des logiciels qui assurent une protection forte de la confidentialité et de l'intégrité des IBAN, par exemple en les masquant partiellement dès lors que la connaissance complète de la donnée n'est pas nécessaire. Ces logiciels peuvent aussi embarquer des modules de détection des virements suspects qui sont utiles dans la prévention de la fraude. Enfin, il est recommandé de mettre régulièrement à jour ces logiciels et de contrôler étroitement les droits d'accès.

En complément, les entreprises et les établissements teneurs de compte sont invités à porter une attention particulière à leurs règles de communication des IBAN, afin d'éviter toute exposition inutile (par exemple, dans les conditions générales de vente, dans les signatures professionnelles, dans le papier à en-tête, dans les bons de commande, etc.). Quand cela est opportun en matière de volumétrie et de coût, les entreprises peuvent également se prémunir du risque de fraude en disposant de comptes dédiés à certains usages (par exemple, compte dédié aux paiements par chèque rejetant tout autre moyen de paiement, compte dédié aux prélèvements clientèle, etc.).

Enfin, il peut être envisagé de faire appel à un mécanisme déjà utilisé dans le cadre de la protection des numéros de cartes de paiement, appelé « tokenisation ». Ce procédé consiste à utiliser, dans un contexte défini (un type d'opérations, un canal d'initiation, une opération unique ou dans un délai limité), un alias en lieu et place de l'IBAN. Ainsi, l'alias présent dans un message intercepté ne pourra pas être exploité par le fraudeur. Un établissement français a mis en œuvre cette technique de « tokenisation » des IBAN dans le cadre d'un service interbancaire (*cf. encadrés 4 et 5 infra*).

3.2.3 Les données d'accès aux espaces de banque en ligne ou mobile

La grande majorité des établissements bancaires propose un espace de banque en ligne, disponible sous forme d'un site web et d'une application mobile. L'accès à ces interfaces s'appuie sur les identifiants personnels délivrés par l'établissement à son client, généralement sous la forme d'un identifiant et d'un code confidentiel. Ces données sont qualifiées de données de paiement sensibles, dans la mesure où elles permettent l'accès à des fonctionnalités de paiement : émission de virement, ajout d'un bénéficiaire, gestion d'une carte de paiement ou modification de ses plafonds d'utilisation, etc.

Au-delà des actions de sensibilisation réalisées par les établissements financiers, plusieurs dispositifs soutiennent la sécurité des données d'accès aux espaces de banque en ligne et mobile.

- La DSP 2 dispose que la connexion entre le terminal de l'utilisateur et le système d'information de l'établissement doit être sécurisée à l'aide de protocoles de communication sécurisés (en règle générale, il s'agit du protocole SSL) et, lorsque cela est possible, que les messages d'échanges soient signés électroniquement par des certificats qualifiés. Pour l'utilisateur, cela se traduit notamment par l'affichage d'un cadenas dans la barre d'état de son navigateur.
- L'établissement peut aussi recourir à un clavier de saisie virtuel pour la saisie du code confidentiel, ce qui permet de réduire le risque d'interception des données.
- Sur mobile, l'accès peut s'effectuer par recours aux capteurs biométriques présents sur le terminal de l'utilisateur, qui se substituent alors à la saisie du code confidentiel.

Enfin, la DSP 2 dispose que l'accès aux comptes de paiement soit protégé par une authentification forte de l'utilisateur au moins tous les quatre-vingt-dix jours, soit le recours à deux facteurs d'authentification de natures différentes. Si la clientèle des entreprises est généralement équipée de dispositifs d'authentification forte pour accéder à leurs comptes, ceci est moins vérifié pour la clientèle des particuliers. De fait, les codes de banque en ligne ne constituent qu'un seul facteur d'authentification dit « de connaissance », qu'il convient donc de compléter par un facteur « de possession » (par exemple par enrôlement du terminal utilisé par le client ou par recours à un matériel physique qui lui a été confié) ou « d'inhérence » (capteur biométrique). L'authentification forte est également requise pour toute opération sensible, c'est-à-dire présentant un risque de fraude, réalisée depuis l'espace de banque en ligne ou mobile, telle que l'ajout d'un bénéficiaire ou l'émission d'un virement vers un nouveau bénéficiaire (*cf. encadré 6 infra*).

3.3 De nouveaux « maillons » pour la sécurité des données de paiement : les prestataires de services d'information sur les comptes et les prestataires d'initiation de paiement

3.3.1 Les conditions d'exercice de ces nouveaux prestataires

Les prestataires tiers : les prestataires de service d'information sur les comptes (PSIC), aussi appelés agrégateurs d'informations sur les comptes, et les prestataires de service d'initiation de paiement (PSIP)

Depuis janvier 2018, la fourniture de services d'initiation de paiement ou d'information sur les comptes est soumise à l'approbation de l'autorité de supervision compétente : en France, cette mission est confiée à l'Autorité de contrôle prudentiel et de résolution (ACPR) et à la Banque de France en ce qui concerne l'analyse *a priori* du respect des exigences de sécurité applicables aux services de paiement envisagés.

Au-delà des aspects sécuritaires, agrégateurs d'informations et initiateurs de paiement doivent se conformer vis-à-vis de l'ACPR à des exigences prudentielles, quoique limitées puisque ces établissements n'entrent pas en possession de fonds. Ils sont également tenus de souscrire à une assurance en responsabilité professionnelle, du fait par exemple des risques de cybersécurité.

Il est à noter que les services d'initiation de paiement et d'information sur les comptes peuvent également être fournis par les établissements de crédit, mais aussi par les établissements de paiement et de monnaie électronique. Enfin, les établissements agréés pour ces services de paiement par un autre pays membre de l'Union européenne sont également habilités à exercer leurs activités en France : c'est le principe de la libre prestation de services ou plus communément du « passeport financier européen ».

Les établissements agréés par l'ACPR pour fournir ces services sont répertoriés dans le Registre des agents financiers (Regafi), accessible via l'adresse Internet *https://www.regafi.fr*. L'ACPR a entrepris une modernisation du registre Regafi et mettra en production prochainement une interface programmable de consultation. Par ailleurs, l'Autorité bancaire européenne (ABE) consolide les registres des différentes autorités nationales, ce qui permet également d'identifier les prestataires de services de paiement agissant sous le régime du passeport européen [4].

Les interfaces sécurisées

Pour pouvoir proposer des services financiers innovants, les prestataires tiers doivent avoir accès aux données bancaires de leurs clients. En absence d'un système d'échange d'informations standardisé, les acteurs tiers avaient recours à la technique dite du *screen scraping* qui consiste à demander au client de partager ses données d'authentification et ensuite à extraire les informations directement depuis la page web du portail bancaire. Cette technique, bien que fonctionnelle, pose des problèmes de sécurité dans la mesure où elle suppose que l'utilisateur confie ses données d'authentification – réputées personnelles – à des prestataires tiers.

La DSP 2, notamment via son règlement délégué (UE) 2018/398 communément appelé « RTS sécurité » (*regulatory technical standards* – RTS), a sensiblement renforcé les exigences de sécurité pour la communication entre les établissements gestionnaires de compte et les prestataires tiers. Le RTS sécurité encourage notamment la mise en place d'une interface de communication dédiée (« API », *application programming interface*) par les établissements gestionnaires de compte permettant aux différents prestataires tiers d'accéder aux données de leurs clients afin de sécuriser les échanges de données et d'endiguer l'usage du *screen scraping*. Pour accéder et utiliser ces interfaces, les prestataires tiers doivent présenter un certificat qualifié, une sorte de « carte d'identité » qui est délivrée par des prestataires de services de confiance (PSCo ou QTSP – *Qualified Trust Service Provider*) au sens du règlement européen eIDAS (*electronic identification and trust services*) [5].

Les chaînes de traitement des données (relation entre les prestataires et leurs agents)

Les prestataires tiers, notamment les prestataires de services d'informations sur les comptes, concluent souvent des partenariats avec des entreprises, qui sont intéressées par l'exploitation des données bancaires pour proposer des services innovants (comptabilité, conseil financier, simplification des démarches administratives, etc.). Ce sont ces entreprises qui ont alors une interaction directe avec l'utilisateur final, tandis que le prestataire tiers assure essentiellement la collecte et la transmission des données. Ces entreprises partenaires peuvent bénéficier d'une autorisation d'établissement financier et elles utilisent alors le prestataire tiers comme un prestataire technique. Si elles ne bénéficient pas d'une autorisation comme établissement financier, elles peuvent aussi être mandatées comme agent du prestataire tiers au sens de l'article L. 523-1 du Code monétaire et financier.

Selon les partenariats, le prestataire tiers peut être alternativement responsable de traitement ou sous-traitant au sens du RGPD. Lorsqu'il est responsable de traitement, le prestataire tiers doit [6] :

- définir les finalités et les moyens mis en œuvre pour le traitement des données personnelles, y compris lorsque le traitement est exécuté par des sous-traitants ;
- veiller au respect des principes qui sous-tendent la protection des données à caractère personnel : licéité [7], loyauté et transparence des traitements, collecte des données limitée aux finalités déterminées, minimisation quantitative des données, exactitude des données, limitation de la conservation et garantie d'intégrité et de confidentialité ;
- être en capacité de prouver que les traitements effectués répondent à ces exigences.

Toutefois, lorsque le prestataire tiers mandate son partenaire comme agent, ce dernier agit sous la responsabilité du prestataire tiers conformément à l'article L. 523-3 du Code monétaire et financier. Dans ce cas, le prestataire tiers doit s'assurer que ses dispositifs de contrôle interne en matière de sécurité des données de paiement couvrent



4 Le registre de l'Autorité bancaire européenne est accessible à partir du lien suivant : *https://eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2*

5 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.Pour en savoir plus, cf. : *https://www.ssi.gouv.fr*

6 Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

7 Article 6 du règlement général sur la protection des données (RGPD).

les agents qu'il a mandatés. Il appartient notamment au prestataire tiers de bien répercuter dans ses relations contractuelles les exigences en matière de sécurité des données de paiement et de prévoir les outils d'évaluation et de contrôle de ses agents.

L'authentification des utilisateurs auprès des prestataires tiers

Les utilisateurs réalisent une authentification forte auprès des prestataires de services de paiement (PSP) gestionnaires de comptes lorsqu'ils ont recours aux services d'un PSP tiers. En revanche, il n'existe aucune exigence ou recommandation de la DSP 2 en ce qui concerne l'authentification des utilisateurs (particuliers ou entreprises) auprès des prestataires tiers, c'est-à-dire lorsque ceux-ci utilisent l'application mobile ou le site web du PSP tiers. Certains PSP tiers toutefois ont fait le choix d'appliquer l'authentification forte à toute connexion à leur application mobile ou à leur site web. Afin d'assurer une sécurité optimale de bout en bout, l'Observatoire recommande aux PSP tiers ainsi qu'à leurs agents d'appliquer autant que possible une procédure d'authentification forte de leurs utilisateurs. Ces mesures peuvent être utilement complétées par des dispositifs de détection des connexions suspectes (connexion à partir d'un nouveau terminal, lieu et horaire inhabituel de connexion, etc.).

3.3.2 La protection des données sensibles de paiement par les prestataires tiers

Les identifiants et mots de passe (*screen scraping*)

Certains établissements gestionnaires de comptes ont fait le choix, à la date butoir fixée par la DSP 2, de ne pas mettre en place une interface dédiée pour l'accès aux comptes bancaires, telle que définie par la DSP 2, ou retardent son déploiement. Dans ce contexte, moyennant une identification par certificat qualifié à la connexion, les PSP tiers conservent la solution technique de *screen scraping* pour accéder aux comptes bancaires.

La solution technique de screen scraping implique le stockage des données d'authentification dans le système d'information des prestataires tiers. La Commission nationale de l'informatique et des libertés (CNIL) recommande que le mot de passe ne soit jamais stocké en clair et, lorsque cela est techniquement faisable, que le mot de passe soit transformé au moyen d'une fonction cryptographique non réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé [8]. L'Observatoire préconise aussi l'utilisation de modules de sécurité matériels (HSM – *hardware security module*) pour la protection des données de sécurité personnalisées recueillies par les prestataires tiers.

Les IBAN

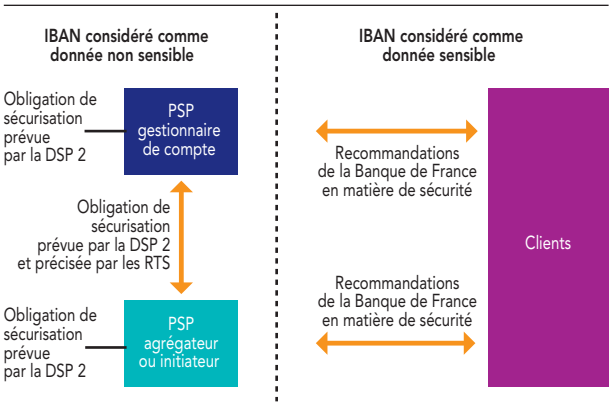
La DSP 2 dispose que l'IBAN et le nom du titulaire du compte ne sont pas considérés comme une donnée de paiement sensible en ce qui concerne l'activité des prestataires tiers (article 4, paragraphe 32, de la DSP 2). Cette disposition se justifie par le fait que la communication de ces données peut être nécessaire à la fourniture des services d'information sur les comptes et d'initiation de paiement. En dehors de ces cas d'utilisation bien définis par la DSP 2 et au regard des risques de fraude via du prélèvement et du virement, la Banque de France recommande la considération de l'IBAN comme une donnée sensible de paiement. Au final, si la DSP 2 encadre strictement l'utilisation des IBAN par les prestataires de services de paiement, différents cas sont à distinguer (*cf. schéma 4*).

L'Observatoire préconise ainsi la mise en place de dispositifs sécurisés similaires à ceux requis pour les données de carte (normes PCI DSS) pour la conservation des IBAN dans les systèmes d'information des PSP, ainsi que le recours à des canaux de communication sécurisés dans les échanges de cette information avec leurs clients.

Les autres données sensibles (adresse, numéro de téléphone, etc.)

Les données telles que les adresses ou les numéros de téléphone sont des données personnelles qui peuvent être collectées par les prestataires tiers lors de la phase d'enrôlement de leurs utilisateurs. Ces données sont également sensibles car elles peuvent servir aux fraudeurs pour préparer leurs attaques.

S4 Dans quels cas faut-il considérer l'IBAN comme une donnée de paiement sensible au regard de la DSP 2 ?



Note : IBAN : *international bank account number*; DSP 2 : deuxième directive européenne sur les services de paiement ; RTS : *regulatory technical standards*; PSP : prestataire de services de paiement.

Source : Banque de France.

Le RGPD dispose que les systèmes d'information recueillant des données personnelles doivent être sécurisés afin d'éviter que ces données soient piratées, endommagées ou bien qu'une tierce personne non autorisée y ait accès. Elle dispose également une durée de conversation maximale de trente-six mois des données personnelles des utilisateurs inactifs.

Afin de respecter ces exigences, lorsque cela est techniquement faisable, l'Observatoire recommande la mise en place de mécanisme de chiffrement de ces données en stockage et lors des transferts de données (dans un fonctionnement dégradé, la pseudonymisation [9] est une technique alternative valable) et la suppression ou l'anonymisation des données personnelles collectées à l'expiration de leur durée de conservation.

3.4 Mesures de sécurité recommandées par l'Observatoire

L'Observatoire renouvelle les recommandations émises dans son rapport annuel 2018 concernant la mise en place de mécanismes fiables pour le stockage sécurisé des informations confidentielles dans les systèmes d'informations des prestataires de services de paiement, ainsi que par extension, dans les applications mobiles mises à la disposition de leurs utilisateurs. Ces recommandations recouvrent aussi bien les données sensibles de paiement (données de carte, IBAN, identifiants personnels, etc.) et les données d'authentification (notamment les facteurs biométriques utilisés dans le cadre des services de paiement sur mobile), que les données personnelles (adresse, environnement familial, etc.) qui sont utilisées par les fraudeurs en vue de mieux préparer et conduire leurs attaques. En outre, les professionnels sont encouragés à minimiser autant que possible la détention de données confidentielles ou personnelles et la durée de leur conservation.

L'Observatoire invite les prestataires de services de paiement ainsi que leurs agents à 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 de leurs utilisateurs pour l'accès à leurs services et à toute donnée sensible. Ces mesures doivent être complétées par des dispositifs de détection des connexions suspectes. Par ailleurs, l'Observatoire rappelle aux prestataires de services de paiement qu'il est de leur responsabilité de contrôler régulièrement l'application des mesures de sécurité, y compris par leurs prestataires techniques et agents, et d'en mesurer l'efficacité au regard des risques identifiés.

Enfin, l'Observatoire rappelle le rôle essentiel joué par les utilisateurs dans la sécurité des paiements, et les invite par conséquent à respecter les principes de prudence établis en matière de protection de leurs données sensibles :

- 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 ;
- saisir des données bancaires exclusivement sur des sites Internet ou des applications mobiles réputés fiables et de confiance ; à cet égard, les utilisateurs sont invités à privilégier les sites et applications référencés et à 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 ;
- dans le cas particulier de l'accès aux services de paiement, n'utiliser que des applications de confiance, notamment celles publiées par leur fournisseur de services de paiement ou dont le fournisseur est dûment autorisé en France pour la prestation de services de paiement (c'est-à-dire présent dans l'annuaire Regafi ou dans le registre de l'Autorité bancaire européenne) ;
- s'informer régulièrement sur les risques numériques et leurs évolutions via, par exemple, le site du gouvernement *www.cybermalveillance.gouv.fr*

8 Cf. *https://www.cnil.fr*

9 La pseudonymisation consiste à scinder de manière réversible les données identifiantes des autres, en utilisant comme pivot des pseudonymes non explicites (par exemple des chaînes de caractères aléatoires) pour faire la correspondance. Cela permet de limiter l'exposition à des données non identifiantes ou quasi-identifiantes.

❽ La nouvelle plateforme Thésée de déclaration des escroqueries aux moyens de communication

L'activité de la plateforme téléphonique info Escroqueries a connu une augmentation de 25 % en 2017 par rapport à 2016. Sur 28 287 appels reçus, 65 % d'entre eux portaient sur des escroqueries commises sur Internet. L'isolement des plaintes des usagers rend difficiles les possibilités de recoupement et affaiblit l'efficacité des investigations techniques.

En réponse à ce constat, la police judiciaire a dévoilé lors du dixième forum international de la cybersécurité une nouvelle plateforme baptisée Thésée, pour le traitement harmonisé des enquêtes et des signalements pour les e-escroqueries. Il s'agit de permettre aux usagers de déposer une plainte ou un signalement en ligne sans avoir à se déplacer dans un commissariat ou une brigade de gendarmerie. Quelques renseignements seront demandés et des questions posées, puis le procès-verbal sera généré automatiquement. À l'autre bout de la chaîne, chaque plainte sera ensuite analysée par un service de police dédié et spécialisé qui fera les premières vérifications et des recoupements avec d'autres plaintes puis saisira la justice pour retrouver les auteurs de l'escroquerie.

Le projet Thésée devrait également inciter un plus grand nombre de victimes à porter plainte. En effet, actuellement, de nombreux utilisateurs se font escroquer et peu osent porter plainte.

Liste des infractions permettant la plainte ou le signalement en ligne :

- piratage de messagerie électronique (courriel, profil, réseau social, etc.),
- chantage en ligne (menaces portant atteinte à l'honneur contre demande d'argent),
- rançongiciel (demande de rançon pour débloquer un ordinateur),
- escroquerie à la romance ou « romance scam » (l'escroc, sous une fausse identité, gagne l'affection d'une personne afin de lui soutirer de l'argent),
- escroquerie à la petite annonce,
- fraude liée aux faux sites de ventes.

Toutes ces infractions ne relèvent pas de la fraude aux moyens de paiement, mais le signalement sur la plateforme Thésée de toute récupération frauduleuse de données de paiement sensibles – on peut notamment penser aux piratages et aux faux sites de vente –, aidera l'action des forces de l'ordre et de la justice dans leur lutte contre la cybercriminalité. La plateforme Thésée complète ainsi la plateforme Perceval (plateforme électronique de recueil de coordonnées bancaires et de leurs conditions d'emploi rapportées par les victimes d'achats frauduleux en ligne) dédiée spécifiquement aux fraudes à la carte bancaire. Enfin, le gouvernement propose le site *www.cybermalveillance.gouv.fr* pour sensibiliser aux risques numériques, fournir de bonnes pratiques à destination des particuliers et des professionnels et assister les victimes d'actes de cybermalveillance.

❾ Les dispositifs innovants de renforcement de la sécurité physique des cartes

Pour les paiements en ligne : la carte à cryptogramme visuel dynamique

Ce type de carte dispose d'un écran à encre électronique alimenté par une batterie miniature d'une durée de vie supérieure à celle de la carte. Cet écran affiche un cryptogramme à validité temporaire, renouvelé selon une fréquence prédéfinie par l'établissement. Ce dispositif permet de réduire efficacement les risques de fraude à la carte sur Internet, dans la mesure où les données volées ou copiées deviennent rapidement obsolètes.

Pour les paiements en ligne : la carte virtuelle

Pour effectuer un achat en ligne, certains établissements proposent à leurs clients de générer une carte virtuelle qui dispose des paramètres habituels d'une carte (numéro, date de validité, cryptogramme), mais dont l'utilisation est plafonnée au montant des transactions souhaitées par le client. Le risque de fraude est ainsi diminué par la durée de vie limitée des données de la carte.

Pour le paiement de proximité : la carte de paiement biométrique

La carte bancaire biométrique est dotée d'un lecteur d'empreinte digitale directement sur la carte, qui permet, en plaçant son doigt sur la zone dédiée, de valider une transaction sur un terminal de paiement en mode sans contact, y compris pour des montants supérieurs au plafond autorisé pour ce mode de paiement. Le code PIN peut toujours être utilisé pour le retrait d'espèces dans un distributeur automatique. Les premiers tests de cette technologie sont en cours sur le marché français, et sa commercialisation devrait intervenir progressivement.

❿ Que faire en cas de fraude à la carte de paiement ?

1. Faire opposition à sa carte de paiement auprès de l'établissement émetteur.

2. Signaler une fraude à la carte bancaire via la plateforme Perceval, accessible depuis le site *www.Service-Public.fr*

3. Poursuivre les démarches de remboursement auprès de ma banque.

Lorsque le titulaire d'un compte constate qu'une opération de paiement qu'il n'a pas autorisée est débitée sur son compte, il doit en informer sans tarder son établissement teneur de compte, et au plus tard dans un délai de treize mois à compter de la date du débit. Il doit être remboursé par son établissement teneur de compte au plus tard à la fin du jour ouvré suivant la notification (article L. 133-18 du Code monétaire et financier). Toutefois, si l'établissement a de bonnes raisons de soupçonner une fraude de l'utilisateur ou une négligence grave de sa part, il peut effectuer certaines vérifications avant de rembourser ou non le payeur. Dans ce cas, l'établissement doit alors notifier à la Banque de France les raisons pour lesquelles il ne rembourse pas immédiatement.

⓫ L'utilisation d'alias : une forme de « tokenisation » de l'IBAN à des fins d'ergonomie

Un des principaux défauts de l'IBAN dans son utilisation au quotidien par les particuliers comme par les entreprises réside dans sa complexité. De fait, contrairement à un identifiant bancaire, l'IBAN est rarement connu des détenteurs de compte, ce qui limite de fait son utilisation, notamment pour des paiements entre personnes.

Les travaux français conduits en soutien au développement du virement instantané ont abouti à la constitution de services d'indexation associant à l'IBAN d'un utilisateur un identifiant numérique simple, tel que son numéro de téléphone ou son adresse électronique. Ce service permet d'initier un virement au moyen du seul numéro de téléphone du bénéficiaire, permettant une ergonomie optimale.

Devant le risque d'un cloisonnement des utilisateurs (chacun n'étant accessible que dans les solutions dans lesquelles il est référencé) et afin de promouvoir une utilisation paneuropéenne des solutions de virement instantané (les solutions existantes étant en grande majorité des solutions propres à chaque pays), le Conseil européen des paiements (*European payment council* – EPC) a mis en place un service de référencement dit SEPA *proxy lookup* (SPL) qui vise à assurer l'interopérabilité, de manière sécurisée, entre les services d'indexation existants.

Via ce service, les utilisateurs pourront à terme utiliser leur appareil mobile pour transférer de l'argent de leur compte bancaire vers le compte d'une autre personne, en Europe, sans échanger manuellement des informations de paiement, telles que l'IBAN. Cette méthode rend le processus de paiement beaucoup plus simple, plus sûr et moins sujet aux erreurs. Cela appelle en contrepartie des mesures de sécurité appropriées des bases de données assurant l'indexation des IBAN.



⓬

Le projet européen OBSIDIAN de partage d'information sur les IBAN comme moyen de lutte contre la fraude

L'absence de partage des IBAN, tant au niveau national qu'européen, pose un problème dans la lutte contre la fraude sur les prélèvements et les virements. Ainsi le manque de communication entre les banques permet au fraudeur de reproduire le même mode opératoire dans des établissements différents sans être réellement inquiété.

Dans ce cadre, le projet OBSIDIAN (*Open banking sensitive data and information sharing network*), porté par la direction générale des réseaux de communication de la Commission européenne, est un projet européen qui vise à étudier la problématique de communication des IBAN frauduleux sous la forme d'un réseau de partage entre établissements bancaires. Il a pour but de favoriser la lutte contre la fraude entre acteurs de paiement et répondre aux enjeux européens de sécurité, de souveraineté et de compétitivité. Ce projet s'articule avec deux grandes démarches conduites par l'Union européenne :

- la stratégie européenne d'investissement en matière d'innovation et de sécurité dans le cadre de la mise en place du Marché unique du numérique [1] ;
- le programme CyberSec4Europe [2], qui a pour objectif de créer un réseau européen et un centre de compétence pour conserver et développer les capacités technologiques et industrielles en matière de cybersécurité.

Les constats à l'origine du lancement du projet sont les suivants :

- le manque de partage d'information entre acteurs de paiement européens affecte considérablement l'efficacité globale du dispositif de maîtrise du risque de fraude ;
- les scénarios d'attaque des fraudeurs évoluent vers des pratiques « en ligne », impliquant plusieurs pays en s'adaptant au contexte DSP 2 ;
- une partie des moyens traditionnels de lutte contre la fraude s'accommodent mal d'une offre digitale en pleine expansion qui impose simplicité, agilité et instantanéité ;
- le nouveau cadre légal proposé par le règlement général sur la protection des données (RGPD) offre une opportunité de réorganiser les moyens de lutte contre la fraude.

La France, avec le concours d'acteurs bancaires européens, collabore pour concevoir de nouveaux outils qui permettraient, par une circulation efficace de l'information sur la fraude entre acteurs des paiements, de mieux protéger les citoyens européens et d'adapter la maîtrise du risque de fraude à la transformation numérique du secteur financier.

1 Marché unique du numérique ou *digital single market*, cf. : *https://ec.europa.eu/digital-single-market/en*

2 Cf. : *https://cybersec4europe.eu/*

⓭

Utilisation d'un smartphone : restez vigilant

Les opérations courantes (consultation, virement, etc.) de banque en ligne sont réalisées de plus en plus fréquemment sur smartphone. Restez vigilant : téléchargez et utilisez l'application officielle de votre banque à partir d'un « *store* » officiel (boutique officielle). Par ailleurs, pensez à réaliser les mises à jour disponibles et n'oubliez pas de vous déconnecter de votre espace de banque en ligne. Enfin, ne conservez pas d'informations bancaires dans d'autres espaces de votre téléphone (notes, mémo, calendrier, etc.).

ANNEXES

A1	Conseils de prudence pour l'utilisation des moyens de paiement	52
A2	Protection du payeur en cas de paiement non autorisé	55
A3	Missions et organisation de l'Observatoire	57
A4	Liste nominative des membres de l'Observatoire	59
A5	Méthodologie de mesure de la fraude aux moyens de paiement scripturaux	62
A6	Dossier statistique	71

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

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

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

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

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

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

SOYEZ RESPONSABLES

- Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, pas même à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.
- Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile, etc.), gardez-le secret, ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui.

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

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

SOYEZ ATTENTIFS

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

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

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

Lors des paiements à un professionnel ou à un particulier

- Vérifiez l'utilisation qui est faite de votre carte bancaire par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider une transaction.
- Lorsqu'un chèque est automatiquement rempli par le commerçant, soyez attentif aux mentions indiquées avant de le signer et vérifiez plus particulièrement le montant.

- Quelques précautions lors du remplissage d'un chèque permettent de réduire les risques de fraude : évitez les ratures ou surcharges, inscrivez le nom du bénéficiaire du chèque et les montants en chiffres et en lettres sans laisser d'espace libre, puis tirez un trait sur l'espace restant non utilisé. Le lieu de paiement et la date doivent être renseignés en même temps que les autres mentions. La signature du chèque ne doit pas déborder sur la ligne de chiffres en bas du chèque. En aucun cas, la signature ne doit être apposée seule sur un chèque, c'est-à-dire sans les mentions relatives au montant et au bénéficiaire préalablement renseignées.

Lors des retraits aux distributeurs de billets

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

Lors des paiements sur Internet

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

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

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

Lors de vos déplacements à l'étranger

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

SACHEZ RÉAGIR

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

- Faites immédiatement opposition en appelant le numéro que vous a communiqué votre banque ou l'émetteur de votre moyen de paiement. Pensez à le faire pour toutes vos cartes, chéquiers ou appareils mobiles

comportant une application de paiement et qui ont été perdus ou volés. De même, contactez votre banque si vous avez communiqué vos coordonnées bancaires (numéro de compte, relevé d'identité bancaire, etc.) à un tiers qui vous paraît douteux.
- En cas de vol, déposez également au plus vite une plainte auprès de la police ou de la gendarmerie.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 50 euros. Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

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

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

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

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

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

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

A2 PROTECTION DU PAYEUR EN CAS DE PAIEMENT NON AUTORISÉ

L'ordonnance de transposition de la deuxième directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 13 janvier 2018, a modifié le cadre législatif concernant la responsabilité du payeur en cas d'opération de paiement non autorisée. Les grands principes issus de la première directive concernant les services de paiement restent toutefois inchangés.

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

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

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

OPÉRATIONS NATIONALES OU INTRACOMMUNAUTAIRES

Ces dispositions de protection du payeur couvrent :

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

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

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

Avant l'information aux fins de blocage de l'instrument de paiement, le payeur peut supporter, à concurrence de cinquante euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de l'instrument de paiement. Toutefois, si l'opération de paiement est effectuée sans utilisation des données de sécurité personnalisées, ou que le payeur ne pouvait pas détecter la perte ou le vol de son instrument de paiement, ou que la perte résulte d'une action d'une personne placée sous la responsabilité du PSP, alors le payeur ne voit pas sa responsabilité engagée et il ne supporte aucune perte financière (même en-deçà de cinquante euros).

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

2 Franc CFP (colonies françaises du Pacifique) ou franc Pacifique.

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

La responsabilité du payeur n'est pas non plus engagée si l'opération de paiement non autorisée a été effectuée en détournant à son insu l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas plus engagée en cas de contrefaçon de l'instrument de paiement si ce dernier était en possession de son titulaire au moment où l'opération non autorisée a été réalisée.

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

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

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

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

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

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

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

OPÉRATIONS EXTRAEUROPÉENNES

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

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

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

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

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

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

A3 MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

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

PÉRIMÈTRE CONCERNÉ

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

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

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

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

La carte de paiement est une catégorie d'instrument de paiement offrant à son titulaire les fonctions de retrait ou de transfert de fonds. On distingue différentes typologies de cartes :

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

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

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

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

ATTRIBUTIONS

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

- il assure le suivi de la mise en œuvre des mesures adoptées par les émetteurs, les commerçants et les entreprises pour renforcer la sécurité des moyens de paiement ;
- il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de moyens de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents moyens de paiement scripturaux ;

- il assure une veille technologique en matière de moyens de paiement scripturaux, avec pour objet de proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des moyens de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

En outre, le ministre chargé de l'Économie et des Finances peut, aux termes de l'article R. 141-2 du Code monétaire et financier, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

COMPOSITION

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

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

La liste nominative des membres de l'Observatoire figure en annexe 4.

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

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

MODALITÉS DE FONCTIONNEMENT

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

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

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'Économie et des Finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail permanents chargés, l'un d'harmoniser et d'établir des statistiques en matière de fraude, l'autre d'assurer une veille technologique relative aux moyens de paiement.

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

A4 LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

En application de l'article R. 142-22 du Code monétaire et financier, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel sont nommés pour trois ans par arrêté du ministre de l'Économie. Le dernier arrêté de nomination date du 18 décembre 2019.

PRÉSIDENT

François VILLEROY DE GALHAU
Gouverneur de la Banque de France

REPRÉSENTANTS DES ASSEMBLÉES

Éric BOCQUET
Sénateur

Rémi REBEYROTTE
Député

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

- Le Secrétaire général ou son représentant :
  Dominique LABOUREIX
  Geoffroy GOFFINET

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 :
  Guillaume POUPARD
  Vincent STRUBEL
  José ARAUJO

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

- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Pierre-Jean CANAULT
  Jean-Philippe PAPILLON
- Le directeur général du Trésor ou son représentant :
  Odile RENAUD-BASSO
  Arnaud DELAUNAY
- Présidente de l'Institut d'émission des départements d'outre-mer (IEDOM) et directrice générale de l'Institut d'émission d'outre-mer (IEOM) :
  Marie-Anne POUSSIN-DELMAS
- Le directeur général de la Concurrence, de la Consommation et de la Répression des fraudes ou sa représentante :
  Éric MAURUS
  Madly MERI

Sur proposition du garde des Sceaux, ministre de la Justice :

- Le directeur des Affaires criminelles et des Grâces ou sa représentante :
  Sophie LACOTE

Sur proposition du ministre de l'Intérieur :

- Le chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ou son représentant :
  François-Xavier MASSON

Sur proposition du ministre de la Défense :

- Le directeur général de la Gendarmerie nationale ou son représentant :
  Arnauld CHEMINANT
  Cyril PIAT

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

- Le chef du service des Affaires économiques ou son représentant :
  Clémence SCOTTEZ

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

Philippe DYSERYN
Membre du bureau
Association française des établissements de paiement et de monnaie électronique (Afepame)

Nathalie CHABERT
Déléguée générale adjointe
Association française pour le développement des services et usages multimédias multi-opérateurs (AFMM)

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

Jean-Marie DRAGON
Responsable monétique et paiements innovants
BNP Paribas (BNPP)

Olivier DURAND
Directeur en charge des projets de place
Office de coordination bancaire et financière (OCBF)

Caroline GAYE
Directrice générale
American Express France (Amex)

Solveig HONORÉ HATTON
Vice-présidente *Business development*
MasterCard France

Philippe LAULANIE
Administrateur
Groupement des cartes bancaires (GCB)

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

Laurence MATTERLIN
Directrice *Risk management* et Lutte contre la fraude
Natixis Payment Solutions

Romain BOISSON
Directeur régional
Visa Europe France

Jérôme RAGUÉNÈS
Directeur – Systèmes et Moyens de paiement
Fédération bancaire française (FBF)

Jean-Marie VALLÉE
Directeur général
STET

Narinda YOU
Directrice – Stratégie et relations de place
Crédit Agricole

REPRÉSENTANTS DES ENTREPRISES

Bernard COHEN-HADAD
Président de la Commission financement des entreprises
Confédération des petites et moyennes entreprises (CPME)

Alexandra LEFEBVRE
Responsable du département des Affaires économiques
Mouvement des entreprises de France (MEDEF)

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

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

Mélissa HOWARD
Juriste
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN
Juriste
Union nationale des associations familiales (Unaf)

Mathieu ROBIN
Chargé de mission Banque Assurance
UFC – Que choisir

Hervé MONDANGE
Juriste
Association Force ouvrière consommateurs (Afoc)

Ariane POMMERY
Juriste
Association de défense, d'éducation et d'information du consommateur (Adeic)

REPRÉSENTANTS DES ORGANISATIONS PROFESSIONNELLES DE COMMERÇANTS

Jean-Michel CHANAVAS
Délégué général
Mercatel

Vincent DEPRIESTER
Membre du groupe Finances
Fédération du commerce et de la distribution (FCD)

Philippe JOGUET
Correspondant sur les questions financières
Conseil du commerce de France (CdCF)

Marc LOLIVIER
Délégué général
Fédération du e-commerce et de la vente à distance (Fevad)

Philippe SOLIGNAC
Vice-président
Chambre de commerce et d'industrie de région Paris - Île-de-France (CCIP)

PERSONNALITÉS QUALIFIÉES EN RAISON DE LEURS COMPÉTENCES

Claude FRANCE
Directeur général des opérations France
Worldline

David NACCACHE
Professeur – École normale supérieure (ENS)

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

CADRE GÉNÉRAL

Définition de la fraude aux moyens de paiement

La fraude est 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 et/ou émetteur du moyen de paiement, le titulaire du moyen de paiement, le bénéficiaire légitime des fonds (l'accepteur et/ou le 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** :
  - les moyens employés pour récupérer, sans motif légitime, les données ou le support du moyen de paiement (vol, détournement du support ou des données, piratage d'un équipement d'acceptation, etc.),
  - les modalités d'utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait, en situation de proximité ou à distance, par utilisation physique de l'instrument de paiement ou des données qui lui sont attachées, etc.),
  - la zone géographique d'émission ou d'utilisation du moyen de paiement ou des données qui lui sont attachées ;
- **et quelle que soit l'identité du fraudeur** : un tiers, l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

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

- les tentatives de fraude (auquel cas la fraude est stoppée avant exécution de l'opération) ;
- les utilisations irrégulières d'un moyen de paiement du seul fait d'un défaut de provision suffisante et se traduisant notamment par un impayé ;
- l'utilisation d'une fausse identité ou d'une identité usurpée pour ouvrir un compte et/ou pour obtenir un moyen de paiement en vue de réaliser des paiements.

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 suite à un recours en justice, etc.). L'Observatoire de la sécurité des cartes de paiement avait estimé dans son rapport annuel 2015 [1] que l'impact des mesures de cette nature réduisait de 5 % l'estimation brute de la fraude pour les paiements par carte.

Les données de fraude sont collectées par le secrétariat de l'Observatoire auprès de l'ensemble des établissements concernés, selon une approche différenciée par moyen de paiement (voir 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.

Typologie de la fraude aux moyens de paiement

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

- **faux** (vol, perte, contrefaçon) : fraude par l'établissement d'un faux ordre de paiement soit au moyen d'un instrument de paiement physique (carte, chéquier, etc.) volé, perdu ou contrefait, soit via le détournement de données ou d'identifiants bancaires ;
- **falsification** : fraude par l'utilisation d'un instrument de paiement falsifié (instrument de paiement authentique dont les caractéristiques physiques ou les données attachées ont été modifiées par le fraudeur ou par un complice) ou par altération d'un ordre de paiement régulièrement émis en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.) ;
- **détournement** : fraude visant à utiliser l'instrument de paiement ou l'ordre de paiement sans altération ou modification d'attribut (à titre d'exemple, un fraudeur encaisse un chèque non altéré sur un compte qui n'est pas détenu par le bénéficiaire légitime du chèque) ;
- **rejeu** : fraude par l'utilisation abusive d'un instrument de paiement par son titulaire légitime après la déclaration de sa perte ou de son

vol ou par la contestation de mauvaise foi d'un ordre de paiement valablement émis par le titulaire légitime de l'instrument de paiement, ou par la réutilisation d'un ordre de paiement déjà traité.

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 billets – DAB/guichet automatique bancaire – GAB) situé en France. Aucune distinction n'est faite quant à la nature du réseau d'acceptation (interbancaire [2] ou privatif [3]) ou la catégorie de carte (carte de débit, carte de crédit, carte commerciale ou carte prépayée) concernée.

1 Cf. *https://www.banque-france.fr/rapport-annuel-2015* (page 12).

2 Qualifie les systèmes de paiement par carte faisant intervenir un nombre élevé de prestataires de services de paiement émetteurs de cartes et acquéreurs de paiements.

3 Qualifie les systèmes de paiement par carte faisant intervenir un nombre restreint de prestataires de services de paiement émetteurs de cartes et acquéreurs de paiements (par exemple, au sein d'un seul groupe bancaire).

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 falsifiée ou contrefaite	La falsification d'une carte de paiement consiste à modifier les données magnétiques, d'embossage [a] ou de programmation d'une carte authentique. La contrefaçon d'une carte suppose, quant à elle, la création d'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.
Numéro de carte non affecté	Utilisation d'un numéro de carte (ou PAN – *personnal account number*) cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance.

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.

Origine des données de fraude

Les données de fraude à la carte de paiement sont collectées par l'Observatoire auprès :

- des membres du Groupement des cartes bancaires CB, de MasterCard et de Visa Europe France 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 fraude, 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.

Canal d'utilisation de la carte	Modalités d'utilisation
Paiement de proximité	Paiement réalisé au point de vente ou sur automate, y compris le paiement en mode sans contact.
Paiement à distance	Paiement réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen.
Retrait	Retrait d'espèces à un distributeur automatique de billets.

Zone géographique	Description
Transaction nationale	L'émetteur et l'accepteur sont, tous deux, établis en France. Pour autant, pour les paiements à distance, le fraudeur peut opérer depuis l'étranger.
Transaction internationale France → espace SEPA	L'émetteur est établi en France et l'accepteur est établi à l'étranger dans l'espace SEPA (*single euro payment area*).
Transaction internationale France → hors espace SEPA	L'émetteur est établi en France et l'accepteur est établi à l'étranger hors espace SEPA.
Transaction internationale espace SEPA → France	L'émetteur est établi à l'étranger dans l'espace SEPA et l'accepteur est établi en France.
Transaction internationale hors espace SEPA → France	L'émetteur est établi à l'étranger hors espace SEPA et l'accepteur est établi en France.

Secteur d'activité du commerçant pour les paiements à distance	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	

MESURE DE LA FRAUDE AU VIREMENT

Instruments de paiement couverts

La fraude au virement, telle que mesurée dans le présent rapport, porte sur les ordres de paiement émis par le débiteur – appelé donneur d'ordre – afin de transférer des fonds de son compte de paiement ou de monnaie électronique vers le compte d'un bénéficiaire tiers. Cette catégorie recouvre à la fois les virements au format européen SEPA (*SEPA credit transfert* et *SEPA credit transfert 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 annuelles de fraude qui lui sont faites par les prestataires de services de paiement [4] agréés.

Éléments d'analyse de la fraude

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

4 Établissements habilités 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 :
- 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 ;
- établissements de crédit, établissements de monnaie électronique et établissements de paiement de droit étranger habilités à intervenir sur le territoire français et implantés sur ce dernier.

Typologie de fraude au virement	Forme de la fraude
Faux	Le fraudeur contrefait un ordre de virement, contraint le titulaire légitime à émettre 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.

Zone géographique d'émission et de destination du virement	Description
Virement national	Virement émis depuis un compte tenu en France vers un compte tenu en France.
Virement européen	Virement émis depuis un compte tenu en France vers un compte tenu dans un autre pays de l'espace SEPA (*single euro payment area*).
Virement hors espace SEPA	Virement émis depuis un compte tenu en France vers un compte tenu dans un pays étranger hors espace SEPA.

Canal d'initiation utilisé	Modalités d'utilisation
Papier	Ordre de virement transmis par courrier, formulaire, courriel, télécopie ou téléphone.
Internet	Ordre de virement transmis par la banque en ligne ou par une application de paiement mobile.
Télématique	Ordre de virement transmis via d'autres canaux électroniques, hors banque en ligne et application de paiement mobile, tels que par exemple 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).

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*), et comprend le prélèvement standard (*SDD Core – SEPA direct debit Core*) et le prélèvement inter-entreprises (*SDD B2B – business to business*).

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.
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.
Rejeu	Le fraudeur créancier émet sciemment des prélèvements déjà émis (qui ont soit déjà été réglés ou ont fait l'objet de rejets pour opposition du débiteur par exemple).

Origine des données de fraude

Les données de fraude au prélèvement sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés.

Éléments d'analyse de la fraude

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

Zone géographique d'émission et de destination du virement	Description
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 SEPA.
Prélèvement hors espace SEPA	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un pays étranger, hors espace SEPA.

Canal d'autorisation utilisé	Modalités d'utilisation
Papier	Mandat de prélèvement collecté par courrier, formulaire, courriel, télécopie ou téléphone.
Internet	Mandat de prélèvement émis depuis un canal Internet (site de banque en ligne, site ou application mobile du créancier).
Télématique	Mandat de prélèvement validé via d'autres canaux électroniques, hors site Internet et application mobile de la banque ou du 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 de ce dernier par sa banque. 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 emploi service entreprise (Tese) ; 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, 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 annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés. Ces derniers effectuent leur déclaration soit en qualité d'établissement recevant de son client des chèques à l'encaissement (établissement remettant), soit en qualité d'établissement qui tient le compte du payeur (établissement tiré).

Éléments d'analyse des données de fraude

Les données de fraude au chèque sont analysées à partir des grands types de fraude 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.

Typologie de fraude au chèque	Forme de la fraude
Faux (vol, perte, ou apocryphe [a])	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 [b] (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 à nouveau à l'encaissement. 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. 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. Émission volontaire d'un chèque par le titulaire après sa mise en opposition.

a Apocryphe : terme utilisé par certains établissements pour désigner un écrit dont l'authenticité n'est pas établie.
b 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 fraude 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 annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés. Ces derniers effectuent leur déclaration soit en qualité d'établissement recevant de son client des effets de commerce à l'encaissement (établissement remettant), soit en qualité d'établissement qui tient le compte du payeur (établissement tiré).

DISPOSITIONS SPÉCIFIQUES POUR LA FRAUDE SUR LES TRANSACTIONS EN MONNAIE ÉLECTRONIQUE

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.

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.

Le suivi de la fraude sur les paiements en monnaie électronique par l'Observatoire est intégré à la mesure de la fraude :

- au titre des cartes de paiement pour la monnaie électronique sur support physique (carte prépayée),
- au titre des virements pour la monnaie électronique sous forme de compte en ligne.

A6 DOSSIER STATISTIQUE

VUE D'ENSEMBLE

T1 Cartographie des moyens de paiement scripturaux en 2019

(nombre en millions, montant en milliards d'euros, montant moyen en euros, variation en pourcentage)

	Nombre de transactions		Montant des transactions		Montant moyen
	2019	Variation 2019/2018	2019	Variation 2019/2018	
Paiement carte [a]	14 485	+ 10	599	+ 6	41
dont sans contact	*3 778*	*+ 59*	*43*	*+ 70*	*11*
Prélèvement	4 370	+ 4	1 711	+ 4	391
Virement	4 269	+ 6	25 164	+ 4	5 895
dont VGM [b]	*12*	*+ 26*	*11 556*	*+ 14*	*937 548*
dont virement instantané (SCT inst) [c]	*14*	*+ 7 959*	*7*	*+ 8 078*	*505*
Chèque	1 586	- 9	814	- 9	513
Effet de commerce	78	- 4	232	- 8	2 984
Monnaie électronique	62	- 5	1	- 47	9
Total	**24 850**	**+ 7**	**28 521**	**+ 3**	**1 274**
Retrait carte [a]	1 392	- 3	137	0	98
Total transactions	**26 242**	**+ 6**	**28 658**	**+ 3**	**1 092**

a) Cartes émises en France uniquement.
b) VGM : virement de gros montant, émis au travers de systèmes de paiement de montant élevé (Target 2, Euro 1), correspondant exclusivement à des paiements professionnels.
c) SCT inst : *SEPA instant credit transfer* (SEPA : *Single Euro Payments Area*).

Source : Observatoire de la sécurité des moyens de paiement.

T2 Répartition de la fraude sur les moyens de paiement en montant et en volume en 2019

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

	Montant		Volume		Montant moyen
	2019	Part	2019	Part	
Paiement carte [a]	428 249 931	36	7 071 095	94	61
Chèque	539 215 175	46	183 488	2	2 939
Virement	161 642 174	14	15 934	0	10 144
Prélèvement	10 990 025	1	43 519	1	253
Effet de commerce	74 686	0	1	0	74 686
Total paiements	**1 140 171 991**	**97**	**7 314 037**	**97**	**156**
Retrait carte [a]	41 651 788	3	165 505	3	252
Total transactions	**1 181 823 779**	**100**	**7 479 542**	**100**	**158**

a) Cartes émises en France uniquement.

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LES CARTES DE PAIEMENT

Les données de fraude sur la carte de paiement sont collectées par l'Observatoire auprès :

- des cent vingt membres du Groupement des cartes bancaires CB par l'intermédiaire de celui-ci, MasterCard et Visa Europe France ;
- huit émetteurs de cartes privatives : American Express, Oney Bank, BNP Paribas Personal Finance (Aurore, Cetelem et Cofinoga), Crédit agricole Consumer Finance (Finaref et Sofinco), Cofidis, Franfinance, JCB et UnionPay.

En 2019, le nombre de cartes en circulation s'élève à 94 millions dont :

- 85,1 millions de cartes de type « interbancaire » (CB, MasterCard, Visa, etc.) ;
- 8,9 millions de cartes de type « privatif ».

Le nombre de cartes[1] mises en opposition en 2019 est de 1 405 624.

1 Cartes mises en opposition pour lesquelles au moins une transaction frauduleuse a été enregistrée.

T3 Le marché des cartes de paiement en France – Émission
(volume en millions, valeur en milliards d'euros)

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	11 651,75	424,88	311,64	14,15	66,44	4,59
Paiements à distance hors internet	32,98	2,61	39,16	1,70	1,46	0,33
Paiements à distance sur internet	1 757,36	107,89	398,06	21,57	58,05	2,46
Retraits	1 338,57	130,10	31,17	3,54	21,13	2,77
Total	**14 780,66**	**665,48**	**780,03**	**40,96**	**147,08**	**10,15**
Cartes de type « privatif »						
Paiements de proximité et sur automate	122,43	12,31	11,22	1,82	8,27	1,31
Paiements à distance hors internet	1,88	0,16	1,51	0,02	0,16	0,02
Paiements à distance sur internet	11,52	1,70	9,21	1,47	1,84	0,25
Retraits	1,06	0,10	0,00	0,00	0,00	0,00
Total	**136,89**	**14,27**	**21,94**	**3,31**	**10,27**	**1,58**
Total général	**14 917,55**	**679,75**	**801,97**	**44,27**	**157,35**	**11,73**

Source : Observatoire de la sécurité des moyens de paiement.

T4 Le marché des cartes de paiement en France – Acceptation

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	11 651,75	424,88	378,82	17,44	106,31	8,63
Paiements à distance hors internet	32,98	2,61	9,07	1,54	4,74	1,26
Paiements à distance sur internet	1 757,36	107,89	102,96	8,76	31,84	3,02
Retraits	1 338,57	130,10	27,00	4,46	8,15	1,81
Total	**14 780,66**	**665,48**	**517,85**	**32,20**	**151,04**	**14,72**
Cartes de type « privatif »						
Paiements de proximité et sur automate	122,43	12,31	6,95	1,50	10,87	4,14
Paiements à distance hors internet	1,88	0,16	0,11	0,01	0,22	0,00
Paiements à distance sur internet	11,52	1,70	1,38	0,28	1,00	0,25
Retraits	1,06	0,10	0,00	0,00	0,37	0,17
Total	**136,89**	**14,27**	**8,44**	**1,79**	**12,46**	**4,56**
Total général	**14 917,55**	**679,75**	**526,29**	**33,99**	**163,50**	**19,28**

Source : Observatoire de la sécurité des moyens de paiement.

T5 Répartition de la fraude par type de carte

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)											
	2014		2015		2016		2017		2018		2019	
Cartes de type « interbancaire »	0,080	(486,4)	0,086	(526,8)	0,082	(531,3)	0,070	(482,2)	0,072	(526,5)	0,071	(544,8)
Cartes de type « privatif »	0,062	(14,2)	0,068	(15,5)	0,060	(13,5)	0,043	(11,6)	0,040	(11,0)	0,048	(12,2)
Total	**0,080**	**(500,6)**	**0,085**	**(542,3)**	**0,081**	**544,8**	**0,069**	**493,8**	**0,071**	**537,5**	**0,071**	**557,0**

Source : Observatoire de la sécurité des moyens de paiement.

T6 Répartition de la fraude par zone géographique

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)											
	2014		2015		2016		2017		2018		2019	
Transactions nationales (carte française et accepteur français)	0,043	(234,6)	0,044	(244,4)	0,042	(244,5)	0,037	(226,5)	0,038	(245,6)	0,040	(270,7)
Transactions internationales	0,316	(266,0)	0,372	(297,9)	0,353	(300,3)	0,281	(267,3)	0,270	(291,9)	0,262	(286,3)
dont carte française et accepteur hors SEPA	*0,636*	*(70,0)*	*0,692*	*(74,5)*	*0,713*	*(68,0)*	*0,511*	*(60,3)*	*0,438*	*(50,3)*	*0,441*	*(51,7)*
dont carte française et accepteur SEPA	*0,374*	*(91,0)*	*0,459*	*(116,8)*	*0,370*	*(113,9)*	*0,308*	*(100,7)*	*0,352*	*(143,3)*	*0,333*	*(147,5)*
dont carte étrangère hors SEPA et accepteur français	*0,336*	*(65,6)*	*0,353*	*(69,7)*	*0,449*	*(73,7)*	*0,386*	*(74,1)*	*0,323*	*(65,5)*	*0,311*	*(59,9)*
dont carte étrangère SEPA et accepteur français	*0,134*	*(39,3)*	*0,153*	*(36,9)*	*0,158*	*(44,7)*	*0,102*	*(32,3)*	*0,092*	*(32,8)*	*0,080*	*(27,2)*
Total	**0,080**	**(500,6)**	**0,085**	**(542,3)**	**0,081**	**(544,8)**	**0,069**	**(493,8)**	**0,071**	**(537,5)**	**0,071**	**(557,0)**

Source : Observatoire de la sécurité des moyens de paiement.

T7 Répartition de la fraude nationale par type de transaction

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)											
	2014		2015		2016		2017		2018		2019	
Carte française – accepteur français												
Paiements	0,046	(193,2)	0,047	(204,5)	0,045	(208,6)	0,039	(191,9)	0,041	(214,7)	0,043	(234,8)
dont paiements de proximité et sur automate	*0,010*	*(37,1)*	*0,012*	*(43,4)*	*0,009*	*(33,6)*	*0,009*	*(35,8)*	*0,010*	*(41,4)*	*0,010*	*(44,2)*
dont paiements à distance	*0,248*	*(156,0)*	*0,244*	*(161,1)*	*0,241*	*(175,0)*	*0,190*	*(156,1)*	*0,173*	*(173,3)*	*0,170*	*(190,6)*
– dont par courrier / téléphone	*0,147*	*(2,8)*	*0,372*	*(9,1)*	*0,280*	*(9,3)*	*0,357*	*(7,4)*	*0,351*	*(9,5)*	*0,270*	*(7,5)*
– dont sur internet	*0,251*	*(153,2)*	*0,239*	*(152,0)*	*0,239*	*(165,7)*	*0,186*	*(148,7)*	*0,168*	*(163,8)*	*0,167*	*(183,1)*
Retraits	0,034	(41,5)	0,033	(39,9)	0,029	(35,9)	0,027	(34,6)	0,024	(30,9)	0,028	(35,9)
Total	**0,043**	**(234,6)**	**0,044**	**(244,4)**	**0,042**	**(244,5)**	**0,037**	**(226,5)**	**0,038**	**245,6**	**0,040**	**(270,7)**

Source : Observatoire de la sécurité des moyens de paiement.

T8 Répartition de la fraude internationale par type de transaction – Cartes françaises

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)									
	2015		2016		2017		2018		2019	
Carte française – accepteur étranger hors SEPA										
Paiements	0,735	(56,3)	0,862	(56,2)	0,608	(53,3)	0,534	(44,4)	0,525	(47,1)
dont paiements de proximité et sur automate	*0,509*	*(25,8)*	*0,485*	*(22,9)*	*0,252*	*(12,7)*	*0,230*	*(12,9)*	*0,187*	*(11,0)*
dont paiements à distance	*1,174*	*(30,5)*	*1,862*	*(33,3)*	*1,096*	*(40,6)*	*1,168*	*(31,5)*	*1,175*	*(36,1)*
– dont par courrier / téléphone	*2,345*	*(9,5)*	*2,783*	*(9,4)*	*1,499*	*(8,4)*	*1,127*	*(4,8)*	*1,263*	*(4,4)*
– dont sur internet	*0,959*	*(21,1)*	*1,648*	*(23,9)*	*1,025*	*(32,3)*	*1,175*	*(26,7)*	*1,164*	*(31,7)*
Retraits	0,586	(18,1)	0,390	(11,8)	0,229	(7,0)	0,184	(5,9)	0,168	(4,6)
Total	**0,692**	**(74,4)**	**0,713**	**(68,0)**	**0,511**	**(60,3)**	**0,438**	**50,3**	**0,441**	**(51,7)**
Carte française – accepteur étranger SEPA										
Paiements	0,526	(115,7)	0,422	(112,9)	0,342	(99,8)	0,385	(142,4)	0,359	(146,4)
dont paiements de proximité et sur automate	*0,071*	*(8,0)*	*0,066*	*(8,3)*	*0,075*	*(10,5)*	*0,066*	*(10,2)*	*0,061*	*(9,8)*
dont paiements à distance	*1,004*	*(107,7)*	*0,754*	*(104,5)*	*0,591*	*(89,2)*	*0,617*	*(132,2)*	*0,552*	*(136,6)*
– dont par courrier / téléphone	*1,399*	*(18,7)*	*1,317*	*(19,7)*	*1,489*	*(14,9)*	*0,911*	*(14,2)*	*1,159*	*(19,9)*
– dont sur internet	*0,948*	*(89,0)*	*0,687*	*(84,9)*	*0,527*	*(74,4)*	*0,594*	*(118,0)*	*0,507*	*(116,7)*
Retraits	0,033	(1,1)	0,024	(0,9)	0,025	(0,9)	0,025	(0,9)	0,030	(1,1)
Total	**0,459**	**(116,8)**	**0,370**	**(113,8)**	**0,308**	**(100,7)**	**0,352**	**(143,3)**	**0,333**	**(147,5)**

Source : Observatoire de la sécurité des moyens de paiement.

T9 Répartition de la fraude internationale par type de transaction – Cartes étrangères

(taux en pourcentage, montant entre parenthèses en millions d'euros)

	Taux de fraude (et montant)									
	2015		2016		2017		2018		2019	
Carte étrangère hors SEPA – accepteur français										
Paiements	0,391	(68,1)	0,507	(73,2)	0,429	(73,3)	0,357	(64,8)	0,342	(59,3)
dont paiements de proximité et sur automate	*0,168*	*(22,8)*	*0,169*	*(17,4)*	*0,135*	*(16,3)*	*0,108*	*(13,7)*	*0,124*	*(15,8)*
dont paiements à distance	*1,185*	*(45,3)*	*1,341*	*(55,8)*	*1,143*	*(57,0)*	*0,947*	*(51,1)*	*0,956*	*(43,5)*
– dont par courrier / téléphone	*1,159*	*(10,8)*	*1,748*	*(18,2)*	*1,488*	*(19,8)*	*0,886*	*(11,5)*	*0,813*	*(10,3)*
– dont sur internet	*1,193*	*(34,5)*	*1,206*	*(37,7)*	*1,017*	*(37,2)*	*0,967*	*(39,6)*	*1,011*	*(33,2)*
Retraits	0,069	(1,6)	0,024	(0,5)	0,038	(0,8)	0,031	(0,7)	0,031	(0,6)
Total	**0,353**	**(69,7)**	**0,449**	**(73,7)**	**0,386**	**(74,1)**	**0,323**	**(65,5)**	**0,311**	**(59,9)**
Carte étrangère SEPA – accepteur français										
Paiements	0,175	(36,0)	0,178	(43,8)	0,114	(31,5)	0,102	(32,0)	0,089	(26,4)
dont paiements de proximité et sur automate	*0,033*	*(4,8)*	*0,024*	*(3,7)*	*0,018*	*(3,5)*	*0,018*	*(3,4)*	*0,023*	*(4,5)*
dont paiements à distance	*0,528*	*(31,3)*	*0,456*	*(40,0)*	*0,337*	*(28,0)*	*0,229*	*(28,6)*	*0,207*	*(21,9)*
– dont par courrier / téléphone	*0,734*	*(7,7)*	*0,695*	*(11,0)*	*0,564*	*(8,9)*	*0,357*	*(6,2)*	*0,348*	*(5,4)*
– dont sur internet	*0,484*	*(23,6)*	*0,403*	*(29,0)*	*0,284*	*(19,1)*	*0,208*	*(22,4)*	*0,183*	*(16,5)*
Retraits	0,025	(0,9)	0,024	(0,9)	0,019	(0,7)	0,019	(0,8)	0,018	(0,8)
Total	**0,153**	**(36,9)**	**0,158**	**(44,7)**	**0,102**	**(32,3)**	**0,092**	**(32,8)**	**0,080**	**(27,2)**

Source : Observatoire de la sécurité des moyens de paiement.

T10 Répartition de la fraude nationale selon son origine et par type de carte en 2019

(montant en millions d'euros, part en pourcentage)

	Tous types de carte		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	82,9	30 ,6	82,5	30,9	0,4	11,9
Carte non parvenue	1,7	0,6	1,6	0,5	0,1	4,3
Carte altérée ou contrefaite	2,3	0,9	2,2	0,8	0,1	2,4
Numéro usurpé	181,0	66,9	180,0	67,4	1,0	28,9
Autres	2,8	1	1,0	0,4	1,8	52,5
Total	**270,7**	**100,00**	**267,3**	**100,00**	**3,4**	**100,00**

Source : Observatoire de la sécurité des moyens de paiement.

T11 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » – Émission

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

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**1 066,0**	**42 513,5**	**74,3**	**9 558,3**	**56,1**	**10 627,6**
Cartes perdues ou volées	1 003,5	38 473,6	39,6	3 993,3	13,9	2 683,1
Cartes non parvenues	14,2	909,9	0,3	120,5	0,3	27,7
Cartes altérées ou contrefaites	25,0	1 216,3	12,0	1 726,6	29,6	4 735,6
Numéros de cartes usurpés	12,2	1 041,2	17,1	2 672,6	7,4	2 191,4
Autres	11,1	872,5	5,3	1 045,3	4,9	989,7
Paiements à distance hors internet	**60,5**	**6 874,3**	**309,7**	**19 125,1**	**14,4**	**4 022,3**
Cartes perdues ou volées	5,7	1 415,7	9,0	754,4	1,1	199,1
Cartes non parvenues	0,0	3,3	0,2	22,2	0,1	1,8
Cartes altérées ou contrefaites	0,3	106	3,4	335,0	0,5	125,0
Numéros de cartes usurpés	54,4	5 343,9	296,5	17 985,3	12,6	3 687,7
Autres	0,1	5,4	0,5	28,2	0,1	8,7
Paiements à distance sur internet	**2 627,8**	**182 078,7**	**2 356,6**	**115 366,1**	**451,8**	**31 295,5**
Cartes perdues ou volées	119,3	7 514,9	54,9	3 905,2	13,1	988,8
Cartes non parvenues	0,2	9,5	0,7	37,3	0,1	16,1
Cartes altérées ou contrefaites	28,3	915,0	123,7	5 181,3	37,5	1 461,0
Numéros de cartes usurpés	2 479,4	173 608,7	2 174,5	106 136,9	399,8	28 788,0
Autres	0,6	30,6	2,7	105,4	1,3	41,6
Retraits	**121,2**	**35 818,7**	**4,6**	**1 065,1**	**38,6**	**4 651,0**
Cartes perdues ou volées	118,4	35 133,8	3,3	873,9	4,9	862,5
Cartes non parvenues	2,0	552,6	0,0	12,5	0,1	12,3
Cartes altérées ou contrefaites	0,0	2,4	0,2	34,7	30,7	3 657,4
Numéros de cartes usurpés	0,1	22,8	0,3	42,6	0,7	84,0
Autres	0,7	107,1	0,7	101,5	2,1	34,7
Total	**38 755**	**267 285,2**	**2 745,2**	**145 114,6**	**560,9**	**50 596,4**

Source : Observatoire de la sécurité des moyens de paiement.

T12 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » – Acceptation

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**1 066,0**	**42 513,6**	**38,1**	**4 005,8**	**59,5**	**13 745,0**
Cartes perdues ou volées	1 003,5	38 473,6	21,5	2 284,1	36,6	8 955,7
Cartes non parvenues	14,2	910,0	0,2	17,8	0,5	155,5
Cartes altérées ou contrefaites	25,0	1 216,3	6,7	450,5	10,5	2 404,3
Numéros de cartes usurpés	12,2	1 041,2	9,2	1 063,5	9,3	1 757,7
Autres	11,1	872,5	0,5	190,0	2,6	471,7
Paiements à distance hors internet	**60,6**	**6 874,3**	**17,8**	**5 032,7**	**23,3**	**9 014,1**
Cartes perdues ou volées	5,7	1 415,7	0,3	60,3	1,6	427,0
Cartes non parvenues	0,0	3,4	0,1	13,1	0,0	30,9
Cartes altérées ou contrefaites	0,3	106,0	0,8	162,2	1,9	578,9
Numéros de cartes usurpés	54,4	5 343,9	16,5	4 786,5	19,7	7 952,0
Autres	0,1	5,4	0,1	10,7	0,1	25,4
Paiements à distance sur internet	**2 627,8**	**182 078,7**	**137,6**	**16 212,6**	**217,4**	**32 436,7**
Cartes perdues ou volées	119,3	7 514,9	2,3	203,8	8,5	1 100,4
Cartes non parvenues	0,2	9,5	0,6	49,0	0,3	32,5
Cartes altérées ou contrefaites	28,3	915,0	4,8	429,6	16,0	2 150,6
Numéros de cartes usurpés	2 479,4	173 608,7	127,9	15 306,6	190,5	28 572,1
Autres	0,6	30,6	1,9	223,6	2,1	581,0
Retraits	**121,2**	**35 818,7**	**3,0**	**805,1**	**1,5**	**507,6**
Cartes perdues ou volées	118,4	35 133,8	2,6	729,5	1,0	285,7
Cartes non parvenues	2,0	552,6	0,0	2,0	0,0	1,7
Cartes altérées ou contrefaites	0,0	2,4	0,1	21,3	0,3	152,7
Numéros de cartes usurpés	0,1	22,8	0,2	40,2	0,1	12,8
Autres	0,7	107,1	0,1	12,2	0,1	54,8
Total	**3 875,6**	**267 285,3**	**196,5**	**26 056,2**	**301,7**	**55 703,4**

Source : Observatoire de la sécurité des moyens de paiement.

T13 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » – Émission

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

	Émetteur français, acquéreur français		Émetteur français, acquéreur étranger SEPA		Émetteur français, acquéreur étranger hors SEPA	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**3,4**	**1 661,5**	**1,3**	**219,6**	**2,0**	**411,6**
Cartes perdues ou volées	1,0	159,3	0,6	99,9	0,8	245,3
Cartes non parvenues	0,2	94,7	0,0	1,0	0,0	1,1
Cartes altérées ou contrefaites	0,1	18,9	0,1	29,9	0,9	103,2
Numéros de cartes usurpés	0,2	33,4	0,4	43,9	0,3	52,1
Autres	1,9	1 355,2	0,2	44,9	0,0	9,9
Paiements à distance hors internet	**3,5**	**623,9**	**17,3**	**818,8**	**3,8**	**342,3**
Cartes perdues ou volées	0,6	106,3	1,5	84,3	0,3	36,1
Cartes non parvenues	0,1	11,0	0,0	1,7	0,0	0,0
Cartes altérées ou contrefaites	0,2	44,3	1,0	41,8	0,8	27,7
Numéros de cartes usurpés	2,5	435,3	14,4	643,7	2,7	272,3
Autres	0,1	27,0	0,4	47,3	0,0	6,2
Paiements à distance sur internet	**2,9**	**989,1**	**16,1**	**1 353,7**	**3,4**	**367,8**
Cartes perdues ou volées	0,3	52,1	1,0	80,1	0,2	20,2
Cartes non parvenues	0,0	10,8	0,0	4,4	0,0	0,0
Cartes altérées ou contrefaites	0,1	19,4	1,0	32,2	0,3	25,1
Numéros de cartes usurpés	2,0	511,3	13,5	1 116,4	2,9	313,1
Autres	0,5	395,5	0,6	120,6	0,0	9,4
Retraits	**1,0**	**117,0**	**0,0**	**0,0**	**0,0**	**0,0**
Cartes perdues ou volées	0,7	85,6	0,0	0,0	0,0	0,0
Cartes non parvenues	0,2	27,3	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,0	0,0	0,0	0,0	0,0
Numéros de cartes usurpés	0,0	0,0	0,0	0,0	0,0	0,0
Autres	0,1	4,1	0,0	0,0	0,0	0,0
Total	**10,8**	**3 391,5**	**34,7**	**2 392,1**	**9,2**	**1 121,7**

Source : Observatoire de la sécurité des moyens de paiement.

T14 Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » – Acceptation

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

	Émetteur français, acquéreur français		Émetteur étranger SEPA, acquéreur français		Émetteur étranger hors SEPA, acquéreur français	
	Volume	Valeur	Volume	Valeur	Volume	Valeur
Paiements de proximité et sur automate	**3,4**	**1 661,5**	**0,4**	**443,2**	**3,0**	**2 079,6**
Cartes perdues ou volées	1,0	159,3	0,2	148,4	1,2	1 166,0
Cartes non parvenues	0,2	94,7	0,1	160,8	0,0	1,7
Cartes altérées ou contrefaites	0,1	18,9	0,0	6,5	1,2	635,4
Numéros de cartes usurpés	0,2	33,4	0,1	28,5	0,5	230,1
Autres	1,9	1 355,2	0,1	99,0	0,1	46,4
Paiements à distance hors internet	**3,5**	**623,9**	**0,8**	**360,7**	**2,1**	**1 261,8**
Cartes perdues ou volées	0,6	106,3	0,0	12,3	0,1	25,6
Cartes non parvenues	0,1	11,0	0,0	0,0	0,0	0,5
Cartes altérées ou contrefaites	0,2	44,3	0,0	54,0	0,3	147,7
Numéros de cartes usurpés	2,5	435,3	0,8	292,7	1,7	1 074,6
Autres	0,1	27,0	0,0	1,7	0,0	13,4
Paiements à distance sur internet	**2,9**	**989,1**	**0,9**	**309,9**	**2,7**	**736,3**
Cartes perdues ou volées	0,3	52,1	0,0	2,6	0,1	30,1
Cartes non parvenues	0,0	10,8	0,0	2,3	0,0	1,7
Cartes altérées ou contrefaites	0,1	19,4	0,0	2,0	0,5	191,1
Numéros de cartes usurpés	2,0	511,3	0,9	281,6	2,0	499,5
Autres	0,5	395,5	0,0	21,4	0,1	13,9
Retraits	**1,0**	**116,9**	**0,0**	**0,0**	**0,3**	**106,5**
Cartes perdues ou volées	0,7	85,6	0,0	0,0	0,0	1,8
Cartes non parvenues	0,2	27,3	0,0	0,0	0,0	0,0
Cartes altérées ou contrefaites	0,0	0,0	0,0	0,0	0,3	101,7
Numéros de cartes usurpés	0,0	0,0	0,0	0,0	0,0	0,0
Autres	0,1	4,0	0,0	0,0	0,0	3,0
Total	**10,9**	**3 391,4**	**2,1**	**1 113,8**	**8,1**	**4 184,2**

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE CHÈQUE

T15 Évolution de la fraude

(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018
En montant de transactions	**276 716 554**	**296 072 847**	+ 7	**450 108 464**	+ 52	**539 215 175**	+ 20
En nombre de transactions	120 295	114 906	- 4	166 421	+ 45	183 488	+ 10

Source : Observatoire de la sécurité des moyens de paiement.

T16 Répartition de la fraude par typologie de fraude

(montant en euros, part entre parenthèses)

	2016		2017		2018		2019	
Détournement, rejeu	5 010 202	(2)	10 002 809	(3)	14 741 262	(3)	20 454 286	(4)
Vol, perte (faux, apocryphe)	123 537 940	(45)	130 815 653	(44)	252 890 727	(56)	296 367 562	(55)
Contrefaçon	32 418 849	(11)	28 097 173	(10)	36 739 051	(8)	76 511 582	(14)
Falsification	115 749 563	(42)	127 157 212	(43)	145 737 424	(33)	145 881 745	(27)
Total	**276 716 554**	**(100)**	**296 072 847**	**(100)**	**450 108 464**	**(100)**	**539 215 175**	**(100)**

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE VIREMENT

T17 Évolution de la fraude

(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018
En montant de transactions	**86 359 473**	**78 286 492**	- 9	**97 307 108**	+ 24	**161 642 174**	+ 66
En nombre de transactions	5 585	4 642	- 17	7 731	+ 67	15 934	+ 106

Source : Observatoire de la sécurité des moyens de paiement.

T18 Répartition de la fraude par typologie de fraude

(montant en euros, part entre parenthèses)

	2016		2017		2018		2019	
Faux	63 707 498	(74)	42 008 522	(53)	51 069 661	(52)	98 525 485	(61)
Falsification	4 477 057	(5)	1 304 143	(2)	485 131	(1)	3 438 923	(2)
Détournement	14 978 462	(17)	32 966 084	(42)	40 250 639	(41)	56 514 755	(35)
Autres	3 196 456	(4)	2 007 743	(3)	5 501 677	(6)	3 163 011	(2)
Total	**86 359 473**	**(100)**	**78 286 492**	**(100)**	**97 307 108**	**(100)**	**161 642 174**	**(100)**

Source : Observatoire de la sécurité des moyens de paiement.

T19 Répartition de la fraude par zone géographique
(montant en euros, part en pourcentage)

	2019	
	Montant	Part
France	83 949 203	52
SEPA hors France	66 060 701	41
Hors SEPA	11 632 270	7
Total	**161 642 174**	**100**

Source : Observatoire de la sécurité des moyens de paiement.

STATISTIQUES DE FRAUDE SUR LE PRÉLÈVEMENT

T20 Évolution de la fraude
(montant en euros, nombre en unités, variation en pourcentage)

	2016	2017	Variation 2017/2016	2018	Variation 2018/2017	2019	Variation 2019/2018
En montant de transactions	**39 935 882**	**8 726 403**	- 78	**58 346 253**	+ 569	**10 990 025**	- 81
En nombre de transactions	1 176	25 806	+ 209	309 377	+ 110	43 519	- 86

Source : Observatoire de la sécurité des moyens de paiement.

T21 Répartition de la fraude par typologie de fraude
(montant en euros, part entre parenthèses)

	2016		2017		2018		2019	
Faux	5 270 858	(13)	6 141 836	(71)	58 329 283	(99)	3 961 260	(34)
Détournement	34 647 562	(87)	2 305 112	(26)	16 703	(0)	6 677 467	(61)
Autres	17 462	(0)	8 726 403	(3)	267	(0)	351 298	(3)
Total	**39 935 882**		**8 726 403**		**58 346 253**		**10 990 025**	

Source : Observatoire de la sécurité des moyens de paiement.

T22 Répartition de la fraude par zone géographique
(montant en euros, part en pourcentage)

	2019	
	Montant	Part
France	10 583 886	96
SEPA hors France	406 139	4
Hors SEPA	0	0
Total	**10 990 025**	**100**

Source : Observatoire de la sécurité des moyens de paiement.

Éditeur
Banque de France

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

Rédactrice en chef
Valérie Fasquelle
Directrice des Infrastructures, de l'Innovation et des Paiements
Banque de France

Secrétariat de rédaction
Pierre Bienvenu, Olivier Catau, Caroline Corcy, Florian Dintilhac, Christelle Guiheneuc, Trân Huynh, Julien Lasalle, Mathieu Vileyn

Réalisation
Studio Création
Direction de la Communication

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

Impression
Banque de France – SG - DISG

Dépôt légal
Septembre 2020
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