# Rapport annuel
# de l'Observatoire de la sécurité des moyens de paiement

2018

BANQUE DE FRANCE
EUROSYSTÈME

bservatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

# Rapport annuel 2018
# de l'Observatoire de la sécurité des moyens de paiement

*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**

*L'Observatoire de la sécurité des moyens de paiement, mentionné au I de l'article L. 141-4 du Code monétaire et financier, a été créé par la loi n° 2016-1691 du 9 décembre 2016. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, entreprises, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des moyens de paiement scripturaux.*

*Conformément à l'alinéa 7 de cet article, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'Économie et des Finances et transmis au Parlement.*

# Synthèse

*Ce troisième rapport annuel de l'Observatoire de la sécurité des moyens de paiement rend compte d'un bilan contrasté en matière de fraude aux moyens de paiement scripturaux.*

*En effet, les tendances suivantes (détaillées dans le* ***chapitre 2****) se dégagent en 2018.*

- *Le chèque devient le moyen de paiement le plus fraudé en France, le montant de la fraude, qui atteint 450 millions d'euros (296 millions en 2017, soit + 52 %), représentant désormais 43,1 % de la fraude totale (40 % en 2017), et ce alors que son utilisation continue de décroître (– 11 % en montant).*

- *Les taux de fraude sur les autres moyens de paiement sont quasi stables, à un niveau bas.*

  *– Ainsi, si le taux de fraude sur les cartes de paiement françaises augmente très légèrement et s'établit désormais à 0,062 %, contre 0,058 % en 2017, les taux de fraude par type de paiement carte en France restent soit maîtrisés à un niveau faible et quasi stable (0,010 %, contre 0,009 % un an auparavant, pour les paiements de proximité et sur automates), soit stabilisés (0,020 %, tout comme en 2017 pour les paiements sans contact, qui ont pourtant quasiment doublé en 2018), soit de nouveau en diminution : c'est en effet le cas des paiements à distance, avec un taux en baisse pour la septième année consécutive, à 0,173 %, contre 0,190 % en 2017, alors même que ces paiements connaissent une forte croissance par rapport à 2017 (+ 22 %).*

  *Pour les transactions internationales, on constate à nouveau une diminution du taux de fraude à 0,270 % en 2018, contre 0,281 % un an auparavant [1]. La fraude en zone SEPA (*single euro payments area*) reste mieux maîtrisée qu'en-dehors de l'espace européen SEPA, tout en soulignant des taux de fraude à l'étranger plus élevés qu'au niveau national : les transactions internationales représentent ainsi 54 % du montant total de la fraude alors qu'elles ne comptent que pour 14 % de la valeur totale des transactions.*

1 C'est-à-dire pour les cartes des porteurs français fraudées à l'étranger, ainsi que celles des porteurs étrangers fraudées en France.

*– Concernant le virement et le prélèvement, ces moyens de paiement présentent toujours des taux de fraude extrêmement bas, à respectivement 0,0035 % et 0,0004 %.*

*Dans ce contexte, l'Observatoire a mené en 2018 et 2019 deux études présentées au* ***chapitre 3*** *sur la sécurité du chèque et des moyens de paiement non connectés en général, ainsi que sur la sécurité des paiements par mobile.*

*• Il ressort de l'analyse conduite sur le chèque que ce dernier ne permet pas la mise en place de dispositifs avancés de sécurisation et demeure donc vulnérable aux actes de falsification et de contrefaçon. Pour autant un renforcement de la sécurité est possible et nécessaire : l'Observatoire invite ainsi l'ensemble des professionnels à mettre en place des moyens d'identification des transactions à risque permettant, par exemple, aux banques d'alerter le titulaire de compte en cas de mouvements suspects ou aux commerçants de refuser une transaction au point de vente en cas de suspicion de fraude. Par ailleurs, et notamment pour ce moyen de paiement, les utilisateurs, qu'ils soient particuliers, entreprises ou administrations, doivent rester vigilants quant à son utilisation, en étant par exemple attentifs à la perte ou au vol de chéquiers (comme rappelé parmi les bonnes pratiques en matière de vigilance présentées en* ***annexe 1*** *de ce rapport).*

*• Par contraste, les téléphones mobiles offrent des capacités de sécurisation avancées des paiements et des données sensibles de paiement (identifiants de carte notamment), bien que le niveau de sécurité des dispositifs déployés reste inégal en fonction des technologies adoptées. L'Observatoire a toutefois constaté un taux de fraude sur les paiements par mobile particulièrement maîtrisé en France (à 0,03 %), et atteignant 0,04 % toutes transactions confondues. Ceci confirme la pertinence des recommandations adressées aux acteurs – banques, systèmes de paiement par carte et fournisseurs de solutions technologiques – appelés à mettre en œuvre l'authentification renforcée, tant pour sécuriser l'enrôlement des utilisateurs au sein des applications de paiement présentes sur les téléphones mobiles que pour identifier et prévenir les transactions à risque.*

*Ces derniers éléments soulignent l'importance de l'entrée en vigueur, à compter du 14 septembre 2019, des normes techniques de réglementation dédiées aux dispositifs de sécurité de la deuxième directive européenne sur les services de paiement (dite DSP2). Ces normes prévoient notamment la généralisation de l'authentification renforcée pour les paiements électroniques, mais aussi la mise en œuvre de dispositifs d'identification des*

*transactions à risque (qui permettront de s'affranchir d'une authentification renforcée si les taux de fraude sont maintenus à des niveaux faibles pour les transactions à distance).*

*À ce sujet, l'Observatoire encourage tous les acteurs du paiement à maintenir leurs efforts pour se mettre en conformité avec ces évolutions réglementaires. Ainsi, de nouveaux dispositifs d'authentification renforcée viendront progressivement remplacer l'utilisation d'un code reçu par SMS. Ces dispositifs pourront par exemple reposer sur une application, pour* smartphone *ou carte SIM (compatible avec tous les mobiles), nécessitant la saisie d'un code secret ou la vérification d'une donnée biométrique. Les établissements veilleront à proposer des solutions adaptées à l'ensemble de leur clientèle, y compris les plus fragiles. Soucieux toutefois d'accompagner dans les meilleures conditions une transition complexe qui ne soit pas pénalisante pour le commerce électronique et ses utilisateurs, l'Observatoire propose une migration ambitieuse mais étalée dans le temps vers ces nouveaux dispositifs, conforme aux orientations définies par l'Autorité bancaire européenne dans son avis [2] du 21 juin 2019. Le plan de migration ainsi élaboré pour la France a reçu l'aval de l'ensemble des acteurs impliqués, banques, commerçants, systèmes de paiement par carte et associations de consommateurs (cf.* ***chapitre 1****), avec l'objectif d'être mis en œuvre pour une nette majorité des clients et transactions d'ici décembre 2020, et complètement achevé en trois ans. L'Observatoire en fera un point régulier au sein de son rapport annuel.*

*Enfin, l'Observatoire s'engage à contribuer activement aux objectifs de la stratégie nationale des paiements scripturaux [3], en faveur du développement de solutions de paiement innovantes et sécurisées.*

2 L'avis de l'Autorité bancaire européenne est consultable en ligne, depuis : *https://eba.europa.eu*

3 La nouvelle stratégie nationale des moyens de paiement scripturaux pour la période 2019-2024 est disponible en ligne à l'adresse suivante : *https://www.banque-france.fr/stabilite-financiere/comite-national-des-paiements-scripturaux/strategie-nationale-sur-les-moyens-de-paiement*

# 1 Plan de migration des solutions d'authentification forte reposant sur la réception d'un code temporaire reçu par SMS (SMS OTP)

Encadré 1

## Synthèse

- En France, la protection des paiements à distance par carte, comme des opérations sensibles de banque en ligne telle l'initiation d'un virement, repose sur un ensemble de dispositifs dont l'authentification forte des transactions jugées à risque, réalisée en grande majorité par l'envoi de codes SMS à usage unique au porteur légitime de la carte.
- Cette méthode d'authentification a prouvé son efficacité en matière de lutte contre la fraude aux paiements par carte en ligne, comme l'attestent les chiffres de l'Observatoire : pour la septième année consécutive, les taux de fraude sur ces paiements s'inscrivent en baisse, pour atteindre un plus bas historique à 0,173 %, soit un euro de fraude pour 578 euros de transactions.
- La réglementation européenne a mis en place des dispositions visant à renforcer encore la sécurité des paiements électroniques, notamment sur internet, et l'accès plus sûr à des services de banque en ligne. Ainsi, à partir du 14 septembre 2019, des dispositifs conformes à la nouvelle réglementation viendront progressivement remplacer l'utilisation du seul code reçu par SMS pour authentifier ces opérations.
- Ces nouveaux dispositifs pourront, par exemple, reposer sur une application, pour *smartphone* ou carte SIM (compatible avec tous les mobiles), qui nécessite la saisie d'un code secret ou la vérification d'une donnée biométrique. Ces solutions sont choisies par les établissements bancaires et les prestataires de services de paiement, et proposées à leurs clients. Les établissements veilleront à proposer des solutions adaptées à l'ensemble de leur clientèle, y compris les plus fragiles.
- Afin d'accompagner l'ensemble des acteurs de marché vers ces nouvelles solutions de renforcement de la sécurité des transactions en ligne, l'Observatoire a élaboré un plan de migration en plusieurs étapes, dont l'objectif est d'être mis en œuvre pour une nette majorité des clients et transactions d'ici décembre 2020, et complètement achevé en trois ans.

## 1.1 Introduction

La deuxième directive sur les services de paiement (DSP2), directive (UE) 2015/2366, qui définit l'authentification forte du client (SCA – *strong customer authentification*), est entrée en application le 13 janvier 2018. Les normes techniques réglementaires (UE) 2018/389 (RTS – *regulatory technical standards*), qui précisent cette directive, entreront en application le 14 septembre 2019 et exigeront l'application d'une « *authentification forte du client lorsque le payeur accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse* ».

L'Autorité bancaire européenne (ABE) contribue à la convergence européenne des pratiques de surveillance, à la création des conditions de concurrence équitables et à offrir une protection élevée aux déposants, aux investisseurs et aux consommateurs. Celle-ci a précisé dans sa lettre publique en date du 13 juin 2018 (EBA-Op-2018-04) ses positions concernant l'implémentation des RTS, notamment en ce qui concerne l'authentification forte du client. Lors d'un paiement sur internet, la saisie des données inscrites sur une carte de paiement ne peut pas constituer l'un des deux facteurs d'authentification nécessaires à la mise en œuvre d'une SCA.

Ainsi, la solution d'authentification considérée jusqu'alors comme forte et mise en œuvre par les principaux établissements bancaires français dans le cadre des paiements par carte sur internet, à savoir la saisie des données de la carte et d'un code temporaire reçu par SMS (SMS OTP – *one time password*), ne constitue pas une solution de SCA conforme à cette nouvelle réglementation. De la même manière, cette même technique utilisée pour authentifier l'utilisateur de la banque en ligne (BEL) lors de certaines opérations sensibles n'est pas conforme.

Afin de respecter la date d'application du RTS fixée au 14 septembre 2019, qui impose l'authentification forte tout en reconnaissant le temps nécessaire au marché pour procéder aux nécessaires adaptations, l'Observatoire de la sécurité des moyens de paiement a souhaité accompagner les principaux acteurs impactés par la mise en œuvre de la DSP2 dans leur migration vers des solutions pleinement conformes à la nouvelle réglementation.

L'ajout d'un nouveau facteur d'authentification à un dispositif existant, comme la mise en place d'un nouveau dispositif d'authentification, conforme à la définition de la SCA, sont des projets qui nécessitent un délai de mise en œuvre technique significatif. Il est conjointement nécessaire que l'ensemble des utilisateurs utilise de manière effective les nouvelles solutions déployées.

Cette migration représente un projet d'ampleur, qui nécessite un découpage en plusieurs étapes et un délai de mise en œuvre important.

## 1.2 Suivi de la migration vers les solutions d'authentification forte du client

Pour suivre l'avancée de cette migration au sein des principaux établissements bancaires, la Banque de France a mis en place des indicateurs qui seront ajoutés au questionnaire « *3D Secure* » existant, adapté à cette fin. Celui-ci

Indicateurs relatifs aux paiements par carte sur internet et aux opérations sensibles sur la banque en ligne (BEL)

a) Paiements par carte sur internet

| Suivi | Indicateurs |
|---|---|
| Tendance du SMS OTP | Nombre de porteurs de carte enrôlés dans un dispositif d'authentification lors d'un paiement par carte sur internet |
| | Nombre de porteurs de carte enrôlés dans un dispositif d'authentification non conforme à la SCA (et non enrôlés dans un dispositif conforme) lors d'un paiement par carte sur internet |
| | Nombre de paiements par carte sur internet lors des trois derniers mois |
| | Nombre de paiements par carte sur internet lors des trois derniers mois requérant, au regard de la réglementation, une authentification forte du porteur |
| | Nombre de paiements par carte sur internet lors des trois derniers mois mettant en œuvre un dispositif d'authentification non conforme à la SCA |
| Développement des dispositifs conformes SCA | Nombre de porteurs de carte enrôlés dans au moins un dispositif d'authentification conforme à la SCA lors d'un paiement par carte sur internet |
| | Nombre de paiements par carte sur internet lors des trois derniers mois mettant en œuvre un dispositif d'authentification conforme à la SCA |

b) Opérations sensibles sur la banque en ligne

| Suivi | Indicateurs |
|---|---|
| Tendance du SMS OTP | Nombre de clients utilisateurs de la BEL, d'un service d'initiation ou d'agrégation, enrôlés dans un dispositif d'authentification lors de l'exécution d'opérations sensibles (ordre de virement, ajout d'un bénéficiaire, renouvellement du jeton trimestriel d'accès aux comptes de paiement en ligne, etc.) |
| | Nombre de clients utilisateurs de la BEL, d'un service d'initiation ou d'agrégation, enrôlés dans un dispositif d'authentification non conforme à la SCA (et non enrôlés dans un dispositif conforme) lors de l'exécution d'opérations sensibles |
| | Nombre d'opérations sur la BEL, ou via un service d'initiation ou d'agrégation, lors des trois derniers mois |
| | Nombres d'opération sensibles sur la BEL, ou via un service d'initiation ou d'agrégation, lors des trois derniers mois requérant, au regard de la réglementation, une authentification forte du porteur |
| | Nombres d'opérations sensibles sur la BEL, ou via un service d'initiation ou d'agrégation, lors des trois derniers mois mettant en œuvre un dispositif d'authentification non conforme à la SCA |
| Développement des dispositifs conformes SCA | Nombre de clients utilisateurs de la BEL, d'un service d'initiation ou d'agrégation, enrôlés dans au moins un dispositif d'authentification conforme à la SCA lors de l'exécution d'opérations sensibles sur la BEL, ou via un service d'initiation ou d'agrégation |
| | Nombre d'opérations sensibles sur la BEL, ou via un service d'initiation ou d'agrégation, lors des trois derniers mois mettant en œuvre un dispositif d'authentification conforme à la SCA |

Note : SMS OTP *(one time password)* : message reçu sur un téléphone portable pour communiquer un code à usage unique ; SCA *(strong customer authentification)* : authentification forte du client.

continuera à être envoyé aux établissements bancaires deux fois par an à des fins de collecte de données et permettra de rendre compte des progrès réalisés sur les aspects suivants :

- la tendance baissière de l'utilisation des dispositifs non conformes à la nouvelle réglementation ;

- le développement des dispositifs d'authentification conformes à la nouvelle réglementation.

Pour ce faire, les indicateurs présentés dans le tableau *supra* seront reportés par les principaux établissements bancaires français et consolidés par la Banque de France. Par ailleurs, l'Observatoire veillera à ce que les acteurs du marché des paiements proposent des solutions adaptées et accessibles à l'ensemble de leurs clients, et notamment ceux dont l'équipement ou les habitudes de consommation constitueraient un frein à l'utilisation de technologies avancées.

## 1.3 Rythme de migration cible

Les objectifs de migration, figurant dans les graphiques 1 et 2, ont été

établis pour les trois prochaines années. Ils seront suivis lors des points d'étape et repris dans les synthèses publiées.

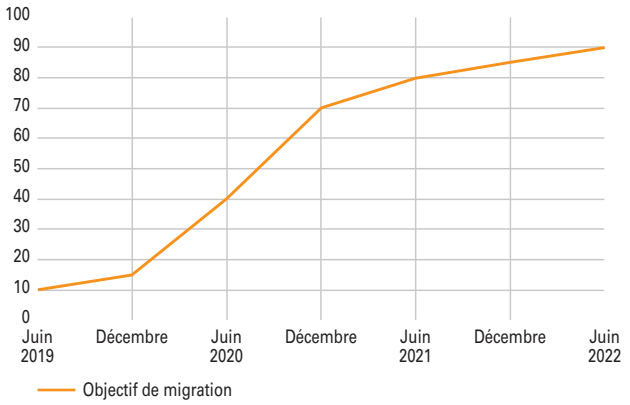
Les hypothèses suivantes sont utilisées lors de l'élaboration de cette montée en charge.

• L'équipement des clients en dispositifs conformes est un prérequis à une montée en charge des transactions authentifiées avec ces nouveaux moyens. Toutefois, dans un second temps, il est envisagé que les porteurs déjà équipés, plus habitués des transactions en ligne, génèrent plus de transactions que ceux n'ayant toujours pas migré, ce qui explique une croissance toujours soutenue de celles-ci en 2021 et après.

• Si le début de la migration est progressif, il s'accélérera sous l'effet des communications des acteurs et de la généralisation des nouveaux dispositifs auprès du grand public. Il est cependant attendu qu'à partir de 80 % de clients équipés, le rythme de migration ralentisse en raison des efforts plus importants à fournir pour enrôler la clientèle retardataire.

G1 Enrôlement des clients

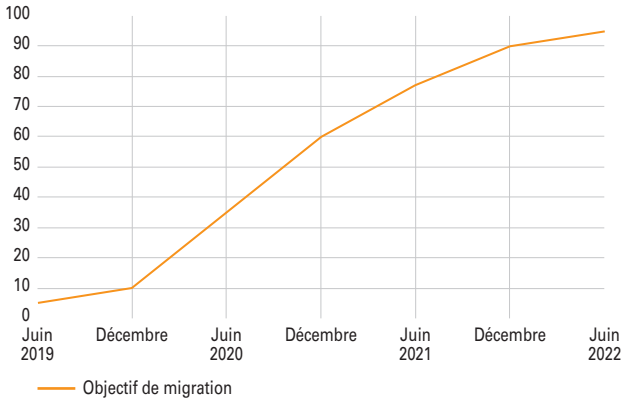
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G2 Authentification des paiements requérant une SCA

(en %)

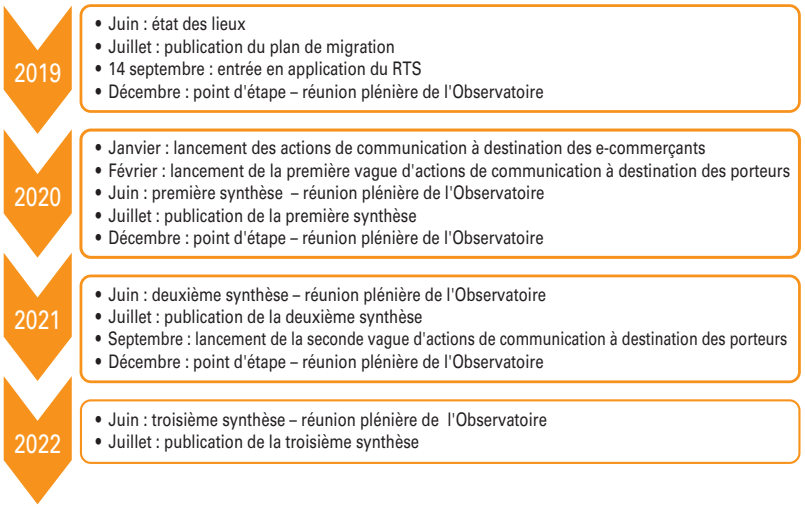



Note : SCA *(strong customer authentification)* : authentification forte du client.
Source : Observatoire de la sécurité des moyens de paiement.

• En conséquence, il conviendra de faire un point de situation en juin 2021 sur le résiduel des « clients utilisateurs de SMS OTP » afin de déterminer la meilleure démarche à suivre compte tenu des exigences réglementaires de la DSP2.

## 1.4 Plan de migration

L'Observatoire présentera un point d'étape lors des réunions plénières de 2019 qui auront lieu en juin et en décembre. La réunion de juin 2019 a permis de présenter le plan de migration retenu, pour publication au sein du rapport annuel, ainsi que la liste des principales technologies d'authentification forte conformes à DSP2 et mises en œuvre par les prestataires de services de paiement. Sur ce dernier point, l'EBA a publié le 21 juin un avis soutenu par les banquiers centraux et superviseurs européens reprenant les principales caractéristiques des dispositifs d'authentification forte conformes à la DSP2, illustrées d'exemples concrets, et invitant les acteurs à définir un plan de migration sous le contrôle des autorités nationales compétentes [1]. Un point d'avancement de cette migration sera publié dans les rapports annuels de l'Observatoire.




Note : RTS *(regulatory technical standard)* : norme technique réglementaire.

1 Cf. *https://eba.europa.eu*

Encadré 2

### Plan de communication

Les éléments de langage suivants sont proposés afin que les représentants de l'Observatoire puissent les utiliser dans leur communication. Ces éléments s'adressent ainsi aux prestataires de services de paiement, aux e-commerçants et à leurs clients.

#### Information des prestataires de services de paiement et e-commerçants

La réglementation européenne a mis en place des dispositions visant à renforcer la sécurité des paiements électroniques, notamment sur internet, et l'accès à des services de banque en ligne plus sûr. Ainsi, à partir du 14 septembre 2019, l'utilisation du seul code reçu par SMS pour authentifier ces opérations n'est plus suffisant et est progressivement renforcée au moyen d'un dispositif conforme à la nouvelle réglementation. Ces nouveaux dispositifs pourront par exemple reposer sur une application, pour *smartphone* ou carte SIM (compatible avec tous les mobiles), qui nécessite la saisie d'un code secret ou la vérification d'une donnée biométrique. Ces solutions sont choisies par les établissements bancaires et les prestataires de services de paiement, et proposées à leurs clients.

.../...

### Information des clients de prestataires de services de paiement et d'e-commerçants

[Ces éléments de langage sont destinés aux prestataires de services de paiement et e-commerçants pour être mis en avant sur leurs sites]

La réglementation européenne a mis en place des dispositions visant à renforcer la sécurité des paiements électroniques, notamment sur internet, et l'accès à des services de banque en ligne plus sûr. Ainsi, à partir du 14 septembre 2019, l'utilisation du seul code reçu par SMS pour authentifier ces opérations n'est plus suffisant et est progressivement renforcée au moyen d'un dispositif conforme à la nouvelle réglementation.

Pour plus de renseignements, veuillez vous adresser à votre établissement bancaire ou votre prestataire de services de paiement habituel.

### Information des porteurs de carte

La réglementation européenne a mis en place des dispositions visant à renforcer la sécurité des paiements à distance, notamment sur internet. Le dispositif actuel consistant en la saisie du seul code reçu par SMS pour valider un paiement par carte sur internet n'est ainsi plus suffisant.

[Votre nouveau dispositif d'authentification nécessitera / reposera sur ...]

### Information des utilisateurs de banques en ligne

La réglementation européenne a mis en place des dispositions visant à renforcer la sécurité de l'accès aux services de banque en ligne. Le dispositif actuel consistant en la saisie du seul code reçu par SMS pour sécuriser certaines opérations accessibles en ligne n'est ainsi plus suffisant.

[Votre nouveau dispositif d'authentification nécessitera / reposera sur ...]

### Information des consommateurs

La réglementation européenne a mis en place des dispositions visant à renforcer la sécurité des paiements électroniques, notamment sur internet, et l'accès à des services de banque en ligne plus sûr. Ainsi, à partir du 14 septembre 2019, l'utilisation du seul code reçu par SMS pour authentifier ces opérations n'est plus suffisant et est progressivement renforcée au moyen d'un dispositif conforme à la nouvelle réglementation.

Ces nouveaux dispositifs pourront par exemple reposer sur une application, pour *smartphone* ou carte SIM (compatible avec tous les mobiles), qui nécessite la saisie d'un code secret ou la vérification d'une donnée biométrique. Ces solutions sont choisies par les établissements bancaires et les prestataires de services de paiement, et proposées à leurs clients.

Pour plus de renseignements, veuillez vous adresser à votre établissement bancaire ou votre prestataire de services de paiement habituel.

# 2 État de la fraude en 2018

## AVERTISSEMENT

Du fait d'une interprétation erronée de la méthodologie de l'Observatoire par un établissement déclarant, certaines données présentées dans le chapitre 2 et dans l'annexe 6 diffèrent de celles publiées précédemment dans les rapports annuels de l'Observatoire. Ces corrections portent sur les données de la fraude nationale à la carte de paiement pour la période allant de 2015 à 2017 ; elles sont détaillées en annexe 6 du rapport. Dans le présent chapitre, ce sont donc les données corrigées qui sont reprises.

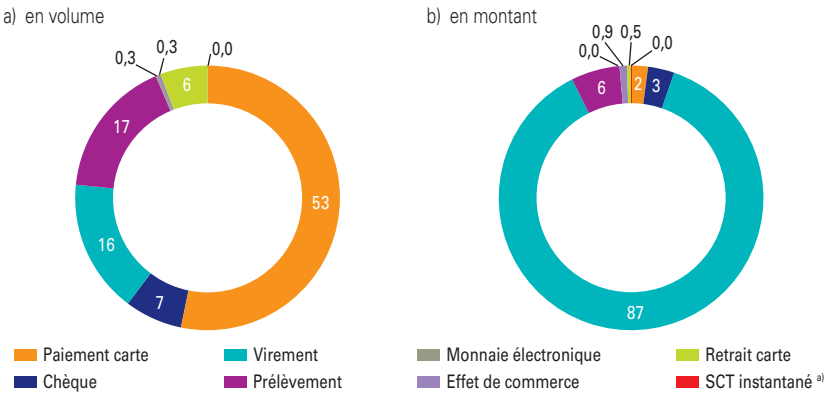
## 2.1 Vue d'ensemble

### Cartographie des moyens de paiement

En 2018, ce sont 24,7 milliards de transactions scripturales qui ont

G1 Usage des moyens de paiement scripturaux en France en 2018

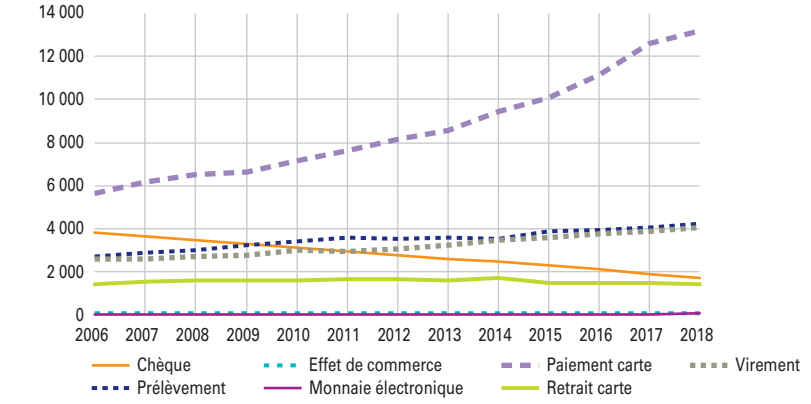
(en %)




a) SCT instantané (*SEPA instant credit transfer*) : virement instantané.
Source : Observatoire de la sécurité des moyens de paiement.

G2 Usage des moyens de paiement en France depuis 2006

(en millions d'opérations)

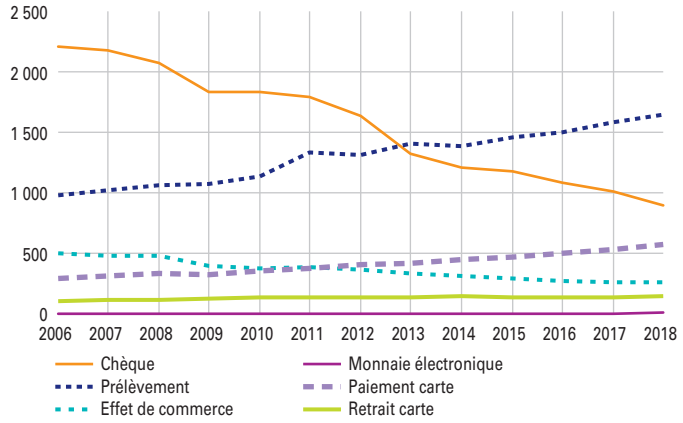



Source : Observatoire de la sécurité des moyens de paiement.

été réalisées par les clients (particuliers et entreprises) des banques et prestataires de services de paiement français pour un montant total de 27 704 milliards d'euros, ce qui représente une progression de 3 % du nombre de transactions et de 0,4 % des montants échangés par rapport à l'année 2017.

G3 Montant des transactions hors virements en France

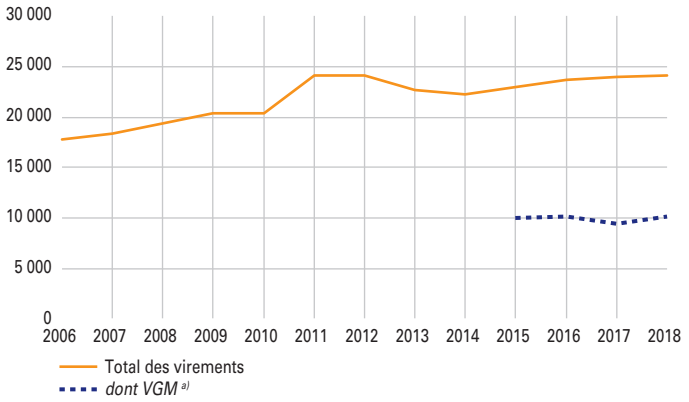
(en milliards d'euros)




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.

**Le paiement par carte** conserve sa place de mode de paiement privilégié des Français, qui l'ont utilisé dans 53 % des paiements scripturaux pour un montant total approchant 568 milliards d'euros en 2018. En complément, les retraits par carte ont représenté 1 439 millions d'opérations en 2018, pour un peu plus de 136 milliards d'euros.

**Le virement** reste l'instrument privilégié pour les paiements de montant élevé (paiements des salaires et pensions, paiements interentreprises, etc.) avec 87 % du montant total des transactions scripturales, comme en 2017. En nombre d'opérations, il conserve la troisième position (16 %), juste après la carte et le prélèvement. Les virements sont principalement nationaux (77 % de la part en montant des virements globaux), contre 23 % à destination de l'étranger (espace SEPA – *single euro payments area* – et en dehors). Plus d'un tiers des virements émis en montant (42 %) transitent via des infrastructures dédiées aux paiements de gros montant.

Ils correspondent exclusivement à des paiements interentreprises dont le montant moyen s'établit à un peu plus d'un million d'euros. Le solde correspond pour l'essentiel au virement SEPA, accessible tant à la clientèle professionnelle qu'aux particuliers, et dont le montant unitaire moyen est de 2 729 euros. Dans une moindre mesure, le solde comprend également d'autres formes de virement (notamment, les virements internationaux hors Union européenne).

**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 2018. Son utilisation est presque exclusivement nationale (99 %), les prélèvements SEPA transfrontaliers ne représentant qu'un pourcent de l'ensemble des flux émis.

Le déclin continu du **chèque**, observé depuis plusieurs années, s'est encore poursuivi en 2018, tant en nombre d'opérations (– 9 %) qu'en valeur (– 11 %), soit une émission de 1,7 milliard de chèques en 2018, pour un montant global de 891 052 milliards d'euros.

**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 (0,9 %), confirment une nouvelle fois le déclin observé depuis plusieurs années.

Enfin, bien que l'utilisation de la **monnaie électronique** soit encore marginale en 2018, elle affiche une légère hausse déjà amorcée en 2017, pour atteindre 65 millions de transactions (+ 18 %) et une valeur totale de 1 053 millions d'euros (+ 17 %) ; portée par le développement de solutions de paiements entre particuliers.

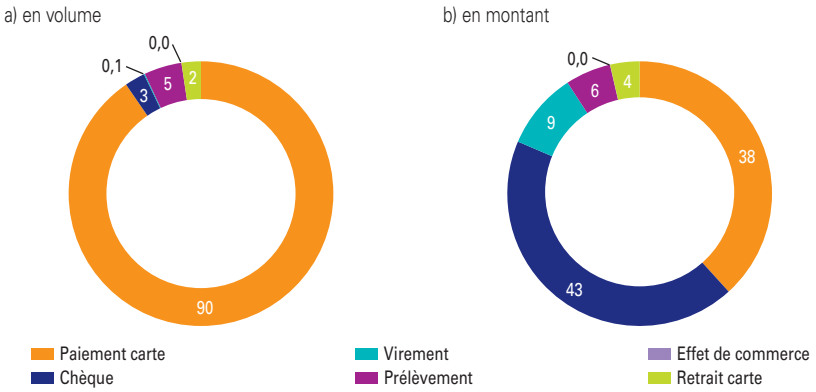
## Fraude aux moyens de paiement

En 2018, la fraude aux transactions scripturales représente un montant global de 1,045 milliard d'euros pour 6,7 millions de transactions frauduleuses, contre 771 millions d'euros et 5,1 millions de cas en 2017, soit une hausse significative de 36 % en montant.

Cette tendance est largement imputable au **chèque**, qui devient le moyen de paiement le plus fraudé en France ; la part de la fraude sur le chèque en montant représente 43,1 % de la fraude totale avec un montant annuel de fraude qui atteint 450 millions d'euros en 2018

G5 Répartition de la fraude sur les moyens de paiement scripturaux en 2018

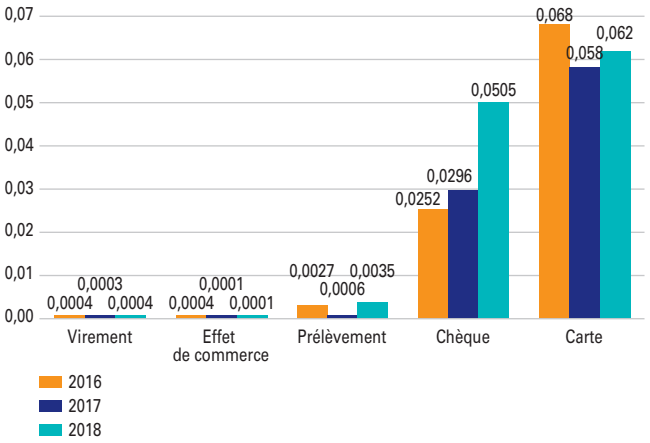
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G6 Évolution du taux de fraude par moyen de paiement, de 2016 à 2018

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

(contre 296 millions en 2017, soit + 52 %), et ce alors que son utilisation continue de décroître. Son taux de fraude s'établit à 0,0505 %, soit un euro de fraude pour 1 980 euros de paiement.

**La carte de paiement** [1] concentre 42,0 % de la fraude en montant (à hauteur de 38,4 % pour les paiements et de 3,6 % pour les retraits), soit 439 millions d'euros en cumulant les transactions de paiement et de retrait, et représente la quasi-totalité (92,4 %) du nombre de transactions frauduleuses. Après une baisse de deux années consécutives, le montant de fraude global sur les cartes émises en France, est en hausse en 2018 (439, contre 387 millions d'euros en 2017, soit + 13,4 % sur les transactions de paiement et de retrait effectuées en France et à l'étranger).

Ainsi, après plusieurs années de stagnation, le taux de fraude sur les opérations par carte progresse pour s'établir à 0,062 %, soit environ un euro de fraude pour 1 612 euros de transactions. 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 (0,173 %, soit un euro de fraude pour 578 euros de paiement), en dépit d'une nouvelle baisse remarquable de la fraude sur ce canal.

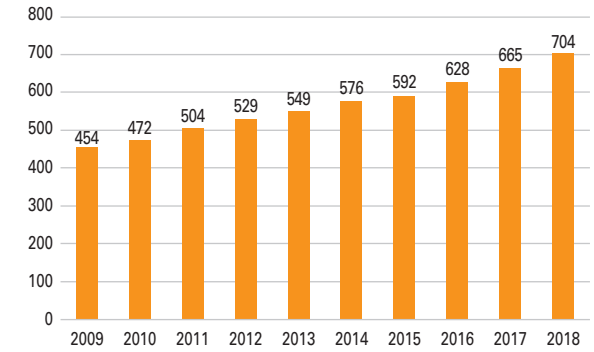
Bien que le montant annuel de fraude au **virement** soit toujours très inférieur à celui de la carte et du chèque (97 millions d'euros en 2018), une hausse est constatée par rapport à 2017 (où elle se situait à 78 millions d'euros, soit + 24 % sur un an). Néanmoins, son taux de fraude reste le plus faible parmi les moyens de paiement accessibles aux particuliers. Il s'établit à 0,0004 %, contre 0,0003 % en 2017, soit l'équivalent d'un euro de fraude pour 244 300 euros de paiement

**Le prélèvement** représente à nouveau le montant annuel de fraude le plus limité parmi les moyens de paiement scripturaux accessibles aux particuliers (58 millions d'euros en 2018), mais augmente très significativement (9 millions d'euros en 2017, soit + 544 %). Son taux de fraude connaît ainsi une forte hausse pour s'établir à 0,0035 % (contre 0,0006 %

1 Cartes émises en France.

G7 Montant total des transactions des cartes françaises

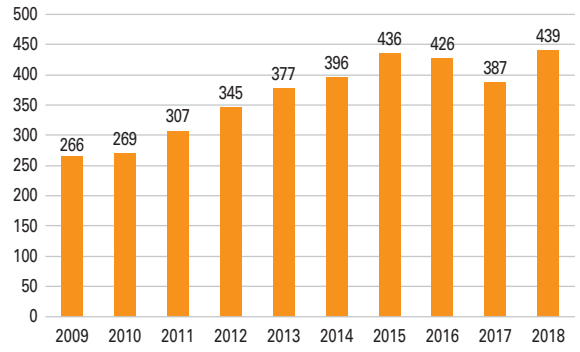
(en milliards d'euros)




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.

Encadré 1

## 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 2018 portent ainsi sur :

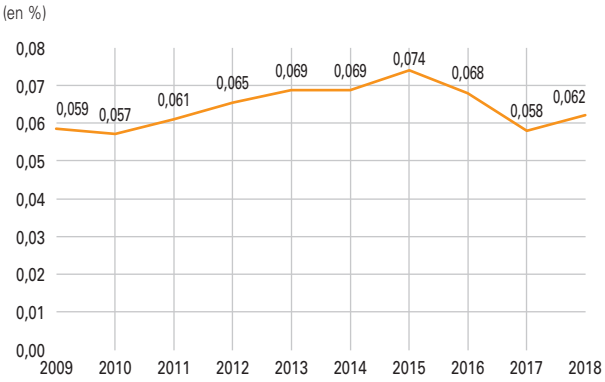
- 683,7 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 79 millions de cartes de type « interbancaire » émises en France (dont 58 millions de cartes sans contact) ;
- 20,8 milliards d'euros de transactions réalisées (principalement en France) avec 9,8 millions de cartes de type « privatif » émises en France ;
- 55,9 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.

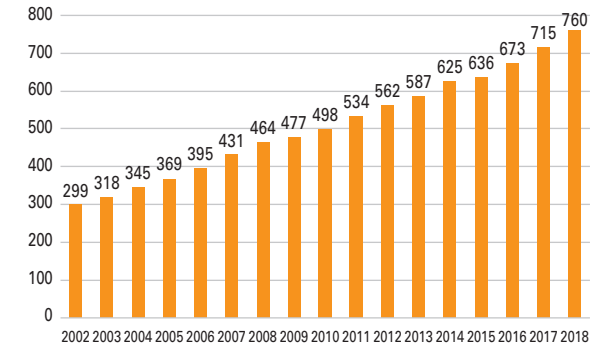
1 Les systèmes de paiement par carte dits « interbancaires » correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. À l'inverse, les systèmes privatifs sont ceux pour lesquels il existe un nombre réduit de prestataires de services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

G9 Taux de fraude des cartes françaises



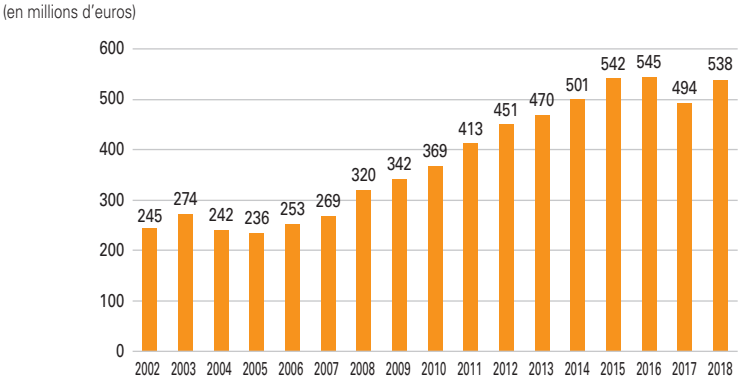

Source : Observatoire de la sécurité des moyens de paiement.

G10 Montant des transactions traitées dans les systèmes français, cartes françaises et étrangères




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




Source : Observatoire de la sécurité des moyens de paiement.

en 2017), soit l'équivalent d'un euro de fraude pour 28 185 euros de prélèvements émis.

Enfin, les **effets de commerce** restent relativement épargnés par la fraude, avec un montant de l'ordre de 226 000 euros en 2018 pour cinq cas de fraude, et un taux de fraude de 0,0001 % équivalent à un euro de fraude pour plus de 1 115 000 euros de paiement.

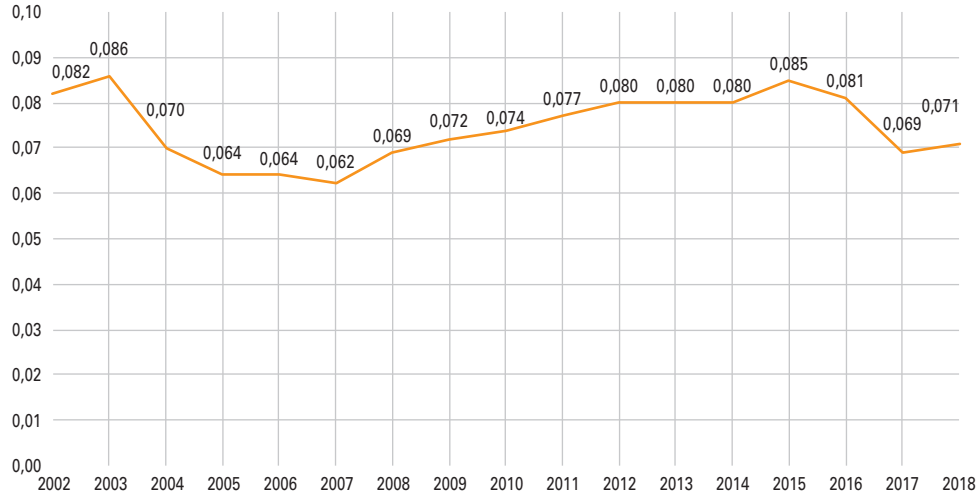
## 2.2 État de la fraude sur le paiement et le retrait par carte

### Vue d'ensemble

Après un recul en 2017, la fraude sur les transactions de paiement et de retrait effectuées en France et à l'étranger avec des cartes françaises est en augmentation en 2018 (+ 13,4 % par rapport à 2017) et s'élève à 439 millions d'euros pour un montant total de transactions de 704,4 milliards d'euros, en augmentation de 5,9 % par rapport à 2017.

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

(en %)



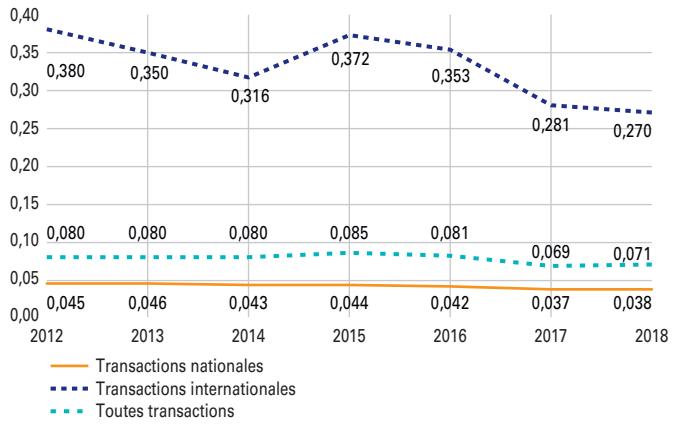

Source : Observatoire de la sécurité des moyens de paiement.

En conséquence, le taux de fraude sur les cartes de paiement françaises se dégrade très légèrement et s'établit désormais à 0,062 %, contre 0,058 % en 2017 (cf. graphique 9), ce qui représente l'équivalent d'un euro de fraude pour 1612 euros de transactions. En tenant compte également de la fraude enregistrée sur les transactions réalisées en France avec des cartes émises dans d'autres pays, la même tendance est observée avec une progression de 8,9 % du montant total de la fraude par rapport à 2017. Celui-ci s'élève à 538 millions d'euros en 2018, pour un montant total de transactions atteignant 760 milliards d'euros, en progression de 6,3 % par rapport à 2017.

Sur la base de ces éléments, le taux de fraude global sur les transactions

G13 Taux de fraude par zone géographique

(en %)




Source : Observatoire de la sécurité des moyens de paiement

par carte traitées dans les systèmes monétiques français, comprenant 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, augmente très légèrement à 0,071 %, contre 0,069 % en 2017 (cf. graphique 12), ce qui représente l'équivalent d'un euro de fraude pour 1 412 euros de transactions.

Enfin, le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2018 s'élève à 1 358 819, ce qui représente une progression de 12 % par rapport à 2017. Toutefois, cette hausse ne s'est pas accompagnée d'une augmentation du montant unitaire des transactions frauduleuses puisque celui-ci reste quasiment stable à 70,5 euros en 2018, contre 69,8 euros en 2017. 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.) conduisant à la détection et désactivation plus rapides des cartes compromises et contraignant ainsi les fraudeurs à devoir multiplier les tentatives de fraude, tout en réduisant leur montant unitaire pour tenter d'échapper aux mécanismes de détection.

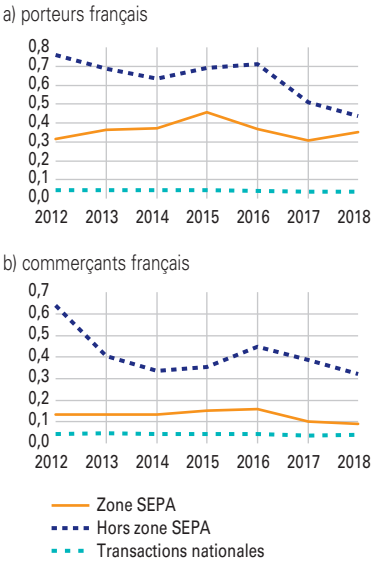
## Répartition de la fraude par zone géographique

Après une année de baisse en 2017, la fraude sur les transactions nationales s'est accrue de 8,4 % en 2018. Le montant de la fraude sur les transactions de paiement et de retrait effectuées en France avec des cartes françaises s'établit à 245,6 millions d'euros cette année, contre 226,5 millions d'euros en 2017. Toutefois, sous l'effet de la croissance des transactions nationales (+ 5,2 % en valeur par rapport à 2017), le taux de fraude reste à un niveau relativement bas, quasiment identique à celui de 2017, soit à 0,038 % (contre 0,037 % en 2017), ce qui représente l'équivalent d'un euro de fraude pour environ 2 600 euros de transactions.

En ce qui concerne les transactions internationales [2], la fraude est également en progression de 9,2 % en 2018, avec un montant total de fraude s'élevant à 291,9 millions d'euros, et résulte largement de la dynamique des transactions internationales qui affichent une croissance de 13,4 % en valeur par rapport à 2017. On constate donc une meilleure maîtrise de la fraude sur les transactions internationales avec un taux de fraude qui ressort en baisse à 0,270 %, contre 0,281 % en 2017, soit à son plus bas niveau historique. Toutefois, il est à noter que ce taux de fraude demeure toujours élevé au regard du montant

G14 Taux de fraude par zone géographique

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

2 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.

Encadré 2

## Fraude aux paiements sans contact

Les paiements sans contact ont continué de progresser à un rythme très important au niveau national avec une augmentation de 82 % en volume et de 89 % en valeur. Ainsi, sur l'ensemble de l'année 2018, ce sont 2,3 milliards de paiement sans contact qui ont été réalisés (contre 1,2 milliard en 2017) pour un montant total de 24,4 milliards d'euros (contre 12,9 milliards d'euros en 2017). Cela représente 6 % en valeur et 21 % en volume des transactions de paiement de proximité, soit un paiement par carte sur cinq. Le montant moyen d'un paiement sans contact s'établit à 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, leur montant total s'élève à 25,8 milliards d'euros pour 2,4 milliards d'opérations soit une progression sur un an de 87 % en valeur et de 82 % en volume.

Cette évolution s'est accompagnée d'une confirmation de la stabilité du taux de fraude sur les transactions nationales à 0,020 %, avec un montant total de fraude de près de 5 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 (0,024 %), bien en-deçà de celui des paiements à distance (0,173 %). 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-identique à celui de 2017, soit à 0,021 %.

En 2018 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 généralement fixé au maximum à 30 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (cumul généralement fixé à 100 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 par terminaux de téléphonie mobile, dont l'usage progresse également, bien que leur part dans les transactions de proximité demeure encore marginale (0,10 % des transactions nationales de proximité). En 2018, les transactions nationales par équipements de téléphonie mobile représentent ainsi 10,9 millions d'opérations, soit près de deux fois et demie de plus qu'en 2017, et un montant total de près de 190,9 millions d'euros, contre 83,5 millions d'euros en 2017. 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 près de 219,6 millions d'euros pour 12,4 millions d'opérations.

En 2018, des cas de fraude ont été enregistrés sur des transactions nationales par équipements de téléphonie mobile, pour un montant total toutefois peu significatif (moins de 50 000 euros) et un taux de fraude de 0,03 %. La fraude sur le paiement mobile, toutes zones confondues, s'établit à 0,04 %, contre 0,03 % en 2017 pour un montant total de fraude d'un peu moins de 88 000 euros.

Encadré 3

## 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.

### Répartition de la fraude par secteur d'activité

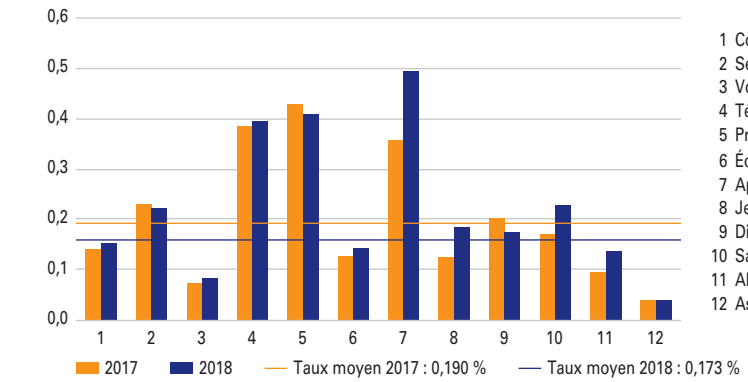
(montant en millions d'euros, part en pourcentage)

| | | Montant | Part |
|---|---|---|---|
| 1 | Commerce généraliste et semi-généraliste | 39,2 | 22,6 |
| 2 | Services aux particuliers et aux professionnels | 38,8 | 22,4 |
| 3 | Voyage, transport | 25,7 | 14,9 |
| 4 | Téléphonie et communication | 24,5 | 14,1 |
| 5 | Produits techniques et culturels | 13,2 | 7,6 |
| 6 | Équipement de la maison, ameublement, bricolage | 8,8 | 5,1 |
| 7 | Approvisionnement d'un compte, vente de particulier à particulier | 7,4 | 4,3 |
| 8 | Jeu en ligne | 5,3 | 3,1 |
| 9 | Divers | 5,3 | 3,1 |
| 10 | Santé, beauté, hygiène | 2,3 | 1,3 |
| 11 | Alimentation | 2,2 | 1,2 |
| 12 | Assurance | 0,6 | 0,3 |
| **Total** | | **173,3** | **100,0** |

Les secteurs « Commerce généraliste et semi-généraliste », « Services aux particuliers et aux professionnels », « Voyage, transport » et « Téléphonie et communication » demeurent toujours les plus exposés, concentrant à eux seuls 74 % du montant total de la fraude en vente à distance. La comparaison des taux de moyens de chacun des secteurs d'activité permet de constater que les secteurs « Approvisionnement d'un compte, vente de particulier à particulier », « Produits techniques et culturels » et « Téléphonie et communication », 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 infra).

### Taux de fraude en vente à distance par secteur d'activité, transactions nationales

(en %)




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

Source : Observatoire de la sécurité des moyens de paiement.

des opérations concernées puisque les transactions internationales représentent 54 % du montant total de la fraude alors qu'elles ne comptent que pour 14 % de la valeur totale des transactions.

Par ailleurs, selon les zones géographiques, on observe :

• pour les cartes françaises, une légère augmentation du taux de fraude sur les opérations réalisées au sein de la zone SEPA [3] qui passe de 0,308 % en 2017 à 0,352 % en 2018, mais qui reste toutefois en-deçà de celui des transactions réalisées hors de l'espace européen SEPA, en diminution en 2018, à 0,438 % (contre 0,511 % en 2017) ;

• pour les cartes étrangères, une diminution du taux de fraude sur les transactions effectuées en France avec des cartes émises hors de l'espace européen SEPA (0,323 %), bien que demeurant à un niveau élevé, soit trois fois et demie supérieur à celui des transactions réalisées en France avec des cartes émises au sein de la zone SEPA (0,092 %).

3 La zone SEPA comprend les 28 pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande et Saint-Martin.

## Répartition de la fraude par type de transaction

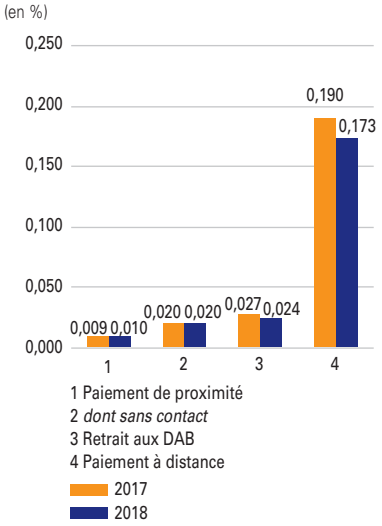
### Fraude sur les transactions nationales

Bien que le montant de la fraude sur les transactions nationales ait progressé en 2018, les taux de fraude des différents types de transaction se sont améliorés à l'exception de celui des paiements de proximité et sur automate qui se dégrade très légèrement.

En effet, selon les différents types de transaction, on observe les faits suivants.

• Pour les paiements de proximité et sur automate et en dépit de l'augmentation de la fraude en 2018, le taux de fraude reste à un niveau très faible, quasiment identique à celui de 2017, soit à 0,010 % (contre 0,009 % en 2017). La hausse observée est en partie imputable à la croissance des paiements sans contact, dont le taux de fraude est sensiblement plus élevé (cf. encadré 2 *supra*). Les paiements de proximité et sur automate représentent toujours une part importante du montant des transactions nationales, près des deux tiers, pour seulement 17 % du montant de la fraude nationale.

G15 Comparaison des taux de fraude par type de transaction, transactions nationales



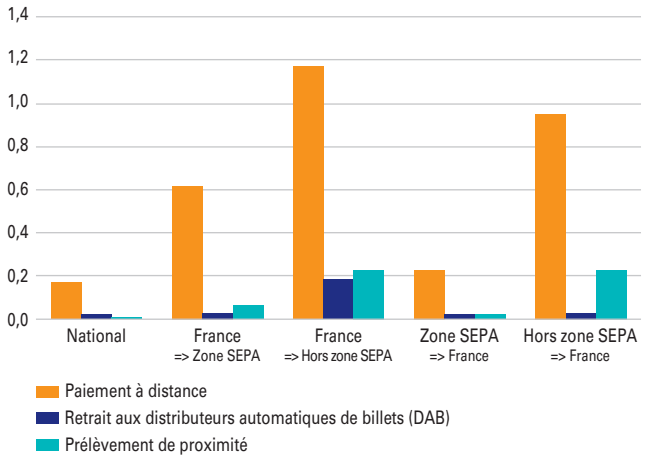

Source : Observatoire de la sécurité des moyens de paiement.

• Pour les paiements à distance, malgré l'augmentation du montant de la fraude en 2018, le taux de fraude s'inscrit à nouveau en baisse, pour la septième année consécutive à 0,173 %, contre 0,190 % en 2017 sous l'effet d'une forte croissance des transactions à distance (22 % en valeur par rapport à 2017). 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 (tel 3D-Secure), ainsi que des outils d'analyse de risque et de *scoring* des transactions, c'est-à-dire des systèmes experts 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 % du montant total), avec un taux de fraude qui reste supérieur de dix-sept fois à celui sur les paiements de proximité. 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 (DSP2), avec notamment l'application au 14 septembre 2019 des dispositions généralisant l'authentification renforcée et l'analyse des transactions à risque, devrait permettre une réduction de la fraude sur les paiements en ligne.

G16 Taux de fraude par type de transaction et origine géographique

(en %)




Note de lecture : Cf. annexe 5.
Source : Observatoire de la sécurité des moyens de paiement.

• Pour les retraits, le mouvement de baisse de la fraude amorcé en 2015 s'est poursuivi en 2018 avec un taux de fraude qui s'établit à 0,024 %, contre 0,027 % en 2017.

**Fraude sur les transactions internationales**

Si la fraude sur les transactions internationales est repartie à la hausse en 2018, les évolutions sont contrastées selon les types de transaction et les zones géographiques, mais on continue à observer une meilleure maîtrise de la fraude sur les transactions réalisées avec la zone SEPA que sur celles effectuées avec les pays situés hors de la zone SEPA en raison 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) [4] et pour renforcer la sécurité des paiements sur internet [5] :

• pour les cartes françaises, la hausse de la fraude sur les transactions effectuées au sein de l'espace européen SEPA est imputable aux transactions sur Internet dont le montant de la fraude qui s'élevait à 74,4 millions d'euros passe à 118 millions d'euros en 2018 avec un taux de fraude s'établissant à 0,594 % (contre 0,527 % en 2017) soit à un niveau trois fois et demie supérieur à celui pour ce

4 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 & PIN* ».

5 Les orientations de l'Autorité bancaire européenne visant au renforcement de la sécurité des paiements sur internet sont entrées en vigueur en août 2015.

Encadré 4

## Indicateurs des services de police et de gendarmerie

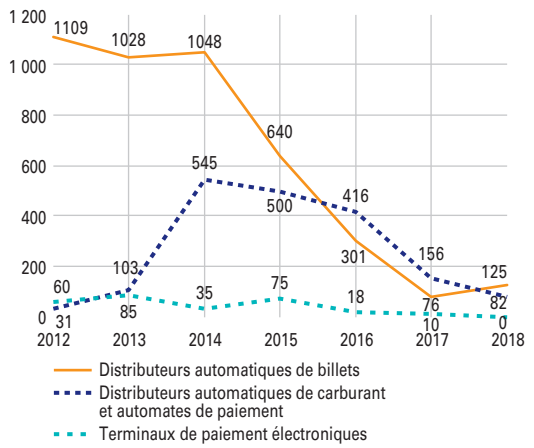
Le nombre de piratages de distributeurs automatiques de billets (DAB) a augmenté en 2018 avec 125 cas recensés, contre 76 l'an passé, mais celui-ci reste à un niveau relativement modéré eu égard à ceux constatés avant 2017. En 2018, il est observé une intensification des compromissions de DAB par la technique du « *jackpotting* » ainsi qu'une diversification des 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*.

À l'inverse, les attaques de distributeurs automatiques de carburant (DAC) sont en baisse avec 64 cas recensés en 2018 (contre 121 cas en 2017) et il en est de même pour les automates de paiement (tels les bornes de parking) dont le nombre de piratages s'élève cette année à 18 (contre 35 cas en 2017). En revanche, aucune compromission de terminaux de paiement chez les commerçants n'a été constatée.

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 est peu déployée, 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.

type transaction au niveau national. À l'inverse, on observe une amélioration de la fraude sur les transactions réalisées en dehors de l'espace européen SEPA (50,3 millions d'euros, contre 60,3 millions d'euros en 2017) avec un taux de fraude à 0,438 % (contre 0,511 % en 2017) mais la fraude sur les paiements à distance, quant à elle, a progressé avec un niveau de fraude relativement élevé (1,168 %) ;

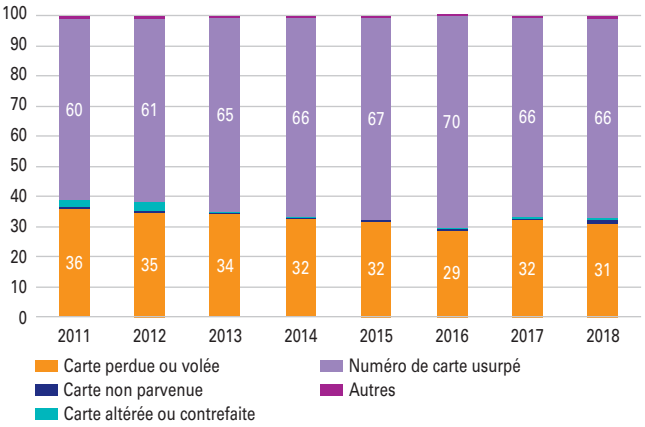
• pour les cartes étrangères ayant réalisé des transactions en France, les taux de fraude sont en amélioration que ce soit pour celles émises au sein de la zone SEPA (0,092 %, contre 0,102 % en 2017) ou en dehors (0,323 %, contre 0,386 % en 2017) mais on continue à observer un taux de fraude élevé (0,947 %) pour les paiements à distance effectués avec des cartes émises hors de l'espace européen SEPA.

## Répartition de la fraude par typologie

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux reste toujours la principale

G17 Répartition de la fraude aux paiements par carte selon la typologie de fraude

(en %)




Note : Transactions nationales hors retraits, en valeur.
Source : Observatoire de la sécurité des moyens de paiement.

origine de la fraude (66 % en montant). Les techniques de fraude les plus utilisées en 2018 pour usurper les numéros de cartes demeurent celles de l'hameçonnage *(phishing)*[6], et des logiciels malveillants *(malwares)* [7]. La perte ou le vol de carte demeure la deuxième origine de la fraude et représente près du tiers de la fraude sur les transactions nationales (31 %).

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 de la sécurité des cartes à puce EMV existantes.

## Suivi du déploiement de solutions d'authentification

Le développement du commerce en ligne a entraîné un usage croissant de la carte pour les paiements à distance, configuration dans laquelle l'impossibilité de recourir à la sécurité embarquée physiquement dans la carte (lecture de la puce et saisie du code confidentiel) nécessite la mise en œuvre d'autres mécanismes de sécurisation des transactions. Dans ce contexte et afin de renforcer la sécurité des paiements à distance, l'Observatoire de la sécurité des cartes de paiement a émis dès 2008 des recommandations visant à généraliser la mise en œuvre de dispositifs d'authentification forte du porteur. Ces recommandations font l'objet d'un suivi statistique depuis 2011.

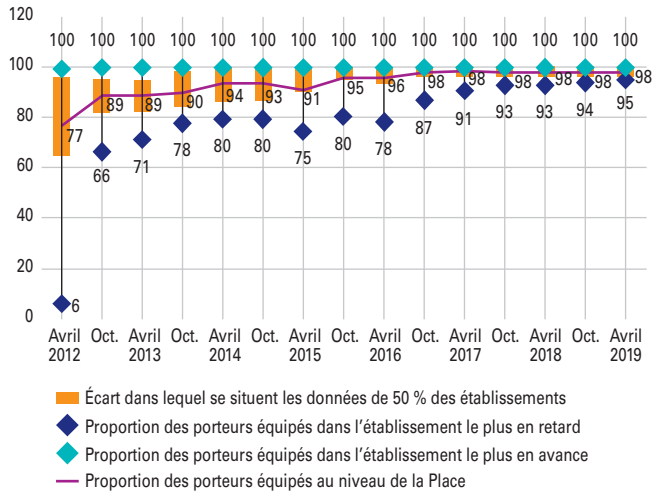
Pour la période de novembre 2018 à avril 2019, le suivi statistique du déploiement des solutions d'authentification réalisé par l'Observatoire auprès des principaux établissements bancaires porte sur un volume de 66,7 millions de cartes de paiement et 61,2 milliards d'euros de transactions en valeur (dont 26,4 milliards d'euros sécurisés par le dispositif « 3D-Secure ») permettant de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification.

6 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.

7 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* », 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.

G18 Distribution du taux d'équipement des porteurs en dispositif d'authentification

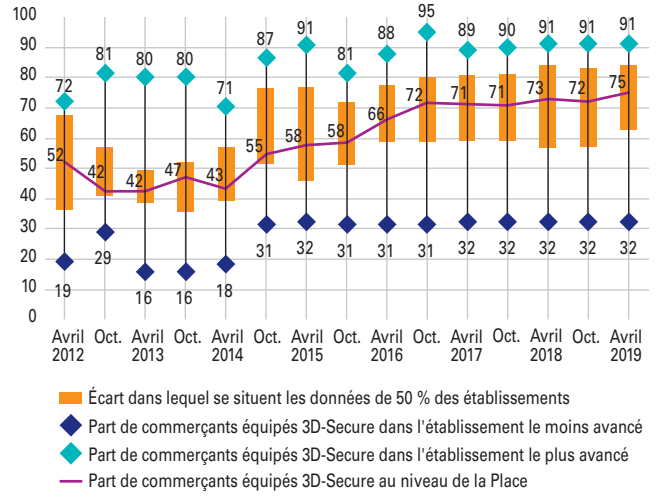
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G19 Distribution du taux d'équipement des commerçants en dispositif 3D-Secure

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

À fin avril 2019, l'équipement des porteurs en solutions d'authentification forte est généralisé, avec un taux moyen d'enrôlement qui s'établit à 98,4 %, permettant ainsi de couvrir la totalité des porteurs susceptibles de réaliser des transactions sur internet. Du côté des e-commerçants, si le taux d'équipement en dispositif 3D-Secure continue à progresser avec un taux moyen qui ressort à 75 %, on observe toutefois une grande disparité entre établissements bancaires, avec des taux compris entre 32 % et 91 %. Il est rappelé que l'équipement des e-commerçants en dispositif d'authentification forte constitue un point de conformité à la deuxième directive européenne sur les services de paiement (DSP2).

L'Observatoire constate que le taux d'échec sur les transactions authentifiées, qui s'établit à 11 %, demeure maitrisé et reste très inférieur à celui des transactions non authentifiées, ce qui permet de souligner la bonne appropriation de ces dispositifs par les particuliers. Cela reflète également la plus grande efficacité des contrôles réalisés sur les sites équipés de l'authentification, laquelle pousse les fraudeurs à privilégier par défaut

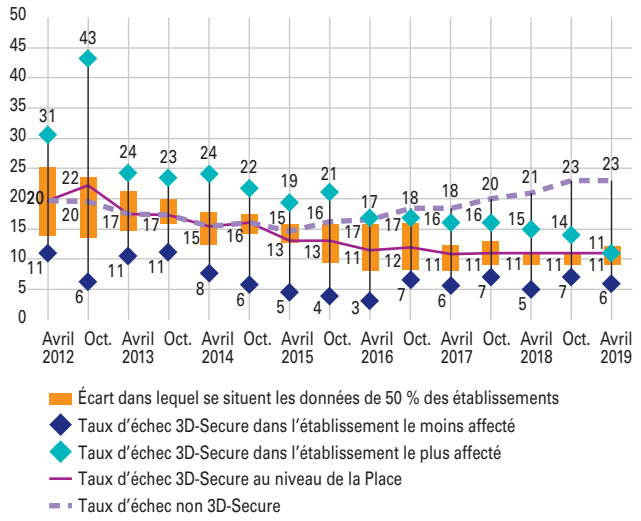
des sites non équipés. L'intérêt de l'utilisation du dispositif 3D-Secure en ressort donc affirmé pour les e-commerçants puisque les transactions non sécurisées connaissent un taux d'échec régulièrement en hausse.

Compte tenu de ces différentes évolutions favorables au développement du recours à des dispositifs d'authentification, la proportion de paiements en ligne authentifiés 3D-Secure poursuit une progression continue depuis 2011, pour atteindre 43 % des montants de paiement par carte à distance à fin avril 2019.

Le taux de fraude sur les transactions nationales authentifiées par le protocole 3D-Secure ressort à 0,07 % pour l'année 2018, quasi identique à celui de 2017 (à 0,06 %). Ce niveau est plus proche du taux de fraude observé sur la totalité des transactions nationales y compris de proximité (0,038 %), que du taux de fraude sur l'ensemble des paiements à distance (0,173 %). Cette hiérarchie des taux de fraude conforte la stratégie de recours à l'authentification du porteur promue depuis 2008 par l'Observatoire et qui fait aujourd'hui partie des exigences en matière de sécurité inscrites dans la deuxième directive sur les services de paiement, en application depuis janvier 2018 dans l'ensemble de l'Union européenne. Sur ce point, il est rappelé que dans son Opinion sur l'implémentation des RTS (*regulatory technical standards*) publiée le 13 juin 2018, l'Autorité bancaire européenne

G20 Distribution du taux d'échec 3D-Secure

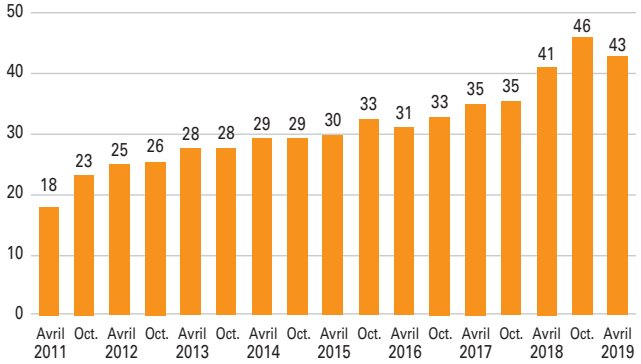
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G21 Part du montant total des paiements en ligne authentifiés par 3D-Secure

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

(ABE) a considéré que la solution d'authentification des paiements par carte sur internet par SMS-OTP (*one time password*), largement déployée en France, n'était pas compatible avec les requis de la DSP2. Afin d'accompagner la Place française à la mise en œuvre coordonnée des dispositions visant à l'authentification forte telle que définie dans la DSP2, l'Observatoire a défini une feuille de route, présentée au chapitre 1 de ce rapport, précisant les modalités de cette migration, tant du point de vue technique que de l'accompagnement des acteurs, des commerçants et des consommateurs.

## 2.3 État de la fraude sur le chèque

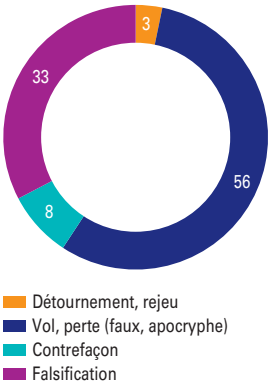
### Vue d'ensemble

Depuis trois années consécutives, le chèque connaît une hausse des montants fraudés, lesquels atteignent 450 millions d'euros en 2018, ce qui représente une progression annuelle de 52 %. Par conséquent, dans un contexte de diminution des flux de paiement par chèque, le taux de fraude enregistre une hausse significative : il est à 0,0505 %, contre 0,0296 % en 2017. Ces données placent le chèque comme premier moyen de paiement le plus fraudé avant la carte de paiement (respectivement 43,1 % et 42,0 % en montant), pour une utilisation pourtant beaucoup moins intensive. En effet, le chèque n'est que le quatrième moyen de paiement scriptural en nombre de paiements annuel, et est ainsi utilisé 8,5 fois moins souvent que la carte. Le montant moyen d'un chèque fraudé remis à l'encaissement est également en légère progression, soit à 2 704 euros, contre 2 577 euros en 2017.

Le renforcement du traitement manuel des données de fraude a permis de mieux qualifier les cas de fraude rencontrés. Ainsi, comme en 2017, deux catégories de fraude concentrent la majeure partie des montants fraudés en 2018 : d'une part, l'utilisation frauduleuse de chèques perdus ou volés, en forte

G22 Répartition de la fraude par chèque en montant par typologie de fraude

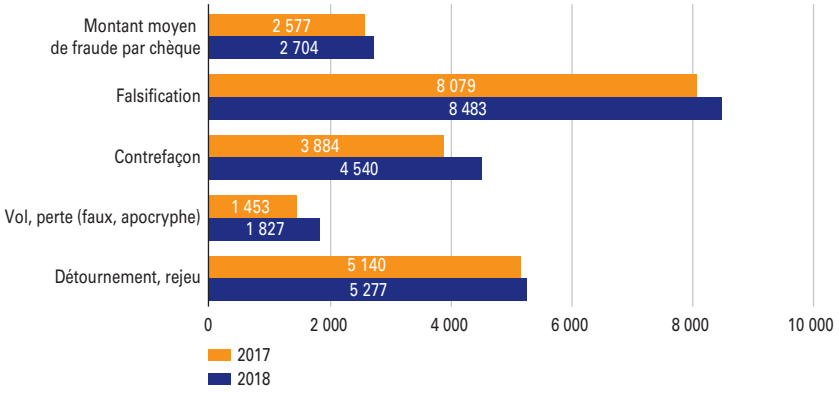
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G23 Montant unitaire de fraude par chèque, par typologie de fraude, 2017–2018

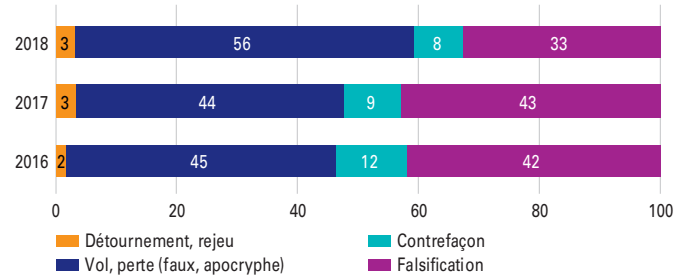
(en euros)




Source : Observatoire de la sécurité des moyens de paiement.

G24 Répartition de la fraude par chèque en montant, par typologie de fraude, de 2016 à 2018

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

augmentation par rapport à 2017 (56 % du total de la fraude sur le chèque, contre 44 % un an auparavant), et d'autre part la falsification d'un chèque régulièrement émis (33 %). La fraude par contrefaçon de chèques et celle par détournement ou rejeu continuent de s'inscrire à des niveaux bien moindres (respectivement 8 % et 3 % de la fraude au chèque).

| 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 :<br>• 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,<br>• lors de la remise en agences bancaires, les fraudeurs utilisent des pièces d'identité volées ou falsifiées pour se faire remettre un chéquier.<br>**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.<br>**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.<br>**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 :<br>• en substituant, par grattage ou gommage, le nom du bénéficiaire légitime inscrit avec une encre faible,<br>• en réécrivant un nom de bénéficiaire sur celui du bénéficiaire légitime,<br>• 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,<br>• 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.<br>**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

La fraude au chèque se caractérise par une progression des montants unitaires, soit 8 483 euros pour les chèques falsifiés, 4 540 euros pour les chèques contrefaits, 1 827 euros pour les chèques volés ou perdus, et enfin 5 277 euros pour les chèques détournés ou rejoués.

Dans ce contexte, l'Observatoire réitère ses recommandations, reprises ci-dessous et au sein de l'étude présentée au chapitre 3 de ce rapport, dédiée aux moyens de paiement non connectés.

## 2.4 État de la fraude sur le virement

### Vue d'ensemble

En 2018, le montant total de la fraude sur les virements émis depuis un compte tenu en France s'élève à près de 97 millions d'euros, soit une en hausse de 24 % par rapport à 2017. Cette hausse a un effet sur le taux de fraude en montant pour ce moyen de paiement qui retrouve son niveau de 2016 à 0,0004 %. Ces données confirment que le virement reste le moyen de paiement scriptural le moins fraudé en proportion, alors qu'il est celui qui véhicule les montants globaux les plus importants (87 % du total des paiements scripturaux émis en France). Le montant moyen d'un virement frauduleux s'établit à 12 586 euros, soit un montant en baisse par rapport à 2017 (16 864 euros).

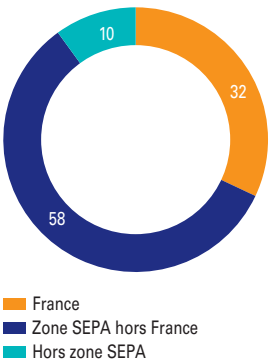
Les virements transfrontaliers subissent en proportion une fraude plus importante que les virements nationaux, et représentent près de 68 % des montants fraudés alors que les transactions transfrontalières ne comptent que pour 23 % des virements émis en montant.

Les travaux méthodologiques de catégorisation des virements frauduleux menés en 2017 permettant d'assurer une meilleure comptabilisation des données (cf. annexe 6) et confirment que le faux virement, c'est-à-dire l'émission d'un ordre de virement par le fraudeur au moyen d'attaques informatiques, reste le type de fraude prédominant (52 % du montant total de la fraude aux virements, contre 54 % en 2017), suivi par le détournement (41 %, contre 42 % en 2017).

La répartition de la fraude au virement reste relativement équilibrée entre les différents canaux d'utilisation de ce moyen de paiement : l'initiation de virement depuis l'espace de banque en ligne (sur internet ou via une application mobile) reste le canal le plus touché (42 % des montants fraudés en valeur en 2018, contre 38 % en 2017), le solde étant réparti entre les canaux télématiques sécurisés (37 %, contre 31 % en 2017) et les virements sur support papier (courrier, fax, etc.), qui affichent une baisse significative (22 % des montants fraudés, contre 31 % en 2017). Toutefois, compte tenu d'un usage désormais très limité du support papier, qui représente moins de 10 % des émissions de virements en montant, le taux de fraude sur les ordres de virement papier ressort en légère baisse à 0,0010 %, contre 0,0011

G25 Répartition de la fraude au virement en montant, par zone géographique

(en %)

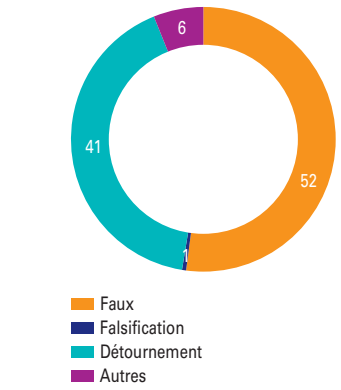



Source : Observatoire de la sécurité des moyens de paiement.

| Cas de fraude rencontrés | Mesures de prévention |
|---|---|
| En 2018, la fraude de type **détournement au moyen de techniques d'ingénierie sociale** a revêtu essentiellement les formes exposées ci-après.<br>• **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.<br>• **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.<br>• **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.<br>• **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.<br>**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.<br>• ***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.<br>• ***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.<br>**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.<br>**Fixation de plafonds maximaux de virements** sur le site de banque en ligne.<br>**Mise à disposition aux clients de solutions informatiques de sécurisation** permettant la recherche d'infections de type *malware* sur les postes de la clientèle.<br>**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.<br>**Actions d'information et de sensibilisation** menées par les banques et les prestataires de services de paiement auprès des particuliers. |

G26 Répartition de la fraude au virement en montant, par typologie de fraude

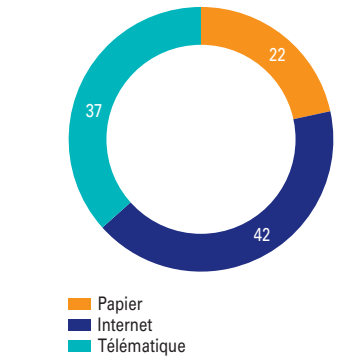
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G27 Répartition de la fraude au virement en montant, par canal d'initiation

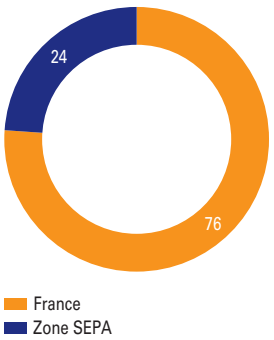
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

G28 Répartition de la fraude au prélèvement en montant, par zone géographique

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

en 2017, soit un niveau supérieur à celui des virements émis via un canal électronique (0,0004 %).

### Principaux cas de fraude en 2017 et mesures de prévention

Les principales techniques de fraude sur le virement constatées en 2018 sont, comme en 2017, la fraude par ingénierie sociale [8] et les attaques informatiques par *malware* et *phishing*. Ainsi, l'inversion de tendance du nombre de cas de *phishing* en baisse en 2016, qui fut constatée en 2017, s'est encore poursuivie en 2018. L'amélioration des dispositifs de détection des attaques informatiques doit donc être accrue afin de contrer les fraudeurs dont les mails de plus en plus perfectionnés peuvent plus facilement tromper les clients titulaires de comptes.

## 2.5 État de la fraude sur le prélèvement

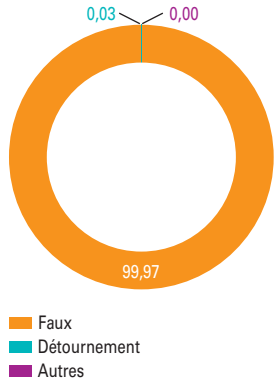
### Vue d'ensemble

En 2018, les prélèvements frauduleux émis au débit d'un compte tenu en France se sont chiffrés en montant à 58 millions d'euros, contre près de 9 millions d'euros en 2017 et 40 millions en 2016, soit une hausse conséquente (544 %) des montants fraudés qui se rapprochent des proportions constatées en 2016 et qui avaient été suivies par une baisse significative de 78 % de 2016 à 2017. Ainsi, dans un contexte de croissance des flux de paiement, le taux de fraude pour le prélèvement s'établit ainsi à 0,0035 %, contre 0,0006 % en 2017, soit l'équivalent d'un euro de fraude pour environ 28 184 euros de prélèvements émis, contre un euro de fraude pour 180 000 euros de prélèvements émis en 2017. Le montant moyen d'un prélèvement frauduleux s'établit à 188 euros, contre 340 euros en 2017.

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

G29 Répartition de la fraude au prélèvement en montant, par typologie de fraude

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

Les travaux méthodologiques de la catégorisation des prélèvements frauduleux menés en 2017 permettant d'assurer une meilleure comptabilisation des données confirment que la fraude est largement imputable à l'émission de faux prélèvements (c'est-à-dire l'émission, par des créanciers frauduleux, d'ordre de prélèvement sans mandat) qui représentent 99,97 % du montant total de la fraude).

Enfin, la fraude sur le prélèvement s'est développée sur les transactions transfrontalières avec la zone SEPA qui étaient peu touchées jusqu'à présent : en 2018, elle représente 24 %, contre 1 % en 2017. Les transactions nationales concentrent en 2018 76 % de la fraude, contre 99 % en 2017.

## Principaux cas de fraude en 2018 et mesures de prévention

La principale technique de fraude sur le prélèvement constatée en 2018 est le faux prélèvement, qui consiste en l'émission d'ordres de prélèvement de façon illégitime et sans aucune autorisation ou réalité économique. Une hausse de ces faux prélèvements initiés depuis la France vers des pays transfrontaliers de la zone SEPA a été ainsi constatée. Deux autres techniques de fraude ont été constatées mais dans une moindre mesure : il s'agit de l'usurpation de l'identité et de l'IBAN [9] d'un tiers par un fraudeur pour la souscription d'un service et de l'entente frauduleuse entre créancier et débiteur.

9 *International bank account number.*

| 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 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.<br>**Envoi d'une alerte aux clients débiteurs** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte.<br>**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 services (détournement) :** le débiteur fraudeur communique à son créancier les coordonnées bancaires d'un tiers lors de la signature du mandat de prélèvement et bénéficie ainsi du service, sans avoir à en honorer les règlements prévus. | **Envoi d'une alerte aux clients débiteurs** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte.<br>**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. |

# 3 Travaux de veille technologique

## 3.1 La sécurité des modes de paiement non connectés

### Introduction

Depuis l'introduction des premières cartes à puce, au début des années 1990, les tendances de développement en matière de moyens de paiement s'illustrent par le recours aux technologies émergentes, telles que les paiements en ligne, le paiement sans contact ou les paiements par mobile. Ces évolutions ont pour conséquence de rendre l'usage des moyens de paiement toujours plus connecté, c'est-à-dire assurant une mise en relation en temps réel entre les différentes parties prenantes de la transaction : le payeur, le bénéficiaire et leurs établissements teneurs de comptes respectifs.

Ce mouvement ne doit toutefois pas occulter la persistance du recours à des modes de paiement non connectés, notamment sur support papier : chèque, virement transmis par bordereau, bulletin de commande ou d'abonnement payé par le renseignement manuscrit d'un numéro de carte, etc. Ces paiements répondent à différents besoins, tant ceux de la clientèle, qui n'est pas nécessairement équipée des matériels permettant le recours aux paiements dématérialisés, que ceux liés à des cas d'usage spécifiques pour lesquels ces modes de paiement non connectés peuvent présenter certains avantages du point de vue des parties prenantes de la transaction.

Ces modes d'initiation des transactions, qui ont ainsi échappé à la transformation numérique des offres de paiement, ne représentent désormais qu'une part limitée des flux : moins de 8 % du nombre de transactions émises en 2018 et 11,3 % de leur montant (respectivement 7 % et 3 % pour le seul chèque) ; toutefois, ils restent une cible privilégiée pour les fraudeurs qui en maîtrisent depuis longtemps les vulnérabilités, et comptent ainsi pour 47,9 % des montants fraudés au cours de l'année 2018.

Or, si les paiements émis électroniquement font l'objet d'un ensemble d'exigences de sécurité définies au niveau réglementaire et visant à réduire la fraude, notamment au travers de la deuxième directive européenne sur les services de paiement (DSP2) [1] par le principe du recours à l'authentification forte du payeur, les modes de paiement non connectés sont exclus de ces dispositions et ne peuvent, par définition, pas bénéficier de ces éléments de sécurisation.

Cette étude dresse un panorama de ces modes de paiement non connectés, et rappelle les différents paramètres pouvant concourir à leur sécurisation.

1 Les apports de la DSP2 en matière de sécurité ont fait l'objet d'une étude dédiée par l'Observatoire (cf. chapitre 1 du *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement* 2017 : https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2017).

## Panorama des modes de paiement non connectés et des risques spécifiques associés

### Périmètre

La présente étude couvre les moyens de paiement au sens du Code monétaire et financier, pour lesquels l'émission d'ordres de paiement repose sur des dispositifs non connectés, c'est-à-dire n'assurant pas une mise en relation automatisée et en temps réel entre l'émetteur de l'ordre et le prestataire de services de paiement (PSP) chargé de l'exécuter. Ce périmètre couvre les paiements par chèque, par virement et par carte (sur support papier, fax, courriel ou par appel téléphonique), et exclut notamment les deux moyens suivants.

- Le prélèvement SEPA (*single euro payments area*) : en effet, indépendamment du mode de collecte du consentement du payeur (qui peut être fait au moyen d'un mandat sous forme papier), l'émission des ordres de paiement par le créancier auprès de son PSP est systématiquement réalisée de façon connectée. Pour mémoire, une analyse complète des risques et mesures de sécurité associées au prélèvement a été publiée par l'Observatoire dans son rapport annuel 2017.

- Les titres de paiement papier émis par des organismes publics et privés matérialisant le droit à une prestation de services : si ces titres comportent très souvent de façon impropre la dénomination de « chèque » (chèque restaurant, chèque énergie, chèque voyage, etc.), il convient de rappeler que ces titres ne sont ni des chèques ni même des moyens de paiement au sens de la réglementation, et ne relèvent pas du champ de compétences de l'Observatoire.

### Le chèque et ses différentes variantes

Le chèque est défini de façon générale comme « l'écrit par lequel une personne, appelée **tireur** (émetteur du chèque), donne l'ordre à un établissement de crédit, appelé **tiré**, de payer à vue une certaine somme à une troisième personne, appelée **bénéficiaire**, ou à son ordre [2] ». Si ce moyen de paiement a connu un certain nombre d'évolutions et d'actions de standardisation visant à en automatiser le traitement et la gestion par les banques, il n'en demeure pas moins le moyen de paiement scriptural le plus ancien.

2 Cf. *Entreprises en difficulté*, Pérochon (F.), 9e édition, collection *Manuel*, Librairie générale de droit et de jurisprudence (LGDJ), 2012 ; *Instruments de crédit et de paiement*, Bonhomme (R.), 9e édition, collection *Exercices pratiques*, LGDJ, 2015.

Encadré 1

### Statut du chèque et dates de référence

Le chèque est apparu en France sous le Second Empire lors de la création des grandes banques de dépôts ; le premier texte le réglementant est une loi du 14 juin 1865.

Par la suite, la convention de Genève du 19 mars 1931 portant loi uniforme sur le chèque a été introduite en France par le décret-loi du 30 octobre 1935, qui est considéré comme la référence de base en la matière. Les dispositions du Code monétaire et financier régissant le chèque en France sont issues de ce texte.

Cet instrument de paiement est encadré par un régime juridique complexe codifié au titre III du livre Ier du Code monétaire et financier (CMF), intitulé « Les instruments de monnaie scripturale ».

Ainsi, aux termes de l'article L. 131-2 du CMF, alinéa 1, le chèque doit contenir « *la dénomination de chèque* ». Selon l'alinéa 2 du même article, le chèque doit contenir « *le mandat pur et simple de payer une somme déterminée* » qui est prérédigé comme ceci « *Payez contre ce chèque non endossable sauf au profit d'une banque ou d'un établissement assimilé la somme de* ». À défaut, le titre de paiement non revêtu de ces mentions, même complété par les autres mentions obligatoires (cf. *infra* paragraphe « Le chèque », dans la partie « Modalités de sécurisation des modes de paiement non connectés »), ne vaut pas comme chèque.

Les supports utilisés (le titre papier), permettant donc au titulaire d'un compte de donner mandat à sa banque de payer la somme inscrite au bénéficiaire, sont normalisés et préimprimés par les banquiers sur les formules délivrées à leurs clients, également appelées « formules prémarquées » et plus communément « chèques ». Ce support papier, hérité de la convention de Genève, revêt un format réputé obligatoire par l'arrêté du 5 novembre 1998 [3] portant homologation et mise en application obligatoire de normes françaises, plus précisément de la norme française NF K11-111 : Banque – Formule de chèque payable en France. Cette norme a pour objet de définir l'imprimé sur lequel doivent être établis les chèques.

Sur ces formules de chèques, deux mentions, bien qu'elles ne soient pas obligatoires au sens de la validité du chèque, apparaissent essentielles. Il s'agit des mentions suivantes :

- « *Payez contre ce chèque* ***non endossable sauf au profit d'une banque ou d'un établissement assimilé la somme de*** » qui a pour but d'interdire l'endossement à une personne autre qu'une banque ou un établissement assimilé ; néanmoins, elle ne fait pas obstacle à la circulation libre du chèque tant que le bénéficiaire n'est pas indiqué sur le chèque, bien qu'une telle pratique ne soit pas recommandée pour des raisons de sécurité ;

- le **barrement du chèque** par le banquier, plus précisément de la préimpression de deux barres parallèles portées au recto de la formule ; aux termes de l'article L. 131-45 du CMF, le chèque barré « *ne peut être payé par le tiré, qu'à un banquier, à un établissement de paiement, à un chef de centre de chèques postaux ou à un client du tiré* ». Par cette disposition, le chèque barré ne peut être remis qu'à l'établissement teneur de compte du bénéficiaire pour encaissement ; de même, un établissement teneur de compte ne peut accepter un chèque barré que de son client ou d'un autre banquier ou assimilé, et ne pourra ainsi encaisser le chèque que pour le compte de ces personnes.

La formule la plus couramment mise à la disposition du client par la banque prend la forme de chéquier. Pour les professionnels et/ou entreprises, elle peut prendre la forme d'une lettre-chèque. En outre, pour des situations particulières, le client peut se faire délivrer un chèque de banque. Plus précisément, ce sont les dispositifs suivants.

- La **lettre-chèque** est un dispositif de remplissage automatique de chèques proposé par les banquiers à leurs clients entreprises émetteurs de gros volumes de chèques, qui leur permet

3 Arrêté publié au *Journal officiel de la République française,* n° 264, du 14 novembre 1998.

d'imprimer un texte d'accompagnement du chèque, ainsi que de compléter la formule du chèque des mentions variables. Toutefois, l'utilisation de ce « format » nécessite certaines conditions préalablement souscrites par le client dans le cadre d'une convention entre la banque et l'entreprise.

• Le **chèque de banque** est un dispositif utilisé par les banquiers sur demande du client dans des cas bien précis, généralement pour des montants importants, tels que pour le paiement d'un achat de véhicule, le paiement d'honoraires auprès de professionnels, etc. Ce chèque de banque dispose par ailleurs d'éléments de sécurité supplémentaires.

Le chèque (y compris ses variantes) est un titre de banque dont la délivrance est, de par la loi, de la compétence exclusive des établissements de crédit, seuls habilités, au titre de l'article L. 131-1, à tenir des comptes sur lesquels des chèques peuvent être tirés. À ce titre, l'émission de ce moyen de paiement n'est pas accessible aux autres catégories de prestataires de services de paiement, que sont les établissements de paiement et les établissements de monnaie électronique.

**Les circuits de traitement du chèque**

Historiquement, l'échange des chèques entre les banques aux fins de compensation avait lieu quotidiennement, de façon manuelle, dans les chambres de compensation mises à leur disposition par la Banque de France (article L. 131-34 du CMF). En pratique, chaque banque présentait à la chambre de compensation les différents chèques qu'elle était chargée d'encaisser sur les autres banques. Une compensation s'opérait entre le montant qu'une banque devait à chaque banque et ceux que chacune d'elles lui devait afin de dégager un solde. Les soldes crédits et/ou débits étaient portés au compte de chaque banque par la chambre de compensation, par l'intermédiaire de la Banque de France. Les chèques papier étaient ainsi remis entre les banques lors des séances tenues au sein des chambres de compensation.

À l'occasion du passage à l'euro, en vue de moderniser le système, les banques ont opté pour une présentation dématérialisée par la voie des systèmes interbancaires de compensation avec la mise en œuvre de l'échange d'images-chèques (EIC) [4] qui remplace les chambres de compensation depuis fin juin 2002 [5]. Au terme de ce processus, par principe, les opérations de paiement par chèques se règlent via l'échange d'images-chèques dématérialisées conformément aux dispositions du règlement n° 2001-04 du Comité de la réglementation bancaire et financière du 29 octobre 2001 relatif à la compensation des chèques. Parallèlement, dans certains cas et notamment pour les chèques de montant élevé, un échange physique de chèques est effectué entre les établissements du remettant et du tiré ; par ailleurs, des copies du chèque peuvent également être échangées entre ces établissements pour divers motifs (vérifications, réquisition, etc.).

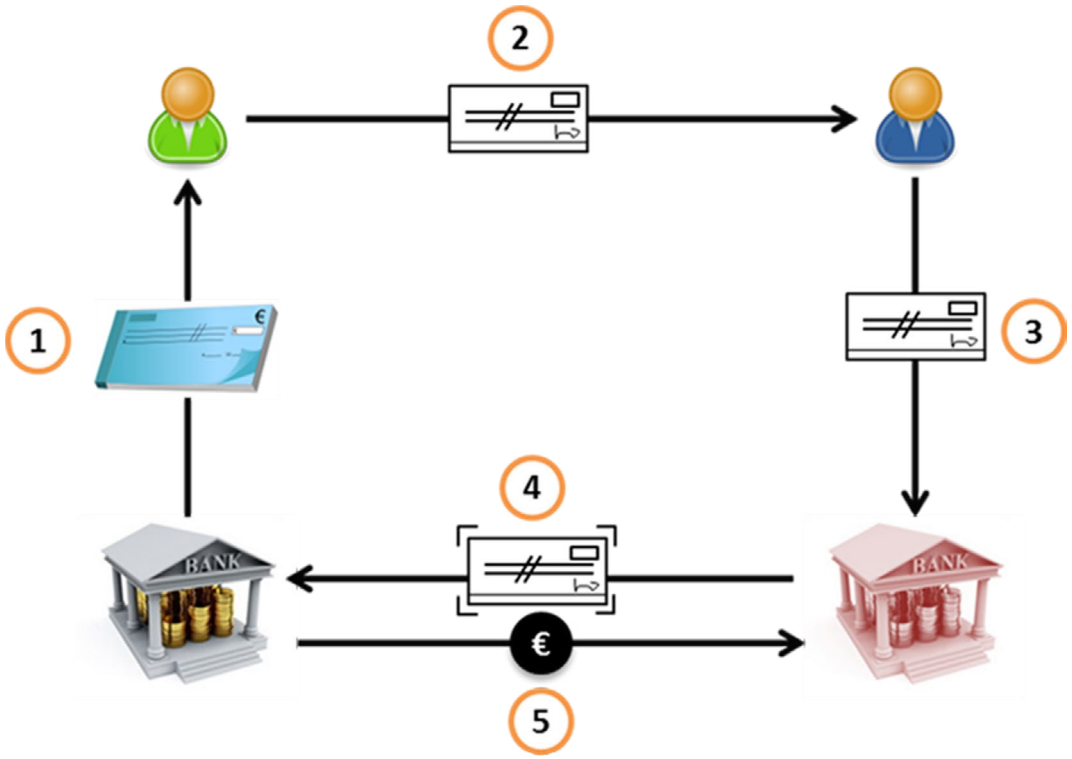
4 Cf. le *Rapport annuel de la Banque de France* 2002 (*https://www.banque-france.fr*) : « *L'échange d'images-chèques vise à substituer à la remise systématique des formules papier dans les chambres de compensation celle, dans le système interbancaire de télécompensation (SIT), d'enregistrements électroniques constitués à partir du contenu de la ligne magnétique des chèques, complété de leur montant.* »

5 Date d'achèvement de la dématérialisation des échanges interbancaires des moyens de paiement (cf. « Le système interbancaire de télécompensation » (2002), *Bulletin de la Banque de France*, n° 107, novembre).

La dématérialisation de la présentation à l'encaissement entre les banques de ce moyen de paiement a permis d'améliorer le service rendu à la clientèle et de raccourcir le temps de traitement des chèques. C'est un système de paiement quadripartite qui peut être résumé simplement dans le schéma présenté dans l'encadré 2.

Encadré 2

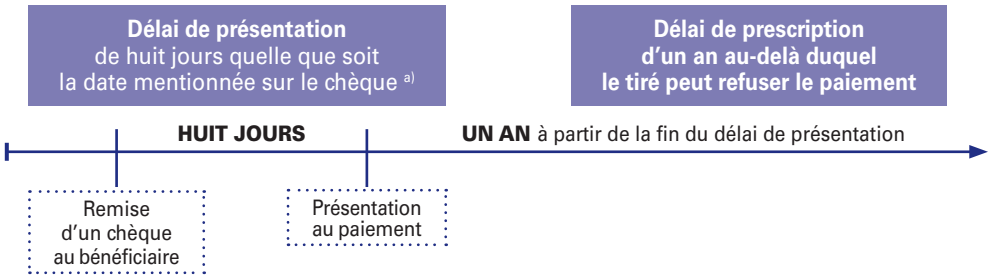
## Système de traitement interbancaire du chèque




1. En amont du paiement (en règle générale), la banque du payeur remet un carnet de chèques à son client.
2. Le payeur (tireur) complète le chèque et le remet au bénéficiaire en règlement d'un montant.
3. Le bénéficiaire remet le chèque à sa banque, généralement accompagné d'un bordereau de remise ou d'une saisie sur un automate de remise.
4. La banque du bénéficiaire dématérialise le chèque et transmet l'image-chèque au système de compensation des paiements.
5. La banque du payeur procède au règlement des fonds à la banque du bénéficiaire.

Encadré 3

## Délais légaux d'encaissement du chèque




a) Ce délai peut être porté à vingt ou à soixante-dix jours selon que le lieu de l'émission du chèque se trouve situé en Europe ou hors Europe, ou être prolongé dans des cas de force majeure.

### Délai de présentation

Une fois le chèque créé et émis, c'est-à-dire lorsqu'il est remis par le tireur à son bénéficiaire, ce dernier peut le présenter au paiement quelle que soit la date qui y est apposée. En effet, un chèque postdaté peut être valablement présenté et pourra être ainsi payé avant même la date d'émission présumée. Pour cette raison, il est recommandé au tireur de ne pas postdater un chèque, cette pratique n'ayant aucun effet sur le délai de présentation du chèque au paiement.

Les règles de présentation au paiement fixent un **délai légal de présentation** de huit jours après l'émission du chèque ou de la date d'émission présumée (article L. 131-32 alinéa 1° du CMF), ce délai étant porté à vingt ou soixante-dix jours si le chèque est émis hors de la France métropolitaine avec une distinction selon que le lieu de l'émission se trouve situé en Europe ou hors Europe (vingt jours dans le premier cas, soixante jours dans le second). Même si des cas de force majeure permettent des prolongations de délais sous certaines conditions, il est conseillé au porteur du chèque de le présenter rapidement au paiement.

### Délai de prescription

Il ne faut pas confondre le délai de présentation avec le **délai de prescription** de l'action du porteur du chèque contre le tiré. Selon l'article L. 131-35 du CMF, le chèque présenté hors délai de présentation doit quand même être payé par le tiré, et ce, pendant un an à partir de ce délai de présentation. Au-delà, le tiré peut se prévaloir de la prescription visée à l'article L. 131-59 du CMF pour en refuser le paiement.

**Une utilisation en déclin, mais portée par des cas d'usages spécifiques**

Depuis plus de quinze ans, les statistiques d'utilisation des moyens de paiement scripturaux montrent un déclin continu du chèque, tant en nombre d'opérations qu'en valeur. Néanmoins, son usage reste encore répandu en France, puisqu'en 2018 il représente encore 7 % des opérations de paiement, soit une émission de 1,7 milliard de chèques, en baisse de 9 % en un an, pour une valeur de 891 milliards d'euros (– 11 %). De premier moyen de paiement en nombre de transactions réalisées au début des années 2000, il est désormais à la quatrième place, après avoir été dépassé progressivement par la carte, puis par le prélèvement et le virement.

Toutefois, certaines pratiques commerciales contribuent à son utilisation qui perdure dans le temps, comme par exemple celles qui offrent la possibilité de :

• payer des sommes significatives (le montant moyen en émission d'un chèque est de 510 euros, alors qu'il n'est que de 43 euros pour la carte bancaire en 2018), notamment au point de vente en raison des plafonds d'utilisation des cartes de paiement ;

• échelonner un paiement en plusieurs fois, par la remise de plusieurs chèques au créancier ;

• s'accorder, avec son créancier, sur la date de remise à l'encaissement du chèque (cas des « opérations chèques différés » pratiquées par certains commerçants) ;

• payer des sommes sans disposer préalablement des coordonnées bancaires du bénéficiaire ;

• de joindre au règlement le détail des prestations ou remboursements effectués (cf. lettre-chèque) ;

• dénoter facilement les paiements émis dans les logiciels comptables des entreprises sur la base du numéro de chèque.

À l'opposé, compte tenu du risque d'impayé et des vulnérabilités de ce moyen de paiement à la fraude, des commerçants peuvent faire le choix de refuser tout paiement par chèque, à condition d'en avoir informé les clients, préalablement et de manière apparente, avant l'acte d'achat, c'est-à-dire par un affichage des conditions de paiement dès l'entrée du point de vente.

En outre, certaines situations peuvent contraindre actuellement consommateurs ou entreprises à utiliser le chèque ou les espèces, notamment pour le paiement de services rendus par des artisans ou des professions libérales non équipés de terminaux de paiement par carte, ou le paiement de biens et services auprès de commerçants en situation de mobilité (marchés, foires, etc.) ou encore pour remplir l'obligation de « dépôt de garantie » pour la prise à bail de locaux ou de locations saisonnières. Les travaux engagés au sein du Comité national des paiements scripturaux (CNPS) visent à ce titre à promouvoir des solutions alternatives crédibles reposant sur les paiements par carte, mais également les instruments SEPA (comme le virement instantané), qui nécessiteront du temps pour être largement utilisées.

Par ailleurs, le chèque fait encore aujourd'hui office de cadeau (mariage, anniversaire) puisqu'il offre un large choix d'utilisation, contrairement aux cartes cadeaux, certes d'utilisation plus pratique en magasin ou sur internet, mais

généralement acceptées dans un périmètre limité d'enseignes.

Enfin, les très petites entreprises contribuent également à l'émission de volumes importants de chèques : les travaux du CNPS [6] avaient ainsi souligné qu'un quart des entreprises de moins de dix personnes recourrait au chèque pour plus de la moitié de leurs transactions, et que cette proportion étaient encore de 14 % pour les petites et moyennes entreprises de 50 à 249 salariés.

**Une vulnérabilité à la fraude**

Bien que le chèque ne soit qu'au quatrième rang des instruments de paiement scripturaux les plus utilisés, il reste le deuxième moyen de paiement le plus fraudé, avec un montant annuel de fraude en hausse qui atteint 450 millions d'euros en 2018. Son taux de fraude a progressé de façon continue de 2016 à 2018 pour s'établir à 0,0508 %, soit un euro de fraude pour 2 000 euros de paiement. Le chèque supporte ainsi 43 % des montants de fraude aux moyens de paiement en France, alors qu'il ne représente que 7 % des transactions en volume.

En dépit des innovations apportées par les banques aux processus de traitement, le chèque reste un instrument de paiement existant exclusivement sur support papier, son statut issu de la convention de Genève restreignant toute possibilité de dématérialisation complète ; ainsi, à l'inverse des autres moyens de paiement, le chèque n'est pas informatisable et a peu évolué dans son format. Il est toujours distribué, en règle générale, sous la forme d'un « carnet de chèques » qui regroupe entre 20 à 50 chèques en un seul support, ce qui représente autant de facultés de fraude en un temps très court lorsqu'il est perdu ou volé, souvent avant même que le titulaire ne s'en aperçoive. Par ailleurs, un chèque régulier intercepté par un fraudeur peut être falsifié par différents procédés tels que le grattage, le gommage ou l'effacement de certaines mentions du chèque ou encore la réécriture ou l'ajout de certaines d'entre elles. Des techniques plus poussées, dites de cavalerie ou visant à faciliter le blanchiment d'argent, sont également constatées [7].

**Le virement en mode « non connecté »**

Le virement est un service de paiement fourni par l'établissement teneur du compte de paiement du payeur et qui consiste à créditer, sur la base d'une instruction du payeur ou d'un mandataire, le compte de paiement d'un bénéficiaire par une opération (virement unitaire) ou une série d'opérations (virement récurrent ou permanent) réalisées à partir du compte de paiement du payeur.

**Les modes d'utilisation du virement**

Les principaux canaux d'émission de virements reposent sur le recours à des interfaces en ligne, assurant une connexion directe entre le client et son établissement teneur de compte :

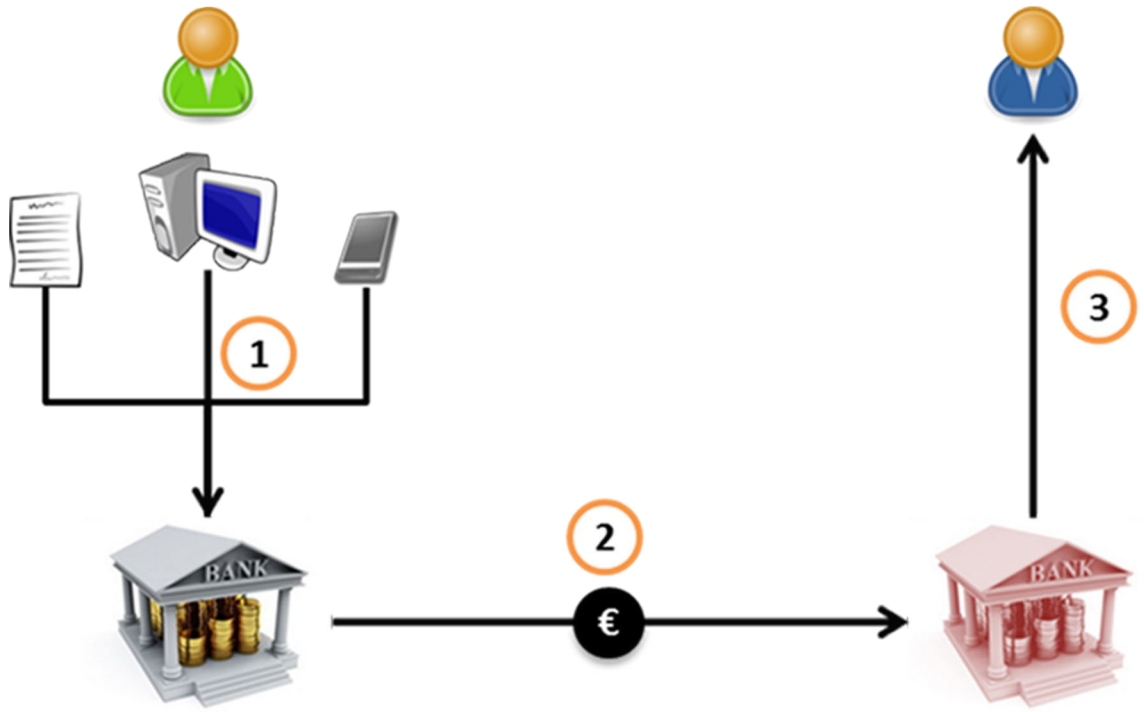
- la transmission automatisée de fichiers comportant plusieurs ordres de paiement, utilisée principalement par la clientèle professionnelle pour le paiement des salaires, pensions ou prestations de ses fournisseurs, qui représente la majorité des virements émis en France, tant en volume (64 %) qu'en valeur (58 %) ;

6 Cf. le rapport d'activité 2016 du CNPS (*https://www.banque-france.fr*).

7 Pour mémoire, ces différentes modalités de fraude au chèque sont présentées dans le chapitre 2 du rapport annuel de l'OSMP 2017 (*https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2017*).

Encadré 4

## Cinématique d'utilisation du virement SEPA




1. Le payeur, titulaire du compte ou mandataire, établit l'ordre de virement indiquant notamment le compte à débiter, le numéro de compte (ou IBAN – *international bank account number*) à créditer, le montant, la date et la fréquence de l'opération si nécessaire, et le transmet à son établissement teneur de compte, qui procède au débit de la somme sur le compte du payeur.

2. L'ordre de virement est échangé dans les circuits de paiement interbancaire, entraînant le règlement des fonds vers l'établissement teneur du compte du bénéficiaire.

3. L'établissement teneur du compte du bénéficiaire crédite le compte destinataire identifié dans l'ordre de virement.

• l'utilisation des interfaces bancaires en ligne, permettant l'émission d'ordres de virement unitaires, qui représente 33 % des virements émis en volume et 32 % en valeur.

Les émissions d'ordres de virement dits « non connectés » représentent ainsi une part très

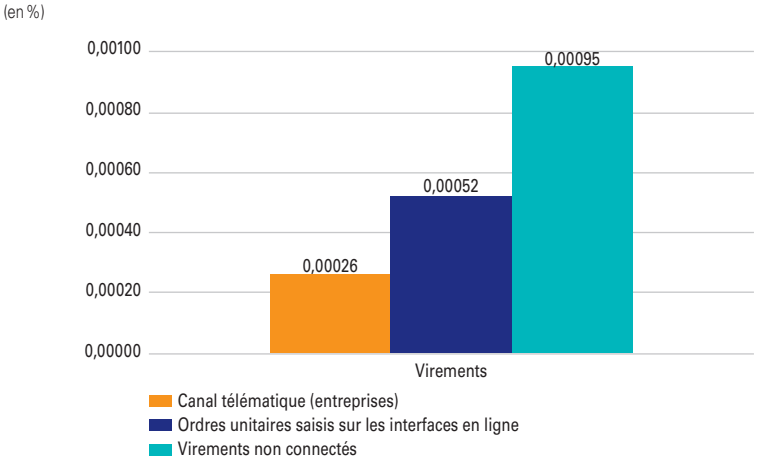
limitée des virements émis en France : 3 % en nombre d'opérations, et 9 % des montants échangés. Elles reposent sur différents canaux :

• la passation d'ordres par téléphone ou en agence,

• la transmission d'ordres ou de bordereaux de virement par fax ou par courrier postal ou électronique.

Ces canaux ont en commun de nécessiter la re-saisie des instructions de paiement par l'établissement teneur de compte, soit par l'interlocuteur habituel du client (guichet, conseiller, agence), soit par un service de back-office de traitement des opérations clientèle.

G1 Taux de fraude sur les virements par canal d'initiation




Source : Observatoire de la sécurité des moyens de paiement.

### La fraude aux virements non connectés

Pour rappel [8], le taux annuel de fraude au virement est le plus faible parmi tous les taux de fraude relatifs aux moyens de paiement accessibles aux particuliers avec un taux de l'ordre 0,0004 %, soit un euro de fraude pour 250 000 euros de paiement. Or, cette fraude est répartie à parts relativement égales entre les différents canaux d'utilisation, et ce alors que les virements non connectés ne représentent qu'une faible proportion des virements émis. Le taux de fraude des virements non connectés s'établit ainsi à 0,0010 %, soit un niveau près de quatre fois supérieur au taux de fraude global de ce moyen de paiement, ce qui représente l'équivalent d'un euro de fraude pour 100 000 euros de paiement et un montant annuel de fraude de 21 millions d'euros.

Les fraudes aux virements non connectés peuvent s'appuyer sur deux grandes familles de techniques communes à tous les modes de virement : d'une part l'émission de faux ordres par le fraudeur, qui usurpe alors l'identité du titulaire du compte débité ; et d'autre part, les techniques de manipulation par ingénierie sociale visant à conduire le titulaire du compte à émettre un ordre de virement illégitime [8].

### La carte de paiement en mode non connecté

Les paiements par carte en mode non connecté, généralement qualifiés de « MOTO » (pour *mail order/telephone order*), sont réalisés par le biais d'un canal de communication de type courrier, télécopie ou téléphone (échange vocal). En règle générale, le

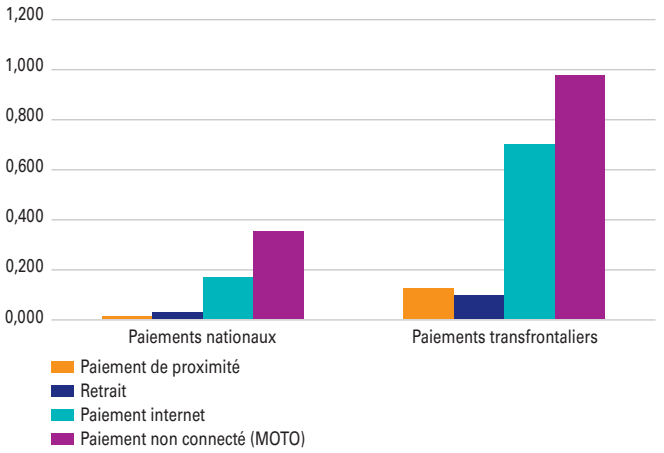
8 Cf. chapitre 2 du rapport annuel de l'OSMP 2017 (*https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2017*).

commerçant n'est en contact direct ni avec la carte de paiement ni avec son porteur au moment de l'initiation du paiement. Cette particularité entraîne les conséquences suivantes.

• Du point de vue du payeur, les informations de paiement (numéro de carte et date d'expiration) sont transmises par le biais d'un canal généralement non sécurisé et doivent être le plus souvent retraitées manuellement. La signature du titulaire de la carte n'est pas requise, et l'impression et la transmission des reçus ne sont pas obligatoires.

G2 Taux de fraude sur les paiements par carte non connectés (porteur français)

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

• Du point de vue du bénéficiaire, l'entreprise qui reçoit les commandes par courrier, par fax, par téléphone ou autre moyen non connecté, peut initier les transactions soit en activant la fonction MOTO lorsqu'elle dispose d'un terminal, soit en saisissant les informations de paiement sur le site web de son établissement teneur de compte, soit en lui transmettant des fichiers contenant ces informations via une liaison sécurisée ou via un autre canal (fax, courrier, etc.).

Ce mode d'initiation est régi par des règles spécifiques des systèmes de paiement par carte : le conseil de normalisation de la sécurité pour l'industrie des cartes de paiement (PCI SSC) [9] a ainsi publié un guide [10] énonçant des principes de sécurité aux acteurs du marché afin qu'ils se conforment aux exigences du standard.

Or, en dépit de ces règles de sécurité, le taux de fraude pour les paiements par carte non connectés est bien supérieur à ceux des autres modes de paiement par carte. Il représente un montant global de l'ordre de 28,5 millions d'euros pour les porteurs français en 2018, soit 7,1 % de la fraude à la carte, alors que ces transactions ne représentent qu'une part infime des paiements réalisés (0,5 % en nombre et 0,8 % en valeur).

En particulier, la mise en conformité progressive des acteurs du marché avec les exigences de sécurité des paiements connectés (carte à puce EMV [11], standards PCI DSS [12] pour le *e-commerce*) a entrainé un

9 *Payment Card Industry Security Standards Council* : organe de standardisation de référence au niveau international en matière de sécurité monétique, constitué des principaux systèmes de paiement par carte.

10 Cf. *https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf*

11 Pour Europay Mastercard Visa.

12 Pour *Payment Card Industry Data Security Standards*, ensemble de règles visant à la sécurité des données dans les systèmes d'information où transitent les données de paiement.

report de la fraude à la carte vers le domaine des paiements MOTO, notamment pour les paiements transfrontaliers : les deux tiers de la fraude MOTO touchant les porteurs français concerne des transactions à l'international.

Par ailleurs, les paiements MOTO constituent également un vecteur privilégié de la compromission de numéros de carte par les fraudeurs, qui les réutilisent ensuite pour initier d'autres types de transactions frauduleuses, notamment des paiements en ligne.

## Modalités de sécurisation des modes de paiement non connectés

### Le chèque

#### Les dispositions de sécurité du point de vue des utilisateurs

Les modalités de sécurisation du chèque sont en partie prévues par les dispositions du Code monétaire et financier, qui encadrent la création d'un chèque. Ainsi, pour valoir comme chèque, ces conditions imposent certaines **mentions obligatoires**, celles-ci sont visées à l'article L. 131-2 du CMF :

- la dénomination de chèque, insérée dans le texte même du titre et exprimée dans la langue employée pour la rédaction du titre,
- le mandat pur et simple de payer une somme déterminée,
- le nom de celui qui doit payer, nommé le tiré,
- l'indication du lieu où le paiement doit s'effectuer,
- l'indication de la date et du lieu où le chèque est créé,
- la signature de celui qui émet le chèque, nommé le tireur.

Les quatre premières mentions ne présentent aucune difficulté pour l'utilisateur (payeur/bénéficiaire) dans la mesure où elles sont préimprimées par les banquiers sur les formules délivrées à la clientèle. Néanmoins, le payeur devra faire preuve de vigilance sur le remplissage des autres mentions afin d'éviter toute tentative de fraude par un tiers entrant en possession du chèque (cf. annexe 2).

En outre, le droit a prévu **l'interdiction de certaines mentions** telles que l'ajout d'une échéance pour la présentation au paiement (article L. 131-31 du CMF) ou la stipulation d'intérêts (article L. 131-8 du CMF). Ces mentions sont tout simplement réputées non écrites et donc de nul effet, ce qui implique que seules les mentions obligatoires sont alors reconnues comme valides.

Enfin, aux côtés des mentions obligatoires, diverses **mentions facultatives** peuvent être apposées.

- Les mentions préimprimées sur les formules délivrées par le banquier à son client qui ne posent donc aucune difficulté (cf. *supra* la mention interdisant l'endossement à une personne autre qu'une banque ou un établissement de crédit et le barrement, qui ne sont pas des éléments requis pour la validité du chèque mais sont la conséquence de la rédaction des articles L. 131-4 et L. 131-44 du CMF).
- Les mentions qui désignent le bénéficiaire paraissent évidentes, pourtant elles doivent être expressément stipulées ; en effet, le chèque peut être payable à une personne dénommée ou au porteur (article L. 131-6 du CMF). De même le chèque sans indication de bénéficiaire est vu comme un chèque au porteur. Par ailleurs, le payeur

(tireur) peut se désigner comme bénéficiaire, par exemple dans les « chèques de retrait » émis à l'ordre de « moi-même » permettant de retirer des fonds ou pour des transferts de fonds de compte à compte détenus par un même titulaire dans des établissements bancaires différents (article L. 131-7 du CMF). Néanmoins, la désignation du bénéficiaire demeure importante car elle permet de lutter contre les chèques tirés par des usurpateurs.

• La mention relative à la certification (article L. 131-14 du CMF), c'est-à-dire qui certifie que la provision correspondante au chèque existe à la disposition du tireur au moment de la certification, doit être conforme à la procédure de certification visée à l'article R. 131-2 du CMF.

L'article L. 131-14 dispose que le tiré a la faculté de remplacer le chèque certifié par un **chèque de banque**. Ce remplacement, devenu courant, est d'ailleurs avantageux pour le bénéficiaire car la garantie

Encadré 5

## Chèque de banque

Le chèque de banque est un chèque délivré par un banquier et tiré sur ses caisses ou celles d'un correspondant en vue d'assurer au bénéficiaire le paiement du chèque pendant toute la durée de sa validité. Lors de la délivrance du chèque de banque, la banque émettrice va débiter le compte du débiteur après contrôle de la provision et bloquer cette somme jusqu'à son encaissement par le bénéficiaire.

En pratique, le chèque de banque se distingue d'un chèque ordinaire par la présence d'un filigrane de haute qualité, comparable à ceux qui figurent sur les billets de banque, qui permet au bénéficiaire de s'assurer de son authenticité :

• ce filigrane étant normalisé, il est identique en motif et en taille pour l'ensemble des banques françaises,

• le filigrane présente un haut niveau de protection car il est visible par transparence et couvre une partie importante de la surface du chèque,

• la présence de la mention « CHEQUE de BANQUE » au verso du chèque, bordée en haut et en bas par deux flammes rayées,

• cette mention est encadrée de part et d'autre, par deux semeuses dont les parties claires et sombres du dessin de l'une sont inversées par rapport à celles de l'autre.

de paiement liée au provisionnement par la banque du tiré du montant du chèque émis ne sera pas limitée à huit jours mais à un an.

Le paiement par chèque de banque peut être parfois exigé par le vendeur lors d'une transaction de montant élevé (vente de véhicule par exemple). Après avoir procédé aux vérifications d'usage (mentions obligatoires et facultatives communes au chèque ordinaire et au chèque de banque, mentions spécifiques du chèque de banque), il est recommandé au vendeur de s'assurer de l'authenticité dudit chèque de banque auprès de l'établissement émetteur, sans utiliser le numéro de téléphone porté sur le chèque (par exemple, en utilisant un annuaire papier ou en ligne) ; en cas de doute, il est recommandé au bénéficiaire de ne pas se déposséder de son bien et de reporter la transaction.

### Règles de vigilance pour les utilisateurs

Afin de lutter contre la fraude, des règles de vigilance sont à observer à tous les niveaux du processus de paiement par chèque et par toutes les personnes intervenant dans ce processus (porteurs, commerçants, banques, etc.).

La convention de compte signée par le client lors de l'ouverture d'un compte en banque doit mentionner les moyens de paiement qui lui sont délivrés. Les **modalités de mise à disposition** d'un chéquier peuvent varier d'une banque à l'autre et doivent être stipulées dans la convention de compte (renouvellement automatique de chéquier, envoi en lettre simple, envoi suivi ou en lettre recommandée avec avis de réception, mise à disposition en agence, etc.). Des règles de vigilance en cas de non réception de chéquiers dans un certain délai, notamment dans le cadre d'une gestion automatique des renouvellements doivent être portées à la connaissance du porteur. De même, lors de la clôture d'un compte en banque, le banquier doit demander la restitution des chèques non utilisés (article L. 131-71 du CMF). Les **modalités de restitution** doivent par conséquent être portées à la connaissance du client afin d'éviter que des formules non restituées par les clients puissent faire l'objet d'une utilisation frauduleuse.

Le porteur doit également veiller à respecter des **règles de conservation** des chèques et chéquiers. Au-delà de simples règles de bon sens comme, par exemple, celle d'éviter le dépôt des chéquiers dans des endroits exposés ou peu protégés (boîte à gants de voiture, sur un meuble, etc.), des règles plus précises sont généralement diffusées par les banquiers auprès de leur clientèle.

En outre, les **règles de vigilance** à observer lors de l'utilisation d'un chèque en paiement d'une transaction diffèrent selon que l'utilisateur agit en tant que payeur ou en tant que bénéficiaire.

En qualité de **tireur**, c'est-à-dire lors de la rédaction d'un chèque :

- remplir le chèque en y apposant les mentions qui ne sont pas déjà préimprimées (dénomination de la somme à payer, bénéficiaire, date – jour/mois/année – et lieu où le chèque est créé, signature) de façon lisible sans possibilité d'interprétation par le tiré ;

- afin de prévenir les risques de modification du chèque : utiliser un stylo à bille noir non effaçable et ne pas laisser d'espaces libres avant et après les mentions remplies manuellement par le tireur ;

- être en capacité de pouvoir, le cas échéant, justifier de son identité au moyen d'un document officiel, voire de deux documents chez certains

commerçants et pour des chèques d'un certain montant ;

• concernant la somme indiquée sur le chèque (article L. 131-10 du CMF), plusieurs points doivent être soulignés :

– le droit n'exige pas que la somme soit inscrite en lettres et en chiffres, la double inscription est notamment en recul en raison de la croissance des systèmes informatisés de remplissage de chèque qui ne portent que sur des chiffres ; toutefois, le remplissage des deux mentions limite les possibilités de falsification et constitue donc une sécurité supplémentaire pour le tiré ;

– si le montant écrit en lettres et celui écrit en chiffres comportent des différences, c'est la somme écrite en toutes lettres qui prévaut ;

– si le montant est écrit plusieurs fois soit en toutes lettres, soit en chiffres, et que les montants ne coïncident pas, c'est la somme la plus faible qui prévaut ;

– il peut arriver que la somme ne soit inscrite sur le chèque que lors de l'encaissement ; il s'agit du chèque « en blanc » qui constitue une pratique dangereuse et donc à proscrire en toute circonstance même lorsque le bénéficiaire est un proche du tireur (cas de vol ou de perte par exemple du chèque en blanc) ;

Encadré 6

## De nouvelles escroqueries basées sur l'abus de confiance et les technologies numériques

L'Observatoire appelle les particuliers et les entreprises à la plus grande vigilance au regard de types d'escroqueries en fort développement, par lesquelles les fraudeurs amènent leur victime à encaisser des chèques frauduleux en s'appuyant sur l'utilisation d'internet. Les modes opératoires identifiés sont les suivants.

• L'envoi d'un chèque d'un montant trop élevé en règlement d'une prestation (par exemple achat sur internet), en demandant au bénéficiaire de rembourser le trop perçu par virement. Dans ce cas de figure, il est recommandé au vendeur de retarder de quelques jours l'envoi du bien et l'émission du virement, afin de se prémunir contre le risque de rejet a posteriori du chèque, voire de décliner la transaction.

• Le recrutement via les réseaux sociaux de personnes chargées d'encaisser les chèques pour le compte d'une tierce personne pour différents motifs (problèmes bancaires rencontrés par le demandeur, domiciliation à l'étranger ou encaissement de chèque non accessible, etc.) et de reverser ensuite à celle-ci la somme (ou un autre montant) par virement. Dans ce cas de figure, les participants au montage, qui peuvent être appâtés par une promesse de commission, contribuent à un dispositif de blanchiment tout en devenant elles-mêmes victimes de fraude, voire complices.

– lorsque le chèque est rempli par un système de remplissage automatique de caisse en magasin, le client se doit, là aussi, de vérifier que toutes les mentions sont bien portées sur le chèque, que la somme est bien lisible et qu'elle correspond à la somme due.

En qualité de **bénéficiaire**, à la réception d'un chèque en paiement :

• contrôler strictement le chèque, somme en lettres et en chiffres, signature, date et lieu de création ;

• vérifier les documents d'identité remis par le tireur, ce qui permet également de vérifier la signature ;

• refuser toute demande éventuelle d'ajout de la part du tireur : délai ou condition d'encaissement par exemple ;

• endosser le chèque en apposant sa signature manuscrite au dos du chèque ;

• déposer le chèque pour encaissement dans les jours suivant sa réception afin d'éviter qu'il ne soit perdu ou volé puis éventuellement falsifié avant sa remise à encaissement par un fraudeur.

### Les règles de vigilance spécifiques applicables aux bénéficiaires marchands

La plupart des marchands bénéficiaires de chèque, notamment du secteur de la grande distribution, utilisent un système automatique de remplissage de chèque. Ce remplissage peut s'avérer imparfait et augmenter le risque de falsification, dans la mesure où dans certains cas :

• la seule mention en chiffres de la somme est apposée sur le chèque ;

• l'encre utilisée est de couleur bleue alors que l'encre noire est recommandée par les banques ;

• des problèmes d'impression (encre trop faible ou encore mal répartie) ou de réglage du système ont pour effet de rendre la mention insuffisante.

Il est de l'intérêt du marchand de respecter des règles de vigilance lorsqu'il accepte des paiements par chèques, notamment du contrôle complet du chèque, de surcroît lorsqu'il intervient dans le remplissage du chèque pour son client via son système automatique de rédaction.

Afin de se prémunir des chèques irréguliers, le marchand a la possibilité d'accéder au fichier national des chèques irréguliers (FNCI) de la Banque de France, service officiel de prévention des impayés en souscrivant un contrat auprès du service Vérifiance accessible à l'adresse *https://www.verifiance-fnci.fr*. Le marchand peut également avoir recours à d'autres prestataires qui proposent un service de garantie de paiement basé sur une analyse du risque qui leur est propre.

Un commerçant peut refuser un chèque en paiement des achats de son client pour différentes raisons :

• soit il n'accepte aucun chèque comme moyen de paiement, sous condition d'en avoir informé ses clients par un affichage visible dès l'entrée au point de vente ;

• soit les conditions à l'acceptation du chèque ne sont pas remplies (présentation de pièce d'identité, etc.) ;

• soit le commerçant considère que le chèque est irrégulier au moyen d'un système expert tel que Vérifiance (cf. encadré 7, FNCI, *supra*) ou d'une solution alternative qu'il a choisie : il consulte ce

Encadré 7

## Fichier national des chèques irréguliers (FNCI)

Le fichier national des chèques irréguliers [1] est un fichier informatique géré par la Banque de France. Il est alimenté par les banques émettrices.

Il recense les chèques dits « irréguliers », c'est-à-dire les chèques relevant d'un des trois cas de figure suivants :

- les chèques faisant l'objet d'une opposition pour perte ou vol,
- les chèques ayant été émis sur un compte clos ou sur le compte d'un interdit de chèque,
- les chèques identifiés comme faux.

Il permet également de détecter l'utilisation frauduleuse d'un chéquier : l'alerte « Information multichèques » signale qu'un nombre élevé de chèques a été émis sur un même compte, pendant une certaine période. Elle prévient les risques d'utilisation frauduleuse de chéquiers.

Il peut être consulté :

- par les bénéficiaires de chèques abonnés au service Vérifiance (FNCI - Banque de France) ;
- par toute personne qui veut savoir si les coordonnées du(des) compte(s) qu'elle détient sont enregistrées et vérifier les informations qui la concernent : c'est le droit d'accès individuel.

1 Pour plus d'information : *https://particuliers.banque-france.fr/fichiers-dincidents/les-trois-fichiers-dincidents-fcc-ficp-fnci/le-fichier-national-des-cheques-irreguliers-fnci*

système par simple lecture de la ligne codée en bas du chèque, qui lui renvoie un résultat sous forme de code d'évaluation de la régularité du chèque par exemple (un code couleur dans le cas de Vérifiance). Là encore, le commerçant est tenu d'informer ses clients du service utilisé (Vérifiance ou tout autre service de garantie de chèque) en apposant des autocollants sur ses vitrines ou à proximité de ses caisses. Dans ce cas de figure, le commerçant doit motiver son refus, en précisant de façon explicite le service utilisé.

### Les règles de vigilance applicables aux banques

Avant de délivrer un chéquier à son client, le banquier est tenu de consulter le fichier central des chèques, c'est-à-dire la base de données tenue par la Banque de France sur laquelle figurent toutes les personnes qui sont interdites d'émettre des chèques (interdiction aussi bien bancaire que judiciaire) ou d'utiliser une carte bancaire.

En sa qualité de tiré, avant de payer un chèque, la banque du tireur doit vérifier i) l'absence d'opposition au paiement du chèque ; ii) l'existence d'une provision suffisante sur le compte de son client, et iii) la présence des mentions obligatoires.

Encadré 8

## Fichier central des chèques (FCC)

Le fichier central des chèques [1] est un fichier informatique géré par la Banque de France. Il est alimenté par les banques émettrices.

Le FCC enregistre :

• les personnes qui sont interdites de chéquier parce qu'elles ont émis un chèque sans provision et n'ont pas régularisé leur situation,

• les personnes auxquelles les banques ont décidé de retirer la carte bancaire en raison d'un incident lié à son utilisation,

• les personnes pour lesquelles les tribunaux ont prononcé une interdiction d'émettre des chèques.

Le FCC peut être consulté :

• par les banques : elles sont tenues de le faire avant de délivrer un chéquier à un client. Elles peuvent aussi le consulter avant de délivrer un autre moyen de paiement ou avant d'accorder un crédit ;

• par toute personne qui veut savoir si elle y est enregistrée : ce droit d'accès individuel s'exerce auprès de la Banque de France.

1 Pour plus d'information : *https://particuliers.banque-france.fr/fichiers-dincidents/les-trois-fichiers-dincidents-fcc-ficp-fnci/le-fichier-central-des-cheques-fcc*

En outre, selon l'article L. 131-35 du CMF, la banque du tireur doit payer même après l'expiration du délai de présentation, et jusqu'à l'expiration du délai de prescription d'un an dans le cadre général (cf. encadré 3 *supra*). Ce principe d'irrévocabilité de l'ordre de payer connaît cependant une dérogation avec l'**opposition**, qui immobilise la provision entre les mains du banquier tiré.

• Cette dérogation permet ainsi au tireur, voire au porteur, de donner l'ordre au banquier tiré de ne pas payer un chèque présenté à l'encaissement. Les cas possibles d'opposition sont strictement limités par ce même article, et toute opposition en dehors des motifs de perte, de vol ou d'utilisation frauduleuse du chèque, de sauvegarde, de redressement ou de liquidation judiciaire du porteur, serait alors considérée comme illicite et pourrait entraîner des sanctions pénales.

• Toutefois, les motifs d'opposition sont interprétés strictement par les tribunaux. Dans les cas de vol ou de perte, lorsque le tireur a remis un chèque litigieux volontairement à un bénéficiaire, il ne peut prétendre, par la suite, en avoir été dépossédé contre son gré ; la perte

et le vol ne sauraient pas non plus être qualifiés dans l'hypothèse de l'envoi d'un chèque par erreur à un bénéficiaire auquel le chèque n'était pas destiné. Concernant le motif de l'utilisation frauduleuse d'un chèque, l'opposition peut être retenue dans les cas de contrefaçon ou de falsification du chèque, mais également lorsque le chèque a été obtenu et utilisé à la suite de manœuvres frauduleuses.

• Enfin, il est à noter que l'opposition en cas de procédures collectives du bénéficiaire du chèque a pour objet d'éviter, en cas de dessaisissement de ce dernier, qu'il puisse procéder à l'encaissement du chèque.

Toutes ces règles de sécurisation du chèque, concernant tant les utilisateurs (tireurs, bénéficiaires) que les banquiers, sont complétées par le **dispositif de surveillance du chèque** mis en place par la Banque de France.

En effet, au regard de l'article L. 141-4 du CMF établissant sa mission de surveillance des moyens de paiement scripturaux, la Banque de France s'assure de la sécurité du chèque et de la pertinence des normes applicables en la matière. Pour l'exercice de cette mission, la Banque de France a défini un **référentiel de sécurité du chèque** (RSC) composé d'un certain nombre d'objectifs de sécurité que les établissements sont tenus d'appliquer.

Ce dispositif de surveillance repose sur l'auto-évaluation annuelle par chaque établissement émetteur ou remettant de chèques de son degré de conformité aux objectifs de sécurité du RSC, sur la base de réponses à un questionnaire qui précise les conditions de mise en application des objectifs.

Encadré 9

### Objectifs de sécurité prévus par le référentiel de sécurité du chèque (RSC)

Le référentiel de sécurité du chèque [1] a défini neuf objectifs de sécurité.

#### Objectif 1 : gouvernance et organisation

[...] La gouvernance de la sécurité vise à assurer que les mesures de sécurité sont en place, optimales et appropriées. Les acteurs [contribuant au système de paiement par chèque] doivent disposer d'un ensemble documentaire formalisé et régulièrement mis à jour définissant ce cadre de gouvernance et l'organisation de la sécurité du système de paiement par chèque, et couvrant l'ensemble des activités associées, y compris les activités externalisées.

1 Le référentiel de sécurité du chèque est public et disponible sur le site internet de la Banque de France : https://www.banque-france.fr/sites/default/files/media/2018/03/13/cheque-referentiel-de-securite_v2017.pdf

.../...

### Objectif 2 : évaluation des risques

La gestion de la sécurité repose sur l'identification des actifs à protéger associée à une analyse des risques encourus ainsi qu'à la mise en place de mesures organisationnelles, techniques et procédurales en vue d'assurer cette protection. Elle prévoit une évaluation périodique des mesures déployées en vue de leur efficacité.

### Objectif 3 : contrôle et encadrement des risques

Les acteurs doivent mettre en œuvre des mesures de sécurité adéquates en vue d'encadrer les risques identifiés, en conformité avec la politique de sécurité de la filière.

### Objectif 4 : gestion des incidents et reporting

Les acteurs doivent disposer d'un système de surveillance des incidents relatif aux opérations et aux réclamations des clients qui permette un recensement exhaustif des incidents. Ce système de surveillance doit comprendre une procédure de remontée des incidents qui produise une information adéquate auprès des instances de gouvernance, ainsi qu'auprès des parties prenantes externes concernées.

### Objectif 5 : traçabilité et piste d'audit

Les acteurs doivent mettre en place un processus permettant une traçabilité destinée à alimenter une piste d'audit ininterrompue pour chacune des opérations couvertes par le système de paiement par chèque.

### Objectif 6 : sécurité physique du chèque

Les acteurs s'assurent de la sécurité des supports physiques du chèque tout au long de leur cycle de vie.

### Objectif 7 : sécurité des environnements des opérations

Les environnements physique et logique du système de paiement par chèque sont sécurisés, et permettent d'assurer la protection des supports physiques et logiques ainsi que des opérations exercées. Ils garantissent la qualité, la disponibilité et l'exploitabilité technique des éléments archivés.

### Objectif 8 : dispositif de surveillance des opérations

La surveillance des opérations vise à prévenir, détecter et bloquer les tentatives de paiement suspectées d'être d'origine frauduleuse. Cette surveillance doit être encadrée par une procédure formalisée définissant les règles et typologies d'alertes.

### Objectif 9 : sensibilisation des clients aux règles de sécurité

Les établissements veillent à la sensibilisation de leurs clients aux règles de vigilance relatives à la conservation d'une formule prémarquée, l'émission ou la réception d'un chèque, sa conservation et sa remise à l'encaissement.

**Le virement non connecté**

La sécurisation des ordres de virement doit prendre en compte les modes opératoires utilisés par les fraudeurs. À cet égard, les virements non connectés présentent des risques accrus :

• d'usurpation d'identité du donneur d'ordre, se traduisant par l'émission de faux ordres imitant notamment la signature du titulaire légitime et de ses éléments d'identification ;

• de modification d'ordres légitimes par le fraudeur, visant à en modifier le bénéficiaire avant leur traitement par la banque.

Pour ce faire, les fraudeurs cherchent à obtenir des informations par téléphone, par courrier ou directement en face à face en usurpant l'identité de personnels de banques ou d'organismes de l'administration publique ou en se faisant passer pour un client, un fournisseur ou même une personne de l'entourage de l'utilisateur. Tout titulaire de compte doit donc être très vigilant lorsqu'on lui demande de mettre à disposition des informations sensibles, telles que son numéro de compte ou sa carte d'identité.

Du point de vue du **payeur** (particulier, entreprise ou administration), des actions de prévention doivent être régulièrement conduites par les établissements teneurs de compte en vue de :

• sensibiliser régulièrement les clients aux différents types de fraudes par le biais de campagnes de prévention et de sensibilisation (encarts sur relevés de comptes, rendez-vous clients) ;

• assurer la mise à jour des données d'identification et d'authentification (adresse postale, numéro de téléphone, pièces d'identité, RIB/IBAN, éléments d'authentification physiques et logiciels) du client, en s'appuyant sur les procédures de sécurité prévues par la convention de compte.

Par ailleurs, les **établissements teneurs de comptes** doivent veiller à la mise à l'état de l'art de leurs dispositifs de prévention de la fraude, notamment par les actions suivantes :

• prévenir et sensibiliser régulièrement les employés aux différents types de fraudes par le biais de campagnes de prévention et de sensibilisation ;

• mettre en place des outils de validation des ordres de paiement (*scoring*) permettant de détecter, valider, alerter, temporiser ou rejeter le cas échéant des opérations présentant *a priori* des risques de fraude ;

• former régulièrement les employés aux différentes procédures à respecter pour contrer les tentatives de fraude (contrôles, alertes, contre-appels, mise en œuvre des outils de sécurisation des opérations) ;

• limiter l'acceptation des ordres de paiement sous forme de fax, document papier ou courrier et instaurer des mécanismes de double validation des opérations en fonction des montants ;

• favoriser la mise en place de listes fermées de bénéficiaires et de plafonds limitant le montant des virements pouvant être exécutés en fonction de la typologie de clientèle.

Enfin, les prestataires de services de paiement (PSP) chargés de traiter les ordres de virement sont assujettis à la **surveillance** par la Banque de France en matière de sécurité des moyens de paiement, conformément aux dispositions de l'article L. 141-4 du CMF. Ce cadre

de surveillance prévoit notamment la remise, par chaque PSP agréé en France par l'Autorité de contrôle prudentiel et de résolution, d'une annexe à leur rapport annuel de contrôle interne portant spécifiquement sur la sécurité des moyens de paiement scripturaux, et présentant les dispositifs de sécurité mis en œuvre sur l'émission de virements.

### La carte de paiement en mode non connecté

Les éléments de sécurisation des ordres de paiements par carte non connectés présentent à la fois des similitudes et des divergences avec ceux énoncés pour les virements non connectés dans la mesure où, si les canaux d'initiation sont globalement similaires, le cadre sécuritaire imposé aux commerçants qui reçoivent les ordres de paiement est moins exigeant que celui des banques ou des établissements de paiement.

Comme pour le virement non connecté, la fraude au paiement par carte en mode non connecté s'appuie sur des techniques d'usurpation de numéros de cartes pour réaliser des paiements frauduleux. La prévention de la fraude repose ainsi sur la mise en place de mesures appropriées pour protéger les systèmes qui stockent, traitent et/ou transmettent les données des titulaires de cartes ; de telles mesures de sécurité s'adressent également à l'enregistrement des appels téléphoniques, au stockage des courriers et au contrôle de l'espace physique des centres d'appels, tous susceptibles d'héberger des numéros de carte.

Les **établissements émetteurs** doivent veiller à conduire des actions de prévention auprès de leurs **porteurs de carte** (particuliers et professionnels) en vue de :

- sensibiliser régulièrement les clients aux différents types de fraudes par le biais de campagnes de prévention ;

- encourager les utilisateurs à communiquer le moins possible leurs données de carte, et plus particulièrement le cryptogramme visuel ;

- proposer des solutions intégrant des données non rejouables (par exemple, cryptogramme dynamique sur les cartes physiques) afin d'éviter tout risque de réutilisation malveillante.

Du côté des **commerçants**, leurs **prestataires de services de paiement** (établissements teneurs de comptes et acquéreurs) doivent veiller à la bonne mise en œuvre de différentes mesures de prévention de la fraude, notamment :

- dans les cas particuliers où aucune solution alternative de paiement en mode connecté n'est possible, encourager les commerçants à vérifier les éléments permettant d'identifier les clients (signatures, contrôles visuels) et à ne collecter que les données de carte strictement nécessaires à la réalisation de la transaction, en assurant la bonne qualification des transactions (en distinguant notamment les transactions MOTO des paiements en ligne) dans les systèmes de paiement ;

- s'assurer que les commerçants et, le cas échéant, leurs prestataires de service (centres d'appels, hébergeur…), respectent les normes PCI DSS pour le traitement des données de carte (transmission, stockage, archivage, destruction, etc.). Ces normes prévoient notamment la mise en œuvre d'une politique de sécurité comprenant des éléments relatifs à l'accès aux informations et aux données sensibles, à la continuité d'activité, au contrôle, à la sécurité

physique et logique, à la formation ou à la responsabilité des personnels ; elles précisent également que la conservation des cryptogrammes visuels figurant sur les cartes de paiement est proscrite ;

• prévenir et sensibiliser régulièrement les commerçants aux différents types de fraudes par le biais de campagnes de prévention.

Enfin, comme pour les virements, les prestataires de services de paiement qui offrent des services d'émission de cartes ou d'acquisition de paiements par carte sont assujettis à la surveillance par la Banque de France en matière de sécurité des moyens de paiement. L'annexe à leur rapport annuel de contrôle interne portant sur la sécurité des moyens de paiement scripturaux doit ainsi décrire précisément les dispositifs de sécurité mis en œuvre sur les activités liées aux cartes de paiement.

## Recommandations de l'Observatoire

Les modes de paiement non connectés présentent des limites avérées en termes de sécurisation, qui sont inhérentes à leurs caractéristiques : d'une part, les supports utilisés (papier, appel téléphonique…) ne permettent pas la mise en place de dispositifs avancés de sécurisation et facilitent pour les fraudeurs le recours à la falsification et à la contrefaçon d'ordres de paiement ; d'autre part, les processus de paiement associés nécessitent de nombreuses manipulations physiques et logiques, tant par le payeur et le bénéficiaire que par leurs établissements teneurs de comptes, qui multiplient les fenêtres d'opportunité pour les fraudeurs. Dans le cas du chèque, ces vulnérabilités sont aggravées par les volumes très importants de chèques et de chéquiers en circulation, avant et après utilisation, qui constituent autant de cibles potentielles, ainsi que l'intervention dans le cycle de vie de ce moyen de paiement d'acteurs présentant des niveaux de sécurité non homogènes, notamment dans les circuits d'acheminement et de distribution.

Ces vulnérabilités et la multiplication des opportunités de fraude qu'elles offrent justifient une vigilance permanente de l'ensemble des acteurs, la sécurité de ces modes de paiement ne pouvant être assurée intégralement par les acteurs professionnels du secteur des paiements.

• Du point de vue des prestataires de services de paiement, l'absence de capacité d'authentification forte du payeur au moment de la transaction rend d'autant plus nécessaire la mise en place de dispositifs avancés d'identification des transactions à risque au moment de leur traitement (c'est-à-dire de l'émission de l'image chèque ou de la saisie de l'ordre de virement ou de paiement par carte), permettant si nécessaire de temporiser les flux et d'alerter le titulaire du compte.

• L'Observatoire invite les commerçants à mettre en place les moyens de s'assurer de la régularité des transactions qu'ils initient, et notamment de veiller à un niveau adéquat de connaissance de leurs clients de façon à pallier autant que possible l'absence d'authentification forte : cela passe notamment par la prise de pièce d'identité et la consultation de services permettant de s'assurer de la validité des chèques pour les paiements en situation de proximité, ou l'analyse des paramètres de la transaction (concordance entre identité de l'acheteur et le titulaire du moyen de paiement, lieu de livraison, etc.) lors d'achats à distance. En outre, lorsqu'ils sont détenteurs de données de paiement sensibles (numéros de

carte ou IBAN par exemple), les commerçants doivent s'attacher à mettre en place des dispositifs techniques visant à en assurer la sécurité, en s'appuyant par exemple sur les exigences définies par les systèmes de paiement par carte [13]. Enfin, l'Observatoire souligne que le recours à des transactions par carte de type MOTO devrait être réservé aux seules situations de vente à distance par courrier, fax et téléphone ; toute transaction résultant d'une commande passée en situation de *e-commerce* ou de *m-commerce* devrait en effet donner lieu à un paiement en mode connecté et authentifié, conformément aux dispositions de la DSP2.

• L'Observatoire rappelle également que les utilisateurs, qu'ils soient particuliers, entreprises ou administrations, doivent rester vigilants quant à la sécurité de leurs propres moyens de paiement, en veillant à appliquer les principes énoncés en annexe 2 de ce rapport. Le respect de ces règles de vigilance est d'autant plus crucial dans le contexte de modes de paiement non connectés, dans la mesure où les autres parties prenantes disposent de leviers plus limités pour lutter contre la fraude que dans le cas de paiements connectés.

Enfin, l'Observatoire réaffirme son attachement aux actions de modernisation engagées dans le cadre de la stratégie nationale des paiements, visant à développer des solutions alternatives à l'usage du chèque et aux autres modes de paiement non connectés. Le développement de solutions innovantes et numériques, permettant de répondre aux cas d'usage qui justifient aujourd'hui l'utilisation de paiements non connectés, apparaît comme la voie la plus à même de répondre au besoin d'une meilleure sécurisation des transactions. Ainsi, le développement de solutions interbancaires et ergonomiques de paiement entre particuliers et entre entreprises reposant sur l'utilisation du virement, et dorénavant du virement instantané, ainsi que le développement des solutions de facturation électronique entre entreprises, constituent parmi d'autres des alternatives appropriées et prometteuses, à même de lever les limitations rencontrées en termes de sécurité sur ces cas d'usage spécifiques. L'Observatoire restera toutefois vigilant à ce que ces évolutions ne se fassent pas au détriment de l'accès des utilisateurs aux services de paiement dont ils ont besoin.

## 3.2 La sécurité des paiements par mobile

### Introduction

Selon le *Baromètre du numérique* 2018 [14] publié par l'Autorité de régulation des communications électroniques et des Postes (Arcep), 75 % des Français possèdent un *smartphone* [15] et près de la moitié d'entre eux l'utilisent comme équipement privilégié pour se connecter à internet. Avec l'assurance de retrouver un outil connecté dans les mains de trois Français sur quatre, les offres de services accessibles depuis le téléphone mobile se sont multipliées et les solutions de paiement utilisant ce support ne font pas exception.

Les *smartphones* se métamorphosent peu à peu en outil de paiement universel, que ce soit à distance ou en magasin, avec notamment l'équipement généralisé

13 Norme PCI-DSS pour la conservation des données de carte.

14 Cf. *https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/numerique/le-barometre-du-numerique.html*

15 Les termes « *smartphone* » et « téléphone mobile » ou encore « mobile » sont employés de manière indifférenciée tout au long de cette étude.

en technologie de communication sans contact NFC (*near field communication*, communication en champ proche) [16] par exemple. Un quart de la population française (26,2 %) a réalisé au moins un achat sur mobile en 2017 selon l'étude *Observatoire du commerce mobile* portant sur le premier semestre 2018 [17], publiée par la Mobile Marketing Association France. 5,9 % des utilisateurs de *smartphones* ont payé sans contact NFC ou par une application de paiement, soit plus de 2,1 millions de Français, ce qui place la France au niveau de l'Allemagne et de l'Italie en termes d'adoption du paiement par mobile (et légèrement en deçà de la moyenne européenne).

Une récente étude du cabinet de recherche américain Forrester [18] précise ces tendances : en Europe 80 % des transactions par téléphone mobile seraient des paiements à distance. Les transactions en magasin, également appelées transactions de proximité, passant par les systèmes de paiement par mobile, devraient croître de 26 % par an pour atteindre 27 milliards d'euros en 2022 dans sept des principaux pays européens (France, Allemagne, Italie, Pays-Bas, Espagne, Suède et Royaume-Uni). Cela représenterait 10 % de l'ensemble des paiements effectués depuis un mobile et un peu moins que le transfert d'argent entre particuliers, soit 30 milliards d'euros en 2022.

Les travaux de veille technologique conduits par l'Observatoire [19] à propos du développement de techniques de paiement de proximité par mobile en mode sans contact ont été initiés dès 2007, en anticipation de leur mise en œuvre. L'Observatoire a ainsi publié ses analyses relatives à l'évolution des mécanismes d'initiation des paiements de proximité par mobile reposant sur des technologies « carte », et à leurs conditions de sécurisation dans ses rapports annuels de 2009, 2011 et 2015. Toutefois, ces analyses n'ont pas intégré les paiements par mobile reposant sur des infrastructures non monétiques [20] dans leurs périmètres d'étude.

Cette étude vise à dresser un état des lieux de l'ensemble des technologies proposées en France permettant à un utilisateur d'initier le paiement d'un bien ou d'un service, ou encore le transfert d'argent, à l'aide de son téléphone mobile. Les enjeux de sécurité liés à la mise en œuvre des principales solutions actuelles de paiement par mobile seront présentés, en excluant i) les solutions de paiement exécutées dans l'environnement d'un navigateur internet mobile [21] ainsi que ii) les solutions de paiement par mobile faiblement voire non utilisées en France, qui pourront être décrites brièvement dans des encadrés.

## Panorama des solutions de paiement par mobile

### Paiement sur facture de l'opérateur téléphonique

Bien avant le développement des *smartphones*, les opérateurs de télécommunication ont mis en place un système de paiement pour les appels majorés et adossés à la facture mensuelle. Par la suite, avec

16 Le NFC est la technologie de communication sans fil mise en œuvre lors des paiements par carte en mode sans contact.

17 Cf. *http://www.mmaf.fr/publication/observatoire-du-commerce-mobile-1er-semestre-2018-extrait/*

18 Cf. *https://www.forrester.com*

19 Le périmètre de l'Observatoire de la sécurité des cartes de paiement a été élargi en 2016 en devenant l'Observatoire de la sécurité des moyens de paiement.

20 Les infrastructures monétiques désignent les équipements mis en œuvre pour réaliser les opérations par carte.

21 Celles-ci ne sont en effet pas spécifiques aux téléphones mobiles.

l'évolution des technologies, mais toujours en utilisant les factures mensuelles des opérateurs, les services suivants sont apparus :

- SMS+ , dédié aux messages de type SMS surtaxés ;

- Gallery, dédié aux paiements sur les boutiques de vente via le protocole WAP [22] ;

- Internet+ , dédié aux paiements sur internet mobile [23] ou en wifi [24], et permettant des achats et abonnements de contenus ou de services numériques via *smartphones*.

Pour le service Internet+ sur *smartphone*, le numéro de téléphone de l'abonné pourra lui être demandé, tout comme ses identifiants de connexion internet, notamment lorsque le *smartphone* est connecté en wifi (et donc à l'équipement du client chez lui). Si l'opérateur le juge nécessaire, il pourra envoyer un code d'authentification par SMS pour authentifier son client. L'Observatoire encourage les opérateurs mobiles à poursuivre leur suivi des réclamations et fraudes pour ce type de paiement grâce aux mécanismes mis en place, et à développer des solutions d'authentification adaptées [25].

L'Association française pour le développement des services et usages multimédias multi-opérateurs (AFMM) propose une charte déontologique appliquée à ces offres de services et intégrée dans les contrats signés entre les acteurs de la chaîne de valeur : opérateurs, agrégateurs et éditeurs de services ou contenus. Pour l'information des consommateurs, l'AFMM met aussi à disposition sur son site internet un service d'annuaire inversé qui permet de trouver l'établissement destinataire d'un paiement via les solutions Internet+ ou SMS+ figurant sur une facture [26], notamment en cas de contestation [27].

Ces modes de paiement étant mis en œuvre par les opérateurs mobiles, éventuellement à travers l'AFMM, et gérés contractuellement avec leurs clients, l'Observatoire n'en approfondira pas l'analyse dans la présente étude.

## Paiements en face à face ou sur automate

### Par communication sans contact avec la technologie NFC

La technologie de communication NFC permet le paiement sans contact de proximité et équipe ainsi désormais une majorité de terminaux de paiement en magasin. Les *smartphones* proposant cette même technologie peuvent ainsi être utilisés comme outil de paiement au point de vente [28].

22 En France, le protocole WAP, *wireless application protocol*, a été mis en œuvre pour la première fois en 1999 et apparaît maintenant sur le déclin. Il permet d'adapter des pages internet pour une consultation depuis un équipement connecté au réseau d'un opérateur mobile, comme un téléphone mobile (hors *smartphones* récents compatibles avec les protocoles standard d'internet). Tous les sites internet ne sont pas accessibles via ce protocole.

23 Utilisant donc des connexions de type 3G, 4G, ou encore 5G demain, donnant accès à internet via le réseau de l'opérateur mobile.

24 Technologie de communication sans fil de moyenne distance (quelques mètres) permettant un accès à internet, le plus souvent via une borne reliée à un réseau de communication terrestre.

25 Pour rappel, ces paiements sur facture des opérateurs sont exclus du périmètre de la DSP2.

26 Cf. *https://annuaire.infoconso-multimedia.fr/*

27 À noter que des grands éditeurs de services ou contenus bénéficiant d'une forte notoriété ont mis en place des modes de paiement similaires en contractualisant directement avec les opérateurs de téléphonie mobile. Ils n'apparaîtront pas dans l'annuaire inversé de l'AFMM et, pour toute réclamation, l'utilisateur devra s'adresser au vendeur ou à son opérateur.

28 Pour rappel, la technologie NFC (*near field communication*, communication en champ proche) permet à deux équipements distants de quelques centimètres d'échanger des informations. Tous les fabricants de terminaux de paiement proposent désormais des modèles compatibles avec une perspective de déploiement couvrant l'ensemble du parc à horizon 2020, et de plus en plus de modèles récents de *smartphones*, voire d'objets connectés tels que les montres ou bracelets, permettent d'échanger des données selon ce standard. Par ailleurs, plusieurs des spécifications de la norme de l'industrie monétique EMV reposent sur ce standard de communication.

Encadré 10

## Le retrait par mobile

En France, certains établissements bancaires ont mis en place depuis 2014 des dispositifs permettant à leurs clients de réaliser des opérations de retrait dans certains distributeurs automatiques de billets (DAB) grâce à la génération d'un code à usage unique accessible sur leur mobile.

Une phase initiale d'enrôlement au service de retrait mobile est généralement requise, pendant laquelle le client reçoit ou définit un code secret de retrait.

L'utilisateur accède ensuite au service à travers le site web ou l'application mobile de ses établissements bancaires pour définir le montant du retrait souhaité. Il obtient en retour un code à usage unique éphémère. Le code secret de retrait et le code à usage unique sont à saisir dans un DAB affilié à son établissement bancaire pour obtenir les billets.

Ce service permet de retirer de l'argent en cas d'oubli de la carte de paiement mais aussi en cas d'urgence et en guise de dépannage après le vol ou la perte de la carte. Il permet également de faciliter le retrait d'argent par une tierce personne de confiance, comme par exemple un membre de la famille en déplacement.

À l'étranger, de grands établissements bancaires ont développé des modes de retrait utilisant la technologie sans contact NFC, en équipant leurs automates de lecteurs compatibles avec cette technologie. Le retrait s'effectue alors de manière similaire à un paiement en mode sans contact au moyen d'une carte ou d'un téléphone mobile, c'est-à-dire en approchant la carte ou le téléphone du lecteur présent sur le DAB, une authentification de la carte/du téléphone ayant lieu d'une part (tout comme pour un paiement, en utilisant les dispositifs de sécurité du mode sans contact) ainsi que la frappe du code confidentiel connu du porteur sur le clavier du DAB. Les avantages du retrait sans contact avancés par ces établissements sont la réduction du temps pour réaliser un retrait et la réduction des fraudes liées à la copie de la piste magnétique des cartes de paiement (« *card skimming* » ou clonage/contrefaçon de cartes à piste).

Cependant, pour proposer un service accessible dans toutes les situations, son fonctionnement ne doit pas nécessiter une connexion permanente au réseau mobile. C'est pourquoi la mise en place de ce type de service de paiement entraîne le stockage de données de paiement qui sont réputées sensibles. L'Observatoire rappelle que ces données sensibles de paiement doivent toujours faire l'objet de mesures de protection adaptées, particulièrement au moment de leur enregistrement, de leur stockage et de leur utilisation.

Les principaux fabricants de téléphones mobiles ainsi que les

éditeurs des systèmes d'exploitation que ces équipements utilisent (Android de Google ou encore iOS d'Apple [29]) permettent le paiement sans contact au moyen de solutions de portefeuilles électroniques. Ces dernières reposent sur l'infrastructure monétique de paiement par carte sans contact [30]. Il est toutefois à noter que certains fabricants, tel Apple, restreignent l'accès aux fonctionnalités du paiement sans contact aux seules solutions qu'ils fournissent.

Dans l'environnement Android, les acteurs tiers, indépendants de Google et des fabricants de téléphones mobiles, peuvent proposer des applications qui utilisent l'antenne NFC des mobiles qui en sont pourvus. Les banques et les grandes enseignes sont alors elles aussi en mesure de proposer des applications mobiles qui intègrent le paiement de proximité sans contact ou qui sont dédiées à cet usage. En France, plusieurs banques ont développé le service « Paylib sans contact » à travers leur application de banque à distance ou via une application dédiée aux paiements par carte. La mise en œuvre de ces applications sur un parc de téléphones mobiles dont les architectures techniques diffèrent nécessite une vigilance accrue sur la protection des données sensibles de paiement. En effet, pour qu'un acteur puisse proposer une application mobile à tous ses clients, celle-ci doit pouvoir s'adapter aux différents *smartphones* disponibles. Généralement, les applications intègrent alors un ensemble de mesures de sécurité, ou d'options de sécurisation, et lors de l'installation, suivant les caractéristiques du téléphone, seulement certaines d'entre elles pourront et seront mises en œuvre.

**Par lecture de codes images**

Reposer sur l'infrastructure monétique n'est pas toujours perçu comme un avantage pour développer une solution de paiement. Certains acteurs ont alors choisi de proposer des services reposant sur la lecture d'images, plus précisément, des codes à barres dits à une dimension, compatibles avec le matériel de caisse traditionnel, ou des codes dits à deux dimensions, comme les codes « QR [31] » par exemple (cf. encadré 12), du reste de plus en plus présents sur les billets de spectacle et de transport. L'interprétation des informations contenues par ces codes permet d'enclencher une opération de paiement par carte, un virement, ou encore faire simplement l'objet d'une écriture comptable dans les livres d'un établissement de monnaie électronique [32] Ces solutions permettent de s'affranchir d'un terminal de paiement compatible avec le mode sans contact NFC et d'un *smartphone* lui aussi équipé d'une antenne NFC, mais requièrent toutefois des capacités de lecture et/ou d'affichage optique pour les équipements de paiement.

Plusieurs solutions de ce type existent, aussi bien en France (Lyf Pay ou encore Lydia) qu'à l'étranger (AliPay, WeChat Pay en Chine, Swish en Suède, etc.).

29 D'après une étude de Kantar Worldpanel portant sur les ventes du dernier trimestre de 2018, en France, la part de marché d'Android serait de 75,2 %, suivi par iOS avec 24,7 %.

30 À noter que Samsung a aussi intégré dans sa solution une technologie permettant à ses utilisateurs sud-coréens de payer avec leur téléphone mobile en émulant une carte à piste dès lors que le lecteur de piste est accessible. Ces utilisateurs peuvent donc être amenés, notamment chez un commerçant français, à présenter leur *smartphone* en face du lecteur de piste et non en face de l'antenne NFC.

31 Codes QR ou *quick-response codes*.

32 L'établissement en question propose alors une solution de paiement qui nécessite l'ouverture de comptes de monnaie électronique chez lui, à la fois par le commerçant et par le client. L'acte d'achat se traduit par le transfert d'unités de monnaie électronique du compte du client vers celui du commerçant.

Encadré 11

## Les transactions par carte avec mobile en mode sans contact

En prérequis, la communication par l'antenne NFC doit être activée. Dans le cas d'un *smartphone* Android, l'utilisateur doit choisir l'application qui prendra en charge le paiement ou a la capacité de désigner une application dite prioritaire pour ce type de service. Cette dernière se lancera alors automatiquement. L'Observatoire observe en conséquence la nécessité de laisser à la main de l'utilisateur la priorisation des applications accédant à l'antenne NFC.


En France, pour chaque transaction sans contact d'un montant supérieur à trente euros, les applications mobiles de paiement mettent systématiquement en œuvre une authentification forte de l'utilisateur. Pour des montants inférieurs, certaines applications laissent la possibilité à l'utilisateur de choisir le montant à partir duquel une authentification forte sera requise.

Du point de vue de la cinématique de paiement, l'application initie la transaction lorsque le *smartphone* est posé sur le terminal de paiement, puis requiert l'authentification du porteur. La validation du paiement se fait ensuite en approchant une seconde fois le *smartphone* du terminal.

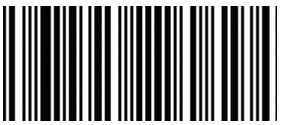

Dans ce cadre, l'authentification de l'utilisateur peut reposer sur la vérification d'un code confidentiel (appelé ici mPIN pour *mobile PIN*) ou d'une caractéristique biométrique (empreinte digitale ou reconnaissance faciale par exemple).

Plusieurs variantes de cette cinématique peuvent exister : par exemple, l'utilisateur peut ouvrir son application et s'authentifier sur son mobile avant de le présenter au terminal de paiement pour finaliser l'opération en un seul mouvement du *smartphone* sur le terminal de paiement. Une autre possibilité, qui n'est pas mise en œuvre par les établissements français, consiste à approcher le *smartphone* une seule fois du terminal et à requérir la saisie du code confidentiel sur le terminal de paiement.

Encadré 12

## Les transactions par lecture d'image

Des technologies de stockage d'information peuvent être appliquées à des images, dont voici quelques exemples.



Code à barres

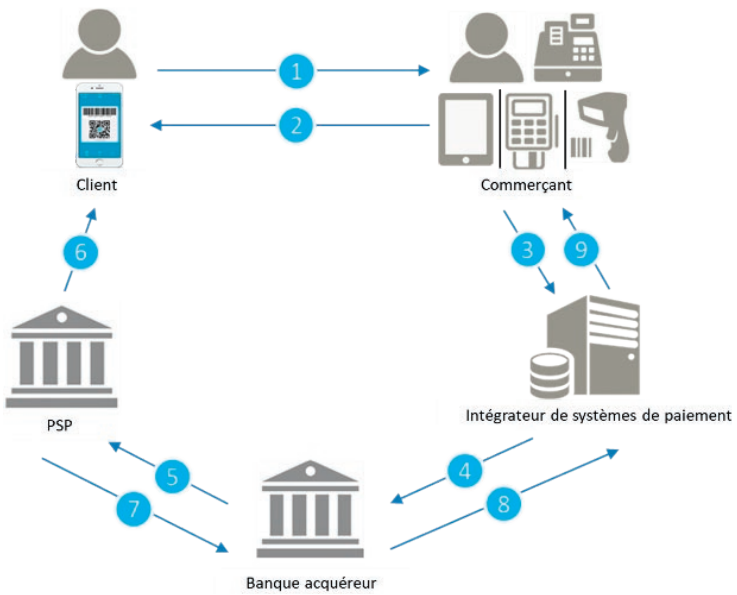
PDF417

Code datamatrix

Code QR

Plusieurs méthodes de paiement peuvent être utilisées dans le cadre de solutions de paiement mettant en œuvre la lecture de telles images.

La première consiste pour le commerçant à scanner une image, faisant office d'identifiant unique de l'acheteur, présenté par celui-ci à partir d'un support physique ou d'un mobile au moment de valider un paiement. Le terminal du commerçant envoie ensuite une demande d'autorisation à l'établissement teneur du compte du client. Le portefeuille électronique de l'acheteur est alors débité du montant de la transaction et une notification est envoyée sur son application mobile.




1. Le client présente l'image à scanner.
2. Le commerçant scanne l'image avec son équipement.
3. Le système d'information du commerçant transfère les informations relatives à l'image à son intégrateur de système de paiement.
4. L'intégrateur transmet une demande de paiement à la banque acquéreur, la banque du commerçant.
5. La banque acquéreur transfère la demande de paiement au prestataire de service de paiement (PSP) du client.
6. Le PSP fait parvenir une notification à son client.
7. Le PSP envoie une confirmation de paiement à la banque acquéreur.
8. La banque acquéreur transfère la confirmation de paiement à l'intégrateur.
9. L'intégrateur transmet au système d'information du commerçant la confirmation du paiement.

.../...

La cinématique inverse, consistant à utiliser une image statique identifiant le commerçant, peut se rencontrer hors de France, notamment en Asie. Dans les deux cas, la sécurité du dispositif est relativement faible puisque l'image employée peut être copiée et réutilisée.

La deuxième méthode de paiement envisageable consiste à renforcer la sécurité de la transaction en utilisant des images à usage unique. Si le circuit de vérification de l'image déclenchant le paiement est identique, des éléments d'authentification de l'application qui l'a générée ainsi que des données de la transaction, voire du client ou du commerçant selon celui qui présente l'image en lecture, sont ajoutés au contenu de l'image. Des mécanismes cryptographiques permettent de garantir l'intégrité des données ainsi générées et vérifiées par les parties.

**Usages innovants**

En complément de ces dispositifs, d'autres usages du téléphone mobile dans le cadre des paiements en magasin apparaissent. Ainsi, certains mettent en œuvre des technologies traditionnellement rencontrées pour les paiements à distance dans des environnements de paiement en magasin, notamment grâce à la géolocalisation permettant la détection de l'entrée et de la sortie d'un magasin, et donc le déclenchement du paiement le cas échéant.

## Paiements intégrés aux applications

Le développement des services mobiles a nécessité la mise en place de solutions de paiement qui puissent être directement intégrées au sein d'une application donnée

Encadré 13

### Deux autres technologies utilisées pour le paiement de proximité par mobile

D'autres technologies sont mises en œuvre par des solutions peu présentes en France, dont deux en particulier.

• Le BLE (*bluetooth low energy*, Bluetooth basse consommation), aussi appelé Bluetooth 4.0 : notamment utilisée dans les pays scandinaves, cette technologie de communication autorise une distance de quelques dizaines de centimètres, et demande que les équipements soient autoalimentés en énergie, ce qui exclut les cartes de paiement. L'utilisation de cette technologie requiert que le terminal du commerçant soit équipé d'une balise compatible, ce qui nécessite généralement un dispositif supplémentaire dédié.

• Les ondes sonores : cette technologie repose sur les ondes sonores émises et reçues depuis les mobiles pour véhiculer les informations de paiement. Les données chiffrées circulent depuis les haut-parleurs jusqu'aux micros. La transaction initiée par l'appareil du marchand génère une onde sonore contenant des données chiffrées concernant le paiement. Le téléphone du client reçoit ces ondes, l'algorithme les reconvertit en données numériques et achève la transaction. Les ondes sonores produites pour réaliser chaque transaction sont uniques et les perturbations lors de la transmission des ondes sont gérées par des codes de détection d'erreurs.

pour offrir un parcours client fluide. On parle alors de paiement « in-app ». Dans ce contexte, ce sont de véritables portefeuilles électroniques qui sont utilisés au sein de l'application en question. L'Observatoire a publié une étude portant sur la sécurité des portefeuilles électroniques dans son rapport annuel de 2011 et dont les enseignements principaux demeurent valides.

Deux types de portefeuilles électroniques intégrés aux applications peuvent exister : ceux appartenant aux commerçants et ceux provenant d'acteurs tiers.

**Applications intégrant des portefeuilles commerçants**

Ces solutions intégrées reposent sur l'enrôlement des clients et l'enregistrement des données de leurs cartes (numéro, date d'expiration et cryptogramme visuel) auprès d'un PSP ou d'un prestataire technique du commerçant. L'Observatoire recommande aux utilisateurs de ces services de s'assurer que l'application provient bien du commerçant souhaité avant d'y renseigner leurs informations de paiement.

Dans ce contexte, même si certaines solutions traitent les opérations de paiement immédiatement, d'autres regroupent les transactions pour envoyer des fichiers consolidés *a posteriori*, de nuit ou à heure fixe. Dans ce dernier cas, l'authentification forte du porteur par sa banque n'est pas possible.

**Applications intégrant des portefeuilles tiers**

Les PSP mettent aussi à disposition des commerçants des interfaces leur permettant d'intégrer leur solution de portefeuille électronique au sein des applications. De cette manière, le commerçant se repose sur les mesures de sécurité mises en œuvre par le portefeuille électronique du PSP.

**Mesures de sécurité appliquées à ces applications**

Les mesures de sécurité appliquées à ces applications sont celles directement liées aux portefeuilles électroniques qu'elles intègrent. Comme détaillé dans l'étude de 2011, elles doivent donc principalement couvrir :

- la protection des données sensibles de paiement (numéros de carte, date d'expiration, cryptogramme visuel), qui doit être adaptée aux environnements techniques des téléphones mobiles ;

- l'enrôlement de la carte de paiement, ce qui est généralement assuré par l'authentification du porteur à l'enregistrement de celle-ci ;

- l'utilisation frauduleuse de l'application et donc du portefeuille électronique, souvent pris en compte dans le cadre du suivi de l'activité des utilisateurs, au besoin en déclenchant une authentification forte en cas de suspicion de fraude [33].

## Paiement entre particuliers

Les modes de paiement décrits précédemment sont adaptés au paiement d'un professionnel ou d'un commerçant mais, à de rares exceptions près, ces solutions ne couvrent pas le paiement entre particuliers, aussi appelé transfert d'argent, ou de fonds, entre particuliers (P2P – *person to person*). Trois types d'offre permettent à des particuliers de s'envoyer des fonds : i) en s'échangeant des unités de monnaie

33 La DSP2 dispose que, pour toute transaction à l'initiative du porteur, l'émetteur qui le juge nécessaire doit être en mesure d'authentifier fortement son client.

électronique, ii) par virement et iii) par carte.

**Par monnaie électronique**

Pour offrir ce service, une des approches consiste à ouvrir des comptes de monnaie électronique (ME) auprès d'un établissement agréé. Le transfert d'argent entre les comptes de paiement de deux clients d'un même établissement se traduit par une écriture comptable sur les livres de compte du PSP. Pour faciliter leur utilisation, les établissements de monnaie électronique mettent à disposition de leurs clients une application mobile permettant de consulter le solde du compte, d'accéder à l'historique des opérations et de réaliser des transferts de fonds. Ce fonctionnement est notamment celui des solutions proposées par Lydia, S-money, Pumpkin, Leetchi et, dans sa configuration initiale, Paypal.

L'Observatoire rappelle que cette activité nécessite un agrément auprès de l'Autorité de contrôle prudentiel et de résolution (ACPR).

**Par virement**

Une autre approche consiste à effectuer un virement au destinataire du paiement. Pour ce faire, l'identifiant de compte de ce dernier (IBAN – *international bank account number*) est requis. En France, une large majorité des établissements qui proposent des services de paiement aux particuliers ont mis en place une application mobile de banque en ligne qui permet ce type de service. En complément, certaines banques proposent le service « Paylib entre amis » qui permet de verser des fonds à un particulier à partir de son numéro de téléphone portable (le service assurant la correspondance avec l'identifiant de compte). L'arrivée du virement instantané [34] pourra encourager ce type d'usage.

**Par carte de paiement**

Les systèmes de paiement par carte, notamment Visa et MasterCard, ont développé des fonctionnalités permettant de créditer sous trente minutes le compte d'un particulier à partir des données de sa carte. Pour assurer un niveau de sécurité satisfaisant, les entreprises qui souhaitent utiliser cette fonctionnalité doivent y être autorisées par le réseau concerné. Ainsi, Leboncoin et Vinted, deux plateformes qui permettent à des particuliers de mettre en vente des biens ou services, proposent à leurs utilisateurs ce type de service.

## Enjeux sur la sécurité des paiements par mobile

L'enjeu majeur de sécurité pour les paiements par mobile concerne la protection des données utilisées pour initier les transactions. L'innovation et la maturité des solutions de sécurisation des données ont contribué sensiblement à l'essor récent des paiements par mobile. Toutefois, il n'existe pas de solution de sécurisation universelle. Chaque contexte de paiement par mobile présenté au chapitre précédent nécessite des dispositifs de sécurisation différents.

En paiement de proximité ainsi qu'en paiement entre particuliers avec un mobile, le mode d'usage le plus répandu à ce jour est le paiement sans contact reposant sur l'infrastructure monétique, avec l'utilisation d'un portefeuille électronique associé à un canal de communication. Ce dernier utilise en majorité la technologie NFC (pour le paiement

34 Au sein de l'espace SEPA, le virement instantané, ou SCT inst (*SEPA Instant Credit Transfer*), permet de virer des fonds sur un compte destinataire en moins de dix secondes.

de proximité) ou celle des codes QR pour réaliser une transaction :

- la sécurisation des paiements par mobile via le canal NFC implique à la fois de sécuriser le système d'exploitation et les applications de paiement, ainsi que les éléments physiques du *smartphone*, notamment l'interface de communication sans contact ;

- les mesures de sécurisation des paiements par mobile par code QR (*quick-response*, réponse rapide) se concentrent essentiellement sur la protection des applications de paiement et des codes QR générés.

## Rappel des recommandations de l'Observatoire applicables aux paiements par mobile

L'Observatoire a formulé des recommandations relatives aux paiements par mobile dans ses rapports annuels de 2007, 2009, 2012 et 2015.

Si l'Observatoire encourage les acteurs à innover dans le domaine des paiements de proximité par mobile, il rappelle toutefois que le déploiement d'une telle solution de paiement doit être conditionné à l'assurance d'un niveau de sécurité équivalent à celui des paiements par carte en mode sans contact. Pour ce faire, l'Observatoire avait souligné le besoin de disposer de référentiels de sécurité adaptés à ces nouveaux dispositifs de paiement de proximité, et permettant d'évaluer et de certifier les solutions proposées. Des certifications portant sur la sécurité des dispositifs dans leur ensemble et sur la totalité du cycle de vie ont vu le jour ces dernières années. L'Observatoire encourage le développement de ces initiatives qui doivent pouvoir prendre en compte toutes les nouvelles fonctionnalités apportées par les solutions disponibles.

À cet effet, l'Observatoire relevait la nécessité de disposer d'expérimentations pilotes, associant émetteurs de cartes et systèmes de paiement par carte, pour la mise en œuvre de nouvelles fonctionnalités et permettant de tester les modalités de sécurisation des différents modèles d'infrastructures envisagés, sur l'ensemble de leur cycle de vie. Ces expérimentations s'attachent à évaluer le niveau de sécurité global offert par les solutions, dans un cadre contractuel protecteur à l'égard des porteurs pilotes de ces solutions en cas de fraude ou de problème technique.

Par ailleurs, l'Observatoire rappelait son attachement au développement de solutions de « tokenisation [35] », qui sont à même d'apporter un niveau de sécurisation supplémentaire en réservant l'utilisation du numéro de carte à l'utilisation en mode contact et en limitant la circulation des données sensibles de paiement. Cette recommandation est devenue une obligation imposée par les réseaux de carte de paiement et a été mise en œuvre dans les différentes solutions proposant le paiement carte par mobile en magasin.

L'Observatoire rappelle son attachement au chiffrement des communications entre le mobile et le terminal de paiement même si le risque lié au vol de données est limité par le recours aux techniques de « tokenisation ». Le standard EMV (Europay Mastercard VISA) [36] actuel utilisant la technologie NFC ne prévoit pas cette possibilité ; cette fonctionnalité devrait être disponible dans le cadre de la future mise à jour du standard EMV, dite *EMV second*

35 Technique permettant d'utiliser un jeton, ou *token*, à usage unique ou limité dans le temps, qui est associé aux données de carte nécessaires à un paiement.

36 Les normes EMV sont utilisées par l'industrie pour une large majorité des spécifications techniques régissant le fonctionnement des paiements par carte.

*generation*. Il est toutefois à noter que l'implémentation de ce nouveau standard supposera une mise à niveau des terminaux, et entraînera donc une migration significative sur plusieurs années.

## Enrôlement d'un instrument de paiement dans un portefeuille électronique

À ce jour, l'enrôlement d'au moins un instrument de paiement dans le portefeuille électronique est nécessaire afin de pouvoir l'utiliser pour le règlement d'un achat. Il existe par ailleurs des portefeuilles électroniques proposés essentiellement par des établissements bancaires ou de monnaie électronique qui autorisent le paiement par virement bancaire.

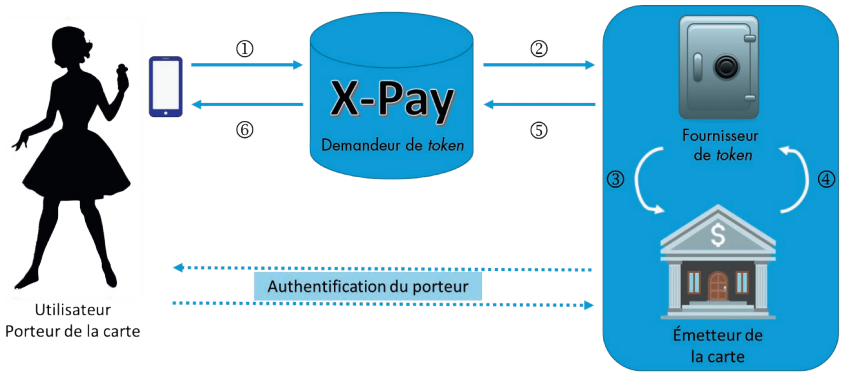
L'enrôlement d'une carte dans un portefeuille électronique consiste à récupérer les données inscrites sur la carte, soit par reconnaissance des caractères à partir d'une photo soit par une saisie manuelle par le porteur. Les capacités NFC du *smartphone* et de la carte pourraient également être mises en œuvre dans ce cadre afin de simplifier davantage l'expérience utilisateur [37].

Dans le cadre d'un usage en magasin et afin de mieux sécuriser le paiement par carte qui en résulte, les portefeuilles électroniques utilisent

37 En raison des mesures de protection des transactions de paiement sans contact, seules certaines données de la carte pourraient ainsi être récupérées (numéro de carte mais pas le nom du porteur par exemple).

Encadré 14

### Tokenisation d'une carte




1. Pour enrôler une nouvelle carte, l'application mobile émet une demande de *token* contenant les données d'identification de la carte, à savoir son numéro, sa date d'expiration et son cryptogramme visuel.
2. Le TR (*token requestor*, demandeur de *token*) demande la génération d'un *token* au TSP (*token service provider*, fournisseur de *token*) de la banque émettrice de la carte.
3. Le TSP demande à l'émetteur de valider la demande, notamment en vérifiant les données de la carte et si celle-ci n'est pas en opposition.
4. L'émetteur valide la demande de *token*.
5. Après avoir généré un nouveau *token*, le TSP transmet celui-ci au TR.
6. Le TR transmet le *token* à l'application mobile pour qu'elle puisse l'utiliser en lieu et place du numéro de la carte enrôlée.

Lors de cette opération, l'émetteur demande généralement à son porteur de s'authentifier en confirmant qu'il est bien à l'origine de la demande de *token*. Cette phase peut être mise en place de différentes manières, suivant le portefeuille électronique.

les techniques de « tokenisation ». À partir du numéro d'identification de la banque [38], le demandeur de *token* (TR – *token requestor*) envoie une requête au fournisseur de *token* (TSP – *token service provider*) pour l'émetteur de la carte. Ce TSP est généralement l'émetteur lui-même ou l'un de ses prestataires. Pour que la génération de cet alias au numéro de carte, le *token*, puisse avoir lieu, il faut notamment que le service de « tokenisation » compatible avec le portefeuille électronique ait été mis en place et que le résultat de l'analyse de risque dédiée au processus d'enrôlement soit conforme aux critères fixés par l'émetteur. Sauf exception, les établissements mettent en œuvre une solution d'authentification pour s'assurer de la légitimité des demandes de *token*.

Plus précisément, le TSP fournit un *token*, qui n'est valable que pour une période limitée et uniquement dans le cadre de l'utilisation dudit portefeuille électronique, ainsi que d'autres éléments de sécurité adaptés aux portefeuilles électroniques, comme des clés cryptographiques par exemple. Ces éléments entrent dans le dispositif mis en œuvre par l'éditeur du portefeuille électronique afin de protéger les données sensibles (par des techniques de chiffrements) et d'authentifier le mobile.

## État de l'art des solutions de sécurité des paiements par mobile

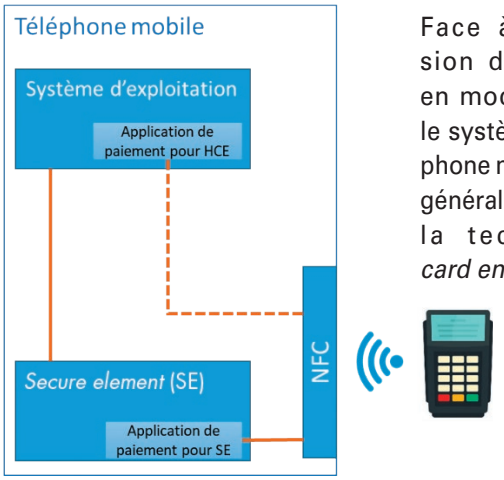
Le paiement par mobile en magasin se généralise lentement, toutefois, les exigences de sécurité liées aux cartes de paiement à puces sont plus élevées que ce qui est mis en œuvre par la plupart des applications fonctionnant sur un téléphone mobile.

Afin d'atteindre un niveau de sécurité similaire aux cartes à puce, les premières solutions techniques proposées étaient toutes centrées sur l'utilisation d'un élément sécurisé physique (SE – *secure element*). Ces solutions permettaient d'atteindre

38 Le numéro d'identification de la banque, BIN – *bank identification number*, désigne les six premiers chiffres du numéro d'une carte.

Schéma 1

SE (*secure element*, élément sécurisé physique) et HCE (*host card emulation*)




Face à cette lente progression du paiement par mobile en mode sans contact, en 2013, le système d'exploitation sur téléphone mobile Android a contribué à généraliser une solution alternative, la technologie HCE (*host card emulation*).

Note : SE : ***secure element***, élément sécurisé physique ; HCE : ***host card emulation***, service intégré au système d'exploitation du mobile permettant de dialoguer directement avec l'interface NFC (***near field communication***, communication en champ proche).

un niveau de sécurité certifié très élevé mais leur complexité de mise en œuvre, tant sur le plan technique mais aussi organisationnel et commercial, a été un frein majeur à leur déploiement.

HCE se définit comme un service intégré au système d'exploitation du mobile permettant à des applications logicielles installées dans le mobile, via des interfaces dédiées (API), de dialoguer directement avec l'interface NFC. La sécurisation du paiement par mobile repose alors sur les composants de sécurité fournis par le système d'exploitation. Ces composants logiciels n'offrent pas le même niveau de sécurité qu'un élément sécurisé physique. Des mesures de sécurité compensatoires sont alors mises en œuvre. Les plus couramment adoptées à ce jour par l'industrie du paiement pour limiter l'exposition des données de paiement aux risques induits par HCE sont les techniques de brouillage [39] des données et des applications, ainsi que la « tokenisation ». Le procédé de « tokenisation » est efficace à condition de stocker les *tokens* dans un espace réputé de confiance sur le téléphone.

Une deuxième technologie, dite TEE (*trusted execution environment*), se détache également parmi les mesures de sécurité compensatoires proposées. Le TEE est une solution logicielle intégrée dans un certain nombre de *smartphones*, qui consiste en un environnement d'exécution proche du niveau de sécurité d'un SE, en fournissant des espaces mémoire et de stockage sécurisés pour les applications. Ainsi, lorsque l'application de paiement s'exécute, celle-ci (ou la partie de l'application la plus sensible) est isolée, par le TEE, du reste des applications en cours d'exécution sur le téléphone mobile.

Les solutions à base de SE, HCE et TEE permettent de sécuriser les paiements sans contact et ne peuvent fonctionner qu'en la présence d'un contrôleur NFC, antenne de communication sans fil avec le terminal de paiement. Pour des raisons de coûts, il est rare de trouver un tel composant dans les *smartphones* d'entrée de gamme. C'est pourquoi un certain nombre de fournisseurs de services ont fait le choix de développer des solutions de paiement basées sur le code QR, qui présente l'avantage de fonctionner sur la quasi-totalité des *smartphones*. La mise en œuvre de ce type de paiement est le plus simple pour les consommateurs, puisqu'une fois l'application compatible installée sur le *smartphone*, la seule photo d'un code QR prise avec la caméra du *smartphone* suffit pour initier un paiement (ou la présentation sur l'écran du *smartphone* d'un tel code généré par l'application, pour lecture, par le terminal du commerçant). Les sections suivantes présentent les principes de fonctionnement des technologies SE, HCE, TEE et code QR, ainsi que leurs avantages et leurs inconvénients.

### Éléments sécurisés physiques (SE – *secure element*)

De manière générale, les premières solutions de paiement par mobile en proximité ont positionné le SE comme un composant central par lequel passe nécessairement toute les communications NFC, en particulier une transaction de

39 Dans ce contexte, les termes d'obscurcissement, d'offuscation et d' « obfuscation » peuvent aussi être utilisés. Ces techniques consistent à protéger les applications contre des attaques dite de « *reverse-engineering* », permettant à une personne malveillante d'interférer avec le bon déroulé d'une application de paiement et par exemple d'autoriser la non-exécution de l'étape d'authentification du porteur. Pareillement, les données sensibles peuvent être stockées de manière fragmentée dans la mémoire de l'appareil, empêchant ainsi leur récupération aisée par un attaquant.

paiement sans contact. Pour ce faire, le protocole SWP (*single wire protocol*), a été développé pour sécuriser les échanges entre le composant NFC du mobile et le SE. Ces solutions sont appelées *SE-centric*.

Pour effectuer des transactions sécurisées, un certain nombre d'opérations doivent être protégées, par exemple l'authentification, la signature et la validation par code PIN. C'est le rôle du SE, qui offre des services de traitement cryptographique et une mémoire sécurisée pour stocker les informations secrètes, telles que les mots de passe, les clés de chiffrement et les données personnelles.

Le SE est un composant hautement sécurisé qui utilise les mêmes principes de sécurité que les puces des cartes de paiement. Il assure les fonctions d'authentification des transactions, de protection des données et de sauvegarde des applications sécurisées telles que le paiement, le contrôle d'accès ou le contrôle d'identité électronique.

Dans un téléphone mobile, il peut prendre plusieurs formats : une carte SIM, un composant du téléphone ou une carte mémoire.

### Trois choix d'architecture proposant des composants de sécurité physiques de type SE

Les solutions reposant sur la technologie du SE sur cartes SIM (SIM-NFC) sont distribuées et gérées en partenariat avec les opérateurs mobiles, qui peuvent permettre aux fournisseurs de service de paiement par mobile d'utiliser la carte SIM. Les opérateurs mobiles ont été parmi les tout premiers promoteurs des applications NFC sécurisées et c'est tout naturellement leurs cartes SIM qui sont utilisées à titre de SE. En développant une infrastructure pour en gérer les droits d'accès via leurs réseaux mobiles, et en s'appuyant sur des standards communs conçus à travers des instances internationales, les opérateurs mobiles représentent une très large majorité du marché en volume. L'avantage principal de ce format réside dans l'hébergement des applications directement dans le SE qui est lui-même intégré dans la carte SIM. Dans le cas d'un vol ou d'une perte de la carte SIM, les données sensibles restent protégées. L'inconvénient principal du format SIM-NFC est la quantité de mémoire disponible, qui peut s'avérer insuffisante pour le bon fonctionnement de certaines applications installées dans le SE.

Les SE dits « embarqués » (eSE – *embedded secure element*) sont de plus en plus souvent présents dans les nouveaux téléphones équipés d'une antenne NFC. Le eSE peut être intégré dans le contrôleur NFC, dans le microprocesseur du téléphone ou bien dans un composant distinct. Cette configuration d'eSE permet aux fabricants de mobiles d'offrir leurs propres services NFC sécurisés en se passant de la carte SIM comme moyen de sécurisation. Les fournisseurs de services de paiement reposant sur cette technologie bénéficient de performances accrues grâce à l'intégration du SE comme composant du téléphone. Si un partenariat avec les opérateurs mobiles n'est alors plus nécessaire pour les fournisseurs de services de paiement, ils se doivent d'en développer avec chaque fabricant de téléphone mobile ou, *a minima*, avec les leaders du marché visé.

Les SE sur carte mémoire enfichable au format microSD (SD-SE) offrent une alternative aux technologies proposées via les opérateurs et les fabricants, mais sont très peu utilisés.

### Une mise en œuvre du paiement faisant intervenir plusieurs acteurs

Ces trois formats de SE peuvent générer des relations

d'interdépendance entre les acteurs du marché et ainsi rendre l'écosystème complexe à mettre en œuvre.

Parmi les solutions déployées, par exemple le modèle centré sur une SIM-NFC, appelé aussi *SIM-centric* et lancé en France il y a déjà quelques années, le parcours de souscription requiert pour le client de détenir un *smartphone* équipé d'une antenne NFC, d'une carte SIM intégrant un SE et d'un abonnement téléphonique auprès d'un opérateur mobile partenaire de sa banque. L'opérateur mobile, propriétaire de la carte SIM, vérifie l'éligibilité au service NFC sollicité afin de permettre à la banque l'administration à distance du service de paiement sur la carte SIM. Un partenariat entre l'opérateur et la banque est donc nécessaire en amont. La banque peut alors avoir accès à un domaine sécurisé sur la carte SIM du client pour lui délivrer le service de paiement mobile.

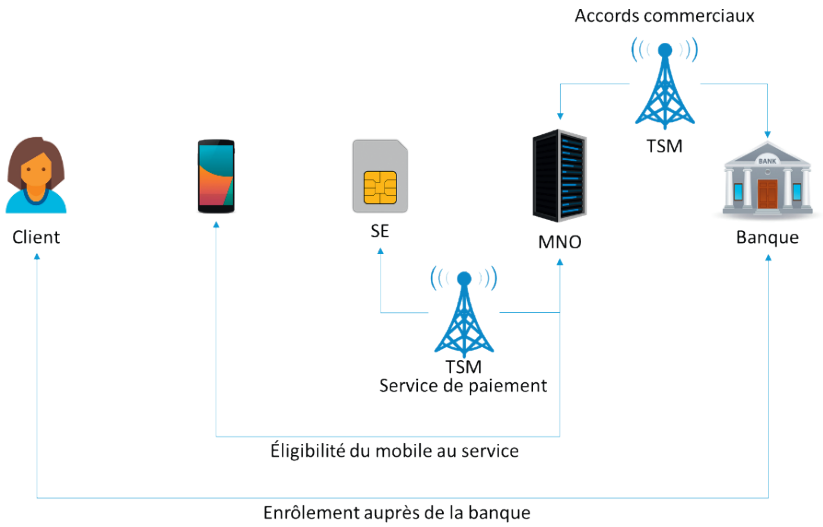
Ce modèle a imposé un nouvel acteur, le TSM (*trusted service manager*, gestionnaire de services de confiance), en charge d'être l'interface de confiance entre les différents acteurs du fonctionnement d'une application NFC sécurisée : il gère les relations techniques entre l'opérateur mobile, la banque et les autres fournisseurs de services sécurisés pour mettre à disposition, télécharger et maintenir les applications dans le mobile de l'utilisateur final.

La multiplicité des acteurs impliqués a toutefois entraîné des problèmes d'interopérabilité sur le terrain, malgré les efforts de standardisation dans le domaine. La lente convergence des solutions vers un cadre normalisé éprouvé (cas d'usages et parcours client) a constitué l'un des obstacles majeurs à la généralisation du paiement NFC par mobile reposant sur ces technologies.

Face à ces obstacles, certains acteurs du marché ont développé une alternative aux solutions de type SE, en introduisant la technologie HCE.

Schéma 2

Les acteurs du service de paiement mobile NFC pour un modèle *SIM-centric*




Note : SE – ***secure element***, éléments sécurisés physiques ; TSM – ***trusted service manager***, gestionnaire de services de confiance.

Les acteurs du service de paiement mobile sont connus sous le nom « MNO » (*mobile network operators*, opérateurs de téléphonie mobile).

### *Host card emulation* (HCE)

Les premières spécifications du HCE ont été proposées en 2012 mais c'est l'adoption par Google au sein du système d'exploitation Android fin 2013 qui a rendu cette technologie d'émulation logicielle de carte de paiement largement diffusée.

L'architecture HCE permet de s'affranchir du SE comme composant central et modifie le modèle établi jusqu'alors par les architectures reposant sur un SE, en particulier celui des solutions SIM-centric, en introduisant une couche logicielle spécifique entre d'une part le contrôleur sans contact NFC et tout autre composant physique présent sur le mobile et, d'autre part, les applications de paiement du mobile. Le rôle de l'opérateur de téléphonie mobile se limite alors à son rôle de fourniture et de gestion des canaux de communication avec le mobile pour l'acheminement des données. Le rôle du TSM dépend alors de la solution retenue pour héberger les données sensibles de l'application bancaire.

#### Une technologie permettant une approche sécurisée flexible

En effet, la technologie HCE offre plus de flexibilité pour l'hébergement des données sensibles associées à l'application de paiement : i) dans l'application elle-même ; ii) dans un SE [40] ou dans un environnement sécurisé du mobile (par exemple, TEE – *trusted execution environment*, environnement d'exécution de confiance) ; iii) dans l'internet en nuage (solution appelée *SE in the cloud*) :

- le stockage des données sensibles dans l'application de paiement est une approche qui demande une grande vigilance en termes de sécurisation et nécessite souvent de combiner plusieurs types de mesures telles que, par exemple, les techniques de brouillage et de chiffrement (en apportant une attention particulière à la gestion des clés cryptographiques utilisées) ;

- si la solution retenue repose sur l'utilisation d'un SE ou d'un service TEE, le TSM garde alors la maîtrise de l'administration des données et des clés cryptographiques ;

- en revanche, un TSM n'est plus nécessaire dans l'hypothèse d'un scénario d'implémentation de type *SE in the cloud*, où la gestion des données sensibles est directement prise en charge par un service distant.

#### *SE in the cloud* : une carte de paiement logicielle sécurisée et hébergée à distance

Les SE hébergés sur un serveur distant sont des solutions reposant sur une émulation de carte de paiement logicielle, n'utilisant pas d'élément sécurisé physique sur le mobile mais requérant une connexion internet mobile. Ces solutions, de plus en plus fréquentes, s'appuient sur un environnement sécurisé intégré au téléphone, le TEE, ou sur un élément sécurisé logiciel minimal à bord du téléphone, pour accéder à un serveur réseau qui joue le rôle d'élément sécurisé complet. Les clés, certificats et droits des transactions sont ainsi gérés à distance sur ce serveur sécurisé, permettant de s'affranchir des capacités de sécurité du *smartphone*, mais aussi des opérateurs de téléphonie mobiles et des fabricants de *smartphones* pour opérer le service. Il en résulte une plus grande souplesse d'utilisation et une adaptation plus aisée à des générations de *smartphone* variées.

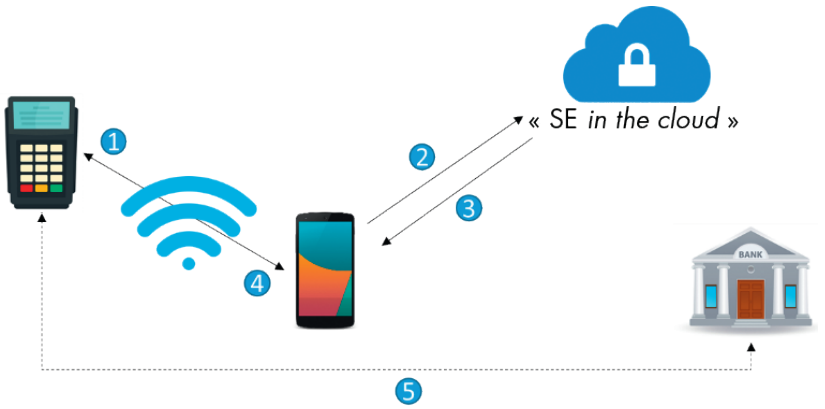
Dans le cas d'une solution HCE de type *SE in the cloud*, la cinématique

40 Conceptuellement, une application HCE peut se limiter à une fonction de routage de commandes exécutables par une application résidant dans le SE (dans ce cas le SE héberge l'application et les données).

de paiement doit toutefois tenir compte des conditions de couverture réseau pour dérouler une transaction, selon l'environnement : soit en mode connecté (A), soit en mode déconnecté (B).

Schéma 3

HCE SE *in the cloud* – paiement en mode connecté




**(A) En mode connecté**, la transaction s'exécute de façon synchronisée avec le serveur *SE in the cloud*. À l'approche du terminal de paiement électronique (TPE), le mobile transmettra la requête sans contact vers l'application hébergée dans le système d'exploitation (1). L'application gère ensuite l'appel vers le serveur distant hébergeant l'élément sécurisé virtuel (2) afin de récupérer en temps réel les données nécessaires pour réaliser une transaction EMV et les fournir au contrôleur NFC du mobile (3). Celui-ci les transmettra à son tour au TPE (4). Pour sécuriser la transaction, certaines données, comme le numéro de carte, sont ici également issues d'un service de « tokenisation ». Ce dernier génère des numéros à usage unique empêchant ainsi toute réutilisation des mêmes données à des fins de fraude. Le reste de la transaction se déroule de façon identique à un paiement par carte à puce en mode sans contact, qui se termine en transmettant la transaction au prestataire de service du commerçant (5). HCE et son mode *SE in the could* ne concerne en effet que l'acquisition sans contact de données d'une carte de paiement dématérialisée et stockée à distance.

**(B) En mode déconnecté**, il suffit de scinder la phase initiale de récupération des données de l'application de paiement NFC (réalisée en mode connecté) de la phase ultérieure de réalisation de la transaction utilisant ces données préalablement récupérées (réalisée en mode déconnecté). La première est réalisée en mode connecté en interrogeant le serveur distant (1) qui renvoie les données utiles à une ou plusieurs transactions (2), celles-ci étant alors chargées sur le mobile. Au moment de réaliser la transaction sans contact (3), ces données chargées sur le mobile sont utilisées, la connexion au réseau de l'opérateur mobile n'étant plus requise, et la transaction peut aboutir comme précédemment (5).

À défaut de disposer d'un espace suffisamment sécurisé dans le mobile, il est cependant nécessaire de limiter, par exemple dans le temps, l'utilisation possible de ces données chargées dans le mobile. Des exigences ont notamment été développées en la matière par les systèmes de paiement par carte tels Visa et MasterCard.

Schéma 4

*HCE SE in the cloud* – récupération des données de paiement en mode connecté

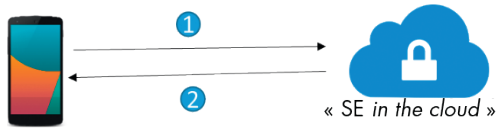
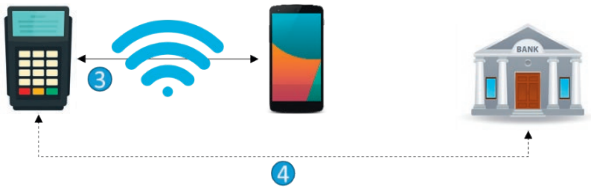



Schéma 5

*HCE* SE *in the cloud* – paiement en mode déconnecté




***Trusted execution environment* (TEE)**

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

Le rôle d'un TEE est plus précisément de protéger les données (clés cryptographiques, mots de passe, données bancaires tels des identifiants de carte, de compte de paiement, etc.) et les applications sensibles des attaques internes et externes au téléphone, en garantissant leur séparation du reste de l'environnement du téléphone, ainsi qu'un accès sous contrôle.

De par ses caractéristiques, les TEE sont donc particulièrement adaptés aux usages bancaires et notamment aux applications de paiement par mobile.

**Code QR**

La technologie de paiement par mobile sans contact avec code QR est accessible à tous les possesseurs de *smartphones*, y compris ceux dépourvus de contrôleur et d'environnements sécurisés tels que décrits précédemment. Elle repose sur une application de paiement, reliée à une carte de paiement ou un compte bancaire, et sur le module caméra du *smartphone*.

Les deux modèles de paiement sans contact avec code QR les plus répandus sont : i) présentation du code QR par le client et ii) présentation du code QR par le marchand (cf. encadré 12). Ces modèles sont couverts par les spécifications sur le paiement par code QR publiées par EMVCo dans le but de promouvoir une plus grande interopérabilité entre les solutions reposant sur cette technologie.

Le besoin de s'assurer d'utiliser des codes QR non altérés

Il n'est pas possible d'altérer le contenu d'un code QR sans en modifier le résultat visuel, ainsi deux codes QR portant des actions différentes seront nécessairement différents. Toutefois, de tels codes ne sont pas aisément déchiffrables par

un humain, il est donc primordial de s'assurer de l'authenticité de l'application de paiement qui les utilise, aussi bien du côté du client que du commerçant, seul moyen de garantir que les codes QR générés sont légitimes.

### L'enjeu de la protection des données sensibles

Les données sensibles, telles que les données personnelles (code confidentiel) et les données de la carte de paiement ou du compte bancaire, sont généralement stockées dans l'application de paiement. Afin de prévenir du vol et des accès frauduleux, ces données sensibles sont chiffrées par des algorithmes cryptographiques.

Cette configuration, où l'application de paiement est installée puis exécutée dans le système d'exploitation du *smartphone* et les données sensibles sont stockées chiffrées dans l'environnement du téléphone, présente toutefois un certain nombre de risques en termes de vols de données et donc de fraude. Une solution plus sécurisée consisterait à déployer l'application de paiement et à stocker les données sensibles dans un environnement sécurisé tel qu'un TEE pour se prémunir contre de tels risques.

Encadré 15

## L'évaluation de la sécurité des dispositifs de paiement par mobile

La sécurité de ces solutions de paiement repose à la fois sur l'évaluation sécuritaire des dispositifs mis en œuvre, mais aussi sur la sécurité des processus de gestion du cycle de vie de la solution, notamment le processus d'enrôlement des utilisateurs au sein des applications de paiement.

Tout comme pour les cartes de paiement à puce EMV, pour les solutions fondées sur un composant de sécurité physique, les processus d'évaluation et de certification existants, tels que ceux conduits sous l'égide de l'Autorité nationale de la sécurité des systèmes d'information (ANSSI), permettent de garantir un niveau de sécurité élevé des dispositifs.

En ce qui concerne les solutions logicielles, le périmètre à considérer est plus large que pour un composant de sécurité physique, dans la mesure où il doit prendre en compte le dispositif complet, c'est-à-dire l'application de paiement et les services potentiellement hébergés sur des serveurs distants. Le processus d'évaluation mis en œuvre doit permettre d'apporter l'assurance que ces solutions logicielles atteignent un niveau de sécurité comparable aux solutions fondées sur un composant de sécurité physique.

Les principaux systèmes de paiement par carte (Cartes Bancaires, Visa, MasterCard, American Express) ont ainsi mis en place des protocoles d'évaluation dédiés aux solutions de sécurité logicielles. Ces protocoles sont adaptés aux évolutions plus rapides de ces solutions tout en s'appuyant sur les compétences des laboratoires d'évaluation, tels ceux reconnus par l'ANSSI. À cela s'ajoute le choix de certains fabricants de *smartphones* ou de fournisseurs de solutions de sécurité pour mobiles de faire certifier leurs solutions de sécurisation (ou tout du moins certaines parties critiques) par une autorité telle l'ANSSI.

## Mesures de sécurité recommandées par l'Observatoire

L'Observatoire renouvelle et élargit ses recommandations émises dans son rapport annuel 2011 concernant les portefeuilles électroniques, précédemment limitées à l'usage de cartes de paiement mais également adaptées aux solutions de paiement par mobile, à savoir la mise en œuvre :

- de la protection des données sensibles de paiement par l'ensemble des acteurs impliqués ;

- du recours à un mécanisme d'authentification forte de l'utilisateur par son prestataire de service de paiement au moment de l'enrôlement de la carte dans l'application de paiement ;

- d'analyses de risque par le gestionnaire de la solution de paiement conduisant au déclenchement d'une authentification forte de l'utilisateur pour les opérations considérées comme risquées ;

- d'un cadre contractuel protecteur pour les utilisateurs de ces solutions.

Plus particulièrement, l'Observatoire recommande que des mécanismes fiables soient mis en œuvre pour le stockage sécurisé des informations confidentielles. Ces dernières recouvrent aussi bien les données sensibles de paiement que les données d'authentification, notamment celles concernant les facteurs biométriques, qui sont de plus en plus mis en œuvre dans le cadre des paiements par mobile.

En complément, l'Observatoire rappelle que l'usage de la biométrie comme composante de dispositifs d'authentification forte est soumis aux recommandations émises dans son rapport annuel 2014.

Par ailleurs, l'Observatoire invite les fournisseurs de systèmes d'exploitation pour mobiles, les fabricants de *smartphones* et tout autre acteur impliqué (tels les fournisseurs de solutions de sécurité ou de paiement) à mettre à disposition des utilisateurs les mises à jour correctives de leurs solutions, dès lors qu'une faille de sécurité de nature à altérer l'intégrité, la confidentialité, voire la disponibilité du système ou des données, est identifiée.

De manière générale, l'Observatoire invite les fournisseurs d'applications de paiement par mobile à donner aux utilisateurs plus de visibilité sur les mesures de sécurité intégrées dans leurs applications tout en insistant sur le besoin de déployer des contre-mesures effectives pour lutter contre l'usage non autorisé de ces applications.

L'Observatoire encourage les acteurs à continuer d'innover dans le développement de solutions qui améliorent à la fois l'expérience utilisateur et la sécurité des paiements, dans le prolongement des exigences règlementaires en matière d'authentification des paiements issues de la DSP2, et en lien avec la stratégie nationale des paiements portée par le Comité national des paiements scripturaux. À ce titre, l'Observatoire renouvelle sa recommandation sur la nécessité d'évaluer régulièrement le niveau de sécurité des solutions de paiement, notamment par mobile.

Enfin, l'Observatoire conseille aux utilisateurs d'applications de paiement par mobile :

- de mettre à jour régulièrement le système d'exploitation de leur téléphone mobile ;

- de choisir de manière non triviale (par exemple : suite numérique « 1234 », date d'anniversaire

et suites alphabétiques, telles que« azerty », sont à éviter) et de changer régulièrement les codes confidentiels, mots de passe et toute autre donnée personnelle utilisée pour les procédés d'authentification sur leur *smartphone*, ou tout du moins pour leurs applications de paiement ;

• d'activer, si le système d'exploitation le permet, l'option d'effacement à distance des données en cas de perte ou de vol de leurs mobiles ;

• de n'utiliser que des applications de confiance, notamment celles recommandées par leurs fournisseurs de services de paiement ;

• d'éviter autant que possible de réaliser des transactions de paiement sur leur mobile lorsque le canal de communication n'est pas fiable (par exemple connexion wifi publique non sécurisée).

# 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 email, compte de réseau social, etc.).

## Soyez attentifs

### 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 paraisse douteuse. 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, 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 (DSP2) 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.

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

## 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 DSP2 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 50 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

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

3 L'ordonnance du 9 août 2017 transposant la DSP2 prévoit qu'une large part de ses dispositions s'applique à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna.

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 50 euros).

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

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 extra-européennes

La DSP2 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 50 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'EEE.

# 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 de la sécurité des moyens de paiement*, 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 11 décembre 2018.

**Président**
**François VILLEROY DE GALHAU**
Gouverneur de la Banque de France

## Représentants des assemblées

**Éric BOCQUET**
Sénat

**Rémi REBEYROTTE**
Assemblée nationale

## Représentants du secrétaire général de l'Autorité de contrôle prudentiel et de résolution

**Édouard FERNANDEZ-BOLLO**
Secrétaire général

**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 :
  **Christian DUFOUR**
  **Jean-Philippe PAPILLON**

- Le directeur général du Trésor
  ou sa représentante :
  **Odile RENAUD-BASSO**
  **Arnaud DELAUNAY**

- Le directeur général des Entreprises
  ou son représentant :
  **Thomas COURBE**
  **Romain BONENFANT**

- Le directeur général de la Concurrence,
  de la Consommation et de la Répression
  des fraudes ou son représentant :
  **Aurélien HAUSER**
  **Madly MERI**

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

- Le directeur des Affaires criminelles
  et des Grâces ou sa représentante :
  **Raphaëlle OLIVE**

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 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**
  **David RUIZ**

## Représentants des émetteurs de moyens de paiement et des opérateurs de systèmes de paiement

**Andrée BERTRAND**
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

**Gérard NEBOUY**
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)

**Delphine KOSSER-GLORIES**
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 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 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 ;

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

- **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 DAB/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 (carte de débit, carte de crédit, carte commerciale ou carte prépayée) de carte concernée.

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).

## 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 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.

| 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.

| 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.

| 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. |
| 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). |

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.

# 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*).

## 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.

| 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). |

| 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 de travail simplifié aux entreprises (TTS) ; 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, les chèques emploi-service universels, etc., 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, contrefaçon 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). |
| | 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 2018

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

| | Nombre de transactions | | Montant des transactions | | Montant moyen |
|---|---|---|---|---|---|
| | 2018 | Variation 2018/2017 | 2018 | Variation 2018/2017 | |
| Paiement carte [a] | 13 179 | + 5 | 568 | + 7,0 | 43 |
| Prélèvement | 4 211 | + 3 | 1 644 | + 4,0 | 391 |
| Virement | 4 037 | + 4 | 24 211 | + 0,6 | 5 997 |
| *dont VGM [b]* | *10* | *0* | *10 130* | *+ 7,0* | *1 038 473* |
| Chèque | 1 747 | - 9 | 891 | - 11,0 | 510 |
| Effet de commerce | 81 | 0 | 252 | - 3,0 | 3 150 |
| Monnaie électronique | 65 | + 18 | 1 | + 17,0 | 16 |
| **Total** | **23 320** | **+ 3** | **27 567** | **+ 0,5** | **1 182** |
| Retrait carte [a] | 1 439 | - 3 | 137 | + 1,0 | 94 |
| **Total transactions** | **24 759** | **+ 3** | **27 704** | **+ 0,5** | **1 119** |

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.
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 2018

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

| | Montant | | Volume | | Montant moyen |
|---|---|---|---|---|---|
| | 2018 | Part | 2018 | Part | |
| Paiement carte [a] | 401 604 986 | 38 | 6 068 959 | 90 | 66 |
| Chèque | 450 108 464 | 43 | 166 421 | 3 | 2 704 |
| Virement | 97 307 108 | 9 | 7 731 | 0 | 12 586 |
| Prélèvement | 58 346 253 | 6 | 309 377 | 5 | 188 |
| Effet de commerce | 226 217 | 0 | 5 | 0 | 45 243 |
| **Total paiements** | **1 007 593 028** | **96** | **6 552 493** | **98** | **154** |
| Retrait carte [a] | 37 630 659 | 4 | 158 908 | 2 | 237 |
| **Total transactions** | **1 044 953 687** | **100** | **6 711 401** | **100** | **156** |

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 ;
- neuf émetteurs de cartes privatives : American Express, Oney Bank, BNP Paribas Personal Finance (Aurore, Cetelem et Cofinoga), Crédit agricole Consumer Finance (Finaref et Sofinco), Cofidis, Diners Club, Franfinance, JCB et UnionPay.

En 2018, le nombre de cartes en circulation s'élève à 88,8 millions dont :

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

Le nombre de cartes [1] mises en opposition en 2018 est d'environ 1 358 819.

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 | 10 739,13 | 407,58 | 281,25 | 14,14 | 59,85 | 4,58 |
| Paiements à distance hors internet | 31,86 | 2,39 | 21,04 | 1,53 | 4,35 | 0,41 |
| Paiements à distance sur internet | 1 504,89 | 95,78 | 340,04 | 18,70 | 27,62 | 2,07 |
| Retraits | 1 383,99 | 129,63 | 32,45 | 3,69 | 21,24 | 3,16 |
| **Total** | **13 659,87** | **635,38** | **674,78** | **38,06** | **113,06** | **10,22** |
| Cartes de type « privatif » | | | | | | |
| Paiements de proximité et sur automate | 125,65 | 14,40 | 10,64 | 1,46 | 6,42 | 1,04 |
| Paiements à distance hors internet | 3,03 | 0,31 | 2,48 | 0,03 | 0,25 | 0,02 |
| Paiements à distance sur internet | 11,10 | 1,98 | 8,44 | 1,17 | 1,35 | 0,20 |
| Retraits | 1,73 | 0,16 | 0,00 | 0,00 | 0,00 | 0,00 |
| **Total** | **141,51** | **16,85** | **21,56** | **2,66** | **8,02** | **1,26** |
| **Total général** | **13 801,38** | **652,23** | **696,34** | **40,72** | **121,08** | **11,48** |

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 | 10 739,13 | 407,58 | 308,82 | 17,32 | 92,74 | 8,48 |
| Paiements à distance hors internet | 31,86 | 2,39 | 9,95 | 1,73 | 5,32 | 1,30 |
| Paiements à distance sur internet | 1 504,90 | 95,78 | 101,70 | 10,46 | 32,40 | 3,86 |
| Retraits | 1 384,00 | 129,63 | 24,88 | 4,26 | 7,82 | 1,94 |
| **Total** | **13 659,89** | **635,38** | **445,35** | **33,77** | **138,28** | **15,58** |
| Cartes de type « privatif » | | | | | | |
| Paiements de proximité et sur automate | 125,65 | 14,40 | 9,19 | 1,56 | 10,98 | 4,27 |
| Paiements à distance hors internet | 3,03 | 0,31 | 0,24 | 0,01 | 0,14 | 0,00 |
| Paiements à distance sur internet | 11,10 | 1,98 | 1,83 | 0,29 | 0,97 | 0,24 |
| Retraits | 1,73 | 0,16 | 0,00 | 0,00 | 0,49 | 0,22 |
| **Total** | **141,51** | **16,85** | **11,26** | **1,86** | **12,58** | **4,73** |
| **Total général** | **13 801,40** | **652,23** | **456,61** | **35,63** | **150,86** | **20,31** |

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) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2013 | | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
| Cartes de type « interbancaire » | 0,080 | (455,9) | 0,080 | (486,4) | 0,086 | (526,8) | 0,082 | (531,3) | 0,070 | (482,2) | 0,072 | (526,5) |
| Cartes de type « privatif » | 0,065 | (14,0) | 0,062 | (14,2) | 0,068 | (15,5) | 0,060 | (13,5) | 0,043 | (11,6) | 0,040 | (11,0) |
| **Total** | **0,080** | **(469,9)** | **0,080** | **(500,6)** | **0,085** | **(542,3)** | **0,081** | **(544,8)** | **0,069** | **(493,8)** | **0,071** | **(537,5)** |

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) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2013 | | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
| Transactions nationales (carte française et accepteur français) | 0,046 | (238,6) | 0,043 | (234,6) | 0,044 | (244,4) | 0,042 | (244,5) | 0,037 | (226,5) | 0,038 | (245,6) |
| Transactions internationales | 0,350 | (231,3) | 0,316 | (266,0) | 0,372 | (297,9) | 0,353 | (300,3) | 0,281 | (267,3) | 0,270 | (291,9) |
| *dont carte française et accepteur hors SEPA* | *0,688* | *(70,2)* | *0,636* | *(70,0)* | *0,692* | *(74,5)* | *0,713* | *(68,0)* | *0,511* | *(60,3)* | *0,438* | *(50,3)* |
| *dont carte française et accepteur SEPA* | *0,366* | *(67,9)* | *0,374* | *(91,0)* | *0,459* | *(116,8)* | *0,370* | *(113,9)* | *0,308* | *(100,7)* | *0,352* | *(143,3)* |
| *dont carte étrangère hors SEPA et accepteur français* | *0,404* | *(64,1)* | *0,336* | *(65,6)* | *0,353* | *(69,7)* | *0,449* | *(73,7)* | *0,386* | *(74,1)* | *0,323* | *(65,5)* |
| *dont carte étrangère SEPA et accepteur français* | *0,135* | *(29,1)* | *0,134* | *(39,3)* | *0,153* | *(36,9)* | *0,158* | *(44,7)* | *0,102* | *(32,3)* | *0,092* | *(32,8)* |
| **Total** | **0,080** | **(469,9)** | **0,080** | **(500,6)** | **0,085** | **(542,3)** | **0,081** | **(544,8)** | **0,069** | **(493,8)** | **0,071** | **(537,5)** |

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) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2013 | | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
| Carte française – accepteur français | | | | | | | | | | | | |
| Paiements | 0,050 | (199,9) | 0,046 | (193,2) | 0,047 | (204,5) | 0,045 | (208,6) | 0,039 | (191,9) | 0,041 | (214,7) |
| *dont paiements de proximité et sur automate* | *0,013* | *(45,8)* | *0,010* | *(37,1)* | *0,012* | *(43,4)* | *0,009* | *(33,6)* | *0,009* | *(35,8)* | *0,010* | *(41,4)* |
| *dont paiements à distance* | *0,269* | *(154,2)* | *0,248* | *(156,0)* | *0,244* | *(161,1)* | *0,241* | *(175,0)* | *0,190* | *(156,1)* | *0,173* | *(173,3)* |
| *– dont par courrier / téléphone* | *1,122* | *(29,2)* | *0,147* | *(2,8)* [a] | *0,372* | *(9,1)* | *0,280* | *(9,3)* | *0,357* | *(7,4)* | *0,351* | *(9,5)* |
| *– dont sur internet* | *0,229* | *(125,0)* | *0,251* | *(153,2)* [a] | *0,239* | *(152,0)* | *0,239* | *(165,7)* | *0,186* | *(148,7)* | *0,168* | *(163,8)* |
| Retraits | 0,033 | (38,6) | 0,034 | (41,5) | 0,033 | (39,9) | 0,029 | (35,9) | 0,027 | (34,6) | 0,024 | (30,9) |
| **Total** | **0,046** | **(238,6)** | **0,043** | **(234,6)** | **0,044** | **(244,4)** | **0,042** | **(244,5)** | **0,037** | **(226,5)** | **0,038** | **245,6** |

a) La diminution très importante entre 2013 et 2014, du montant de la fraude sur les paiements à distance effectués par courrier ou par téléphone, et à l'inverse l'augmentation de celle sur les paiements sur internet, s'expliquent pour grande partie par une modification de la méthodologie statistique utilisée par le Groupement des cartes bancaires CB. Un ajustement plus léger a également été effectué en 2015. Voir le rapport annuel 2014 pour plus de détails.
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) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
| Carte française – accepteur étranger hors SEPA | | | | | | | | | | |
| Paiements | 0,532 | (41,7) | 0,735 | (56,3) | 0,862 | (56,2) | 0,608 | (53,3) | 0,534 | (44,4) |
| *dont paiements de proximité et sur automate* | *0,350* | *(19,2)* | *0,509* | *(25,8)* | *0,485* | *(22,9)* | *0,252* | *(12,7)* | *0,230* | *(12,9)* |
| *dont paiements à distance* | *0,960* | *(22,5)* | *1,174* | *(30,5)* | *1,862* | *(33,3)* | *1,096* | *(40,6)* | *1,168* | *(31,5)* |
| *– dont par courrier / téléphone* | *4,955* | *(7,5)* | *2,345* | *(9,5)* | *2,783* | *(9,4)* | *1,499* | *(8,4)* | *1,127* | *(4,8)* |
| *– dont sur internet* | *0,682* | *(14,9)* | *0,959* | *(21,1)* | *1,648* | *(23,9)* | *1,025* | *(32,3)* | *1,175* | *(26,7)* |
| Retraits | 0,890 | (28,3) | 0,586 | (18,1) | 0,390 | (11,8) | 0,229 | (7,0) | 0,184 | (5,9) |
| **Total** | **0,636** | **(70,0)** | **0,692** | **(74,4)** | **0,713** | **(68,0)** | **0,511** | **(60,3)** | **0,438** | **50,3** |
| Carte française – accepteur étranger SEPA | | | | | | | | | | |
| Paiements | 0,434 | (89,8) | 0,526 | (115,7) | 0,422 | (112,9) | 0,342 | (99,8) | 0,385 | (142,4) |
| *dont paiements de proximité et sur automate* | *0,067* | *(7,8)* | *0,071* | *(8,0)* | *0,066* | *(8,3)* | *0,075* | *(10,5)* | *0,066* | *(10,2)* |
| *dont paiements à distance* | *0,910* | *(82,0)* | *1,004* | *(107,7)* | *0,754* | *(104,5)* | *0,591* | *(89,2)* | *0,617* | *(132,2)* |
| *– dont par courrier / téléphone* | *1,317* | *(13,9)* | *1,399* | *(18,7)* | *1,317* | *(19,7)* | *1,489* | *(14,9)* | *0,911* | *(14,2)* |
| *– dont sur internet* | *0,856* | *(68,1)* | *0,948* | *(89,0)* | *0,687* | *(84,9)* | *0,527* | *(74,4)* | *0,594* | *(118,0)* |
| Retraits | 0,033 | (1,2) | 0,033 | (1,1) | 0,024 | (0,9) | 0,025 | (0,9) | 0,025 | (0,9) |
| **Total** | **0,374** | **(91,0)** | **0,459** | **(116,8)** | **0,370** | **(113,8)** | **0,308** | **(100,7)** | **0,352** | **(143,3)** |

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) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
| Carte étrangère hors SEPA – accepteur français | | | | | | | | | | |
| Paiements | 0,380 | (65,0) | 0,391 | (68,1) | 0,507 | (73,2) | 0,429 | (73,3) | 0,357 | (64,8) |
| *dont paiements de proximité et sur automate* | *0,162* | *(21,9)* | *0,168* | *(22,8)* | *0,169* | *(17,4)* | *0,135* | *(16,3)* | *0,108* | *(13,7)* |
| *dont paiements à distance* | *1,213* | *(43,1)* | *1,185* | *(45,3)* | *1,341* | *(55,8)* | *1,143* | *(57,0)* | *0,947* | *(51,1)* |
| *– dont par courrier / téléphone* | *1,018* | *(7,7)* | *1,159* | *(10,8)* | *1,748* | *(18,2)* | *1,488* | *(19,8)* | *0,886* | *(11,5)* |
| *– dont sur internet* | *1,265* | *(35,4)* | *1,193* | *(34,5)* | *1,206* | *(37,7)* | *1,017* | *(37,2)* | *0,967* | *(39,6)* |
| Retraits | 0,026 | (0,6) | 0,069 | (1,6) | 0,024 | (0,5) | 0,038 | (0,8) | 0,031 | (0,7) |
| **Total** | **0,336** | **(65,6)** | **0,353** | **(69,7)** | **0,449** | **(73,7)** | **0,386** | **(74,1)** | **0,323** | **(65,5)** |
| Carte étrangère SEPA – accepteur français | | | | | | | | | | |
| Paiements | 0,156 | (38,5) | 0,175 | (36,0) | 0,178 | (43,8) | 0,114 | (31,5) | 0,102 | (32,0) |
| *dont paiements de proximité et sur automate* | *0,026* | *(5,1)* | *0,033* | *(4,8)* | *0,024* | *(3,7)* | *0,018* | *(3,5)* | *0,018* | *(3,4)* |
| *dont paiements à distance* | *0,476* | *(33,1)* | *0,528* | *(31,3)* | *0,456* | *(40,0)* | *0,337* | *(28,0)* | *0,229* | *(28,6)* |
| *– dont par courrier / téléphone* | *0,397* | *(4,8)* | *0,734* | *(7,7)* | *0,695* | *(11,0)* | *0,564* | *(8,9)* | *0,357* | *(6,2)* |
| *– dont sur internet* | *0,492* | *(28,6)* | *0,484* | *(23,6)* | *0,403* | *(29,0)* | *0,284* | *(19,1)* | *0,208* | *(22,4)* |
| Retraits | 0,018 | (0,9) | 0,025 | (0,9) | 0,024 | (0,9) | 0,019 | (0,7) | 0,019 | (0,8) |
| **Total** | **0,134** | **(39,3)** | **0,153** | **(36,9)** | **0,158** | **(44,7)** | **0,102** | **(32,3)** | **0,092** | **(32,8)** |

Source : Observatoire de la sécurité des moyens de paiement.

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

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

| 2018 | Tous types de carte | | Cartes de type « interbancaire » | | Cartes de type « privatif » | |
|---|---|---|---|---|---|---|
| | Montant | Part | Montant | Part | Montant | Part |
| Carte perdue ou volée | 76,4 | 31,1 | 76,1 | 31,4 | 0,3 | 9,5 |
| Carte non parvenue | 1,5 | 0,6 | 1,4 | 0,6 | 0,1 | 3,4 |
| Carte altérée ou contrefaite | 1,4 | 0,6 | 1,3 | 0,6 | 0,1 | 1,9 |
| Numéro usurpé | 164,0 | 66,7 | 163,0 | 67,2 | 1,0 | 30,2 |
| Autres | 2,4 | 1,0 | 0,6 | 0,2 | 1,8 | 55,0 |
| **Total** | **245,7** | **100,0** | **242,4** | **100,0** | **3,3** | **100,0** |

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 | 971,1 | 39404,0 | 88,9 | 9900,5 | 72,6 | 12522,1 |
| Cartes perdues ou volées | 904,3 | 35770,9 | 53,3 | 4659,6 | 16,2 | 2960,6 |
| Cartes non parvenues | 14,6 | 979,3 | 0,4 | 101,6 | 0,3 | 53,3 |
| Cartes altérées ou contrefaites | 30,0 | 863,0 | 11,8 | 1801,5 | 42,9 | 6945,0 |
| Numéros de cartes usurpés | 17,3 | 1321,7 | 18,4 | 2514,5 | 8,7 | 1826,2 |
| Autres | 4,9 | 469,1 | 5,0 | 823,3 | 4,5 | 737,0 |
| Paiements à distance hors internet | 157,8 | 9190,4 | 194,0 | 13523,9 | 37,3 | 4577,8 |
| Cartes perdues ou volées | 98,2 | 5343,5 | 11,7 | 1036,9 | 3,7 | 367,6 |
| Cartes non parvenues | 0,1 | 4,7 | 0,1 | 6,8 | 0,0 | 3,2 |
| Cartes altérées ou contrefaites | 0,4 | 77,6 | 2,9 | 296,1 | 1,2 | 132,0 |
| Numéros de cartes usurpés | 59,0 | 3760,1 | 178,9 | 12157,1 | 32,2 | 4066,8 |
| Autres | 0,1 | 4,5 | 0,4 | 27,0 | 0,2 | 8,2 |
| Paiements à distance sur internet | 2177,9 | 162975,9 | 2002,0 | 116824,5 | 317,4 | 26288,1 |
| Cartes perdues ou volées | 41,8 | 4670,2 | 95,7 | 6698,5 | 16,5 | 1538,0 |
| Cartes non parvenues | 0,1 | 6,2 | 0,8 | 33,3 | 0,1 | 4,3 |
| Cartes altérées ou contrefaites | 4,3 | 380,9 | 27,1 | 2359,4 | 6,3 | 531,2 |
| Numéros de cartes usurpés | 2131,3 | 157883,0 | 1876,3 | 107599,6 | 293,6 | 24123,5 |
| Autres | 0,4 | 35,6 | 2,1 | 133,7 | 0,9 | 91,1 |
| Retraits | 109,0 | 30786,3 | 4,2 | 904,1 | 44,8 | 5833,1 |
| Cartes perdues ou volées | 107,0 | 30267,8 | 3,0 | 733,2 | 5,2 | 805,4 |
| Cartes non parvenues | 1,2 | 413,6 | 0,1 | 19,4 | 0,3 | 25,6 |
| Cartes altérées ou contrefaites | 0,0 | 6,5 | 0,2 | 23,1 | 36,5 | 4626,0 |
| Numéros de cartes usurpés | 0,1 | 7,3 | 0,3 | 28,8 | 0,8 | 101,3 |
| Autres | 0,7 | 91,1 | 0,6 | 99,6 | 2,0 | 274,8 |
| **Total** | **3415,8** | **242356,6** | **2289,1** | **141153,0** | **472,1** | **49221,1** |

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 | 971,1 | 39404,0 | 27,6 | 3275,3 | 56,6 | 12541,2 |
| Cartes perdues ou volées | 904,3 | 35770,9 | 15,9 | 1977,9 | 31,2 | 6986,2 |
| Cartes non parvenues | 14,6 | 979,3 | 0,5 | 61,2 | 0,5 | 66,4 |
| Cartes altérées ou contrefaites | 30,0 | 863,0 | 4,2 | 281,3 | 16,1 | 3579,2 |
| Numéros de cartes usurpés | 17,3 | 1321,7 | 6,6 | 833,3 | 7,0 | 1609,5 |
| Autres | 4,9 | 469,1 | 0,4 | 121,6 | 1,8 | 299,9 |
| Paiements à distance hors internet | 157,8 | 9190,4 | 19,3 | 5806,7 | 24,6 | 10430,6 |
| Cartes perdues ou volées | 98,2 | 5343,5 | 0,5 | 94,8 | 1,2 | 524,8 |
| Cartes non parvenues | 0,1 | 4,7 | 0,1 | 8,6 | 0,0 | 5,0 |
| Cartes altérées ou contrefaites | 0,4 | 77,6 | 0,9 | 317,1 | 2,1 | 782,7 |
| Numéros de cartes usurpés | 59,0 | 3760,1 | 17,7 | 5351,5 | 21,1 | 9020,1 |
| Autres | 0,1 | 4,5 | 0,1 | 34,7 | 0,2 | 98,0 |
| Paiements à distance sur internet | 2177,9 | 162975,9 | 135,5 | 21860,6 | 216,3 | 38508,3 |
| Cartes perdues ou volées | 41,8 | 4670,2 | 2,2 | 267,0 | 9,0 | 1401,5 |
| Cartes non parvenues | 0,1 | 6,2 | 0,3 | 20,7 | 0,3 | 43,8 |
| Cartes altérées ou contrefaites | 4,3 | 380,9 | 4,3 | 686,0 | 19,7 | 3710,0 |
| Numéros de cartes usurpés | 2131,3 | 157883,0 | 127,7 | 20681,3 | 185,6 | 32879,1 |
| Autres | 0,4 | 35,6 | 1,0 | 205,6 | 1,7 | 474,0 |
| Retraits | 109,0 | 30786,3 | 3,1 | 795,0 | 1,4 | 557,2 |
| Cartes perdues ou volées | 107,0 | 30267,8 | 2,7 | 700,7 | 0,8 | 222,9 |
| Cartes non parvenues | 1,2 | 413,6 | 0,1 | 24,5 | 0,0 | 26,1 |
| Cartes altérées ou contrefaites | 0,0 | 6,5 | 0,1 | 24,8 | 0,4 | 140,1 |
| Numéros de cartes usurpés | 0,1 | 7,3 | 0,2 | 34,6 | 0,0 | 6,7 |
| Autres | 0,7 | 91,1 | 0,0 | 10,4 | 0,2 | 161,4 |
| **Total** | **3415,8** | **242356,6** | **185,5** | **31737,6** | **298,9** | **62037.3** |

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 | 6,5 | 1 979,0 | 1,3 | 361,7 | 2,6 | 379,5 |
| Cartes perdues ou volées | 1,0 | 207,6 | 0,6 | 111,6 | 0,7 | 139,4 |
| Cartes non parvenues | 0,1 | 64,3 | 0,0 | 3,8 | 0,0 | 1,1 |
| Cartes altérées ou contrefaites | 0,1 | 56,6 | 0,2 | 72,0 | 1,3 | 130,2 |
| Numéros de cartes usurpés | 0,4 | 34,4 | 0,3 | 127,4 | 0,6 | 104,5 |
| Autres | 4,9 | 1 616,1 | 0,2 | 46,8 | 0,0 | 4,32 |
| Paiements à distance hors internet | 2,1 | 321,6 | 12,4 | 690,7 | 3,1 | 257,6 |
| Cartes perdues ou volées | 0,1 | 12,3 | 0,7 | 27,0 | 0,2 | 6,6 |
| Cartes non parvenues | 0,0 | 1,4 | 0,0 | 0,2 | 0,0 | 0,1 |
| Cartes altérées ou contrefaites | 0,0 | 2,0 | 0,2 | 11,3 | 0,1 | 6,3 |
| Numéros de cartes usurpés | 1,8 | 286,3 | 11,1 | 641,0 | 2,8 | 243,7 |
| Autres | 0,2 | 19,6 | 0,4 | 11,2 | 0,0 | 0,9 |
| Paiements à distance sur internet | 2,4 | 849,0 | 15,3 | 1 137,9 | 4,4 | 420,1 |
| Cartes perdues ou volées | 0,1 | 29,0 | 0,5 | 27,8 | 0,2 | 8,2 |
| Cartes non parvenues | 0,0 | 3,1 | 0,0 | 0,9 | 0,0 | 0,0 |
| Cartes altérées ou contrefaites | 0,1 | 4,2 | 0,2 | 9,2 | 0,1 | 5,2 |
| Numéros de cartes usurpés | 1,9 | 659,1 | 14,1 | 1 002,7 | 4,0 | 398,2 |
| Autres | 0,3 | 153,6 | 0,5 | 97,3 | 0,1 | 8,5 |
| Retraits | 0,8 | 107,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| Cartes perdues ou volées | 0,4 | 61,4 | 0,0 | 0,0 | 0,0 | 0,0 |
| Cartes non parvenues | 0,4 | 41,1 | 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 | 4,5 | 0,0 | 0,0 | 0,0 | 0,0 |
| Autres | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| **Total** | **11,8** | **3 256,6** | **29,0** | **2 190,3** | **10,1** | **1 057,2** |

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 | 6,5 | 1 979,0 | 0,3 | 93,7 | 2,8 | 1 192,1 |
| Cartes perdues ou volées | 1,0 | 207,6 | 0,1 | 63,7 | 1,0 | 505,6 |
| Cartes non parvenues | 0,1 | 64,3 | 0,0 | 1,3 | 0,0 | 0,4 |
| Cartes altérées ou contrefaites | 0,1 | 56,6 | 0,0 | 5,8 | 1,3 | 560,8 |
| Numéros de cartes usurpés | 0,4 | 34,4 | 0,2 | 20,9 | 0,3 | 100,5 |
| Autres | 4,9 | 1 616,1 | 0,0 | 2,0 | 0,2 | 24,8 |
| Paiements à distance hors internet | 2,1 | 321.2 | 0,9 | 438,4 | 2,3 | 1 086,7 |
| Cartes perdues ou volées | 0,1 | 12,3 | 0,0 | 5,5 | 0,1 | 32,3 |
| Cartes non parvenues | 0,0 | 1,4 | 0,0 | 0,0 | 0,0 | 0,3 |
| Cartes altérées ou contrefaites | 0,0 | 2,0 | 0,0 | 3,9 | 0,4 | 159,7 |
| Numéros de cartes usurpés | 1,8 | 286,3 | 0,9 | 426,0 | 1,8 | 860,5 |
| Autres | 0,2 | 19,6 | 0,0 | 3,0 | 0,0 | 33,9 |
| Paiements à distance sur internet | 2,4 | 849,0 | 1,2 | 500,4 | 3,8 | 1 124,9 |
| Cartes perdues ou volées | 0,1 | 29,0 | 0,0 | 0,8 | 0,1 | 16,9 |
| Cartes non parvenues | 0,0 | 3,1 | 0,0 | 1,2 | 0,0 | 1,7 |
| Cartes altérées ou contrefaites | 0,1 | 4,2 | 0,0 | 10,5 | 0,8 | 167,8 |
| Numéros de cartes usurpés | 1,9 | 659,1 | 1,2 | 480,6 | 2,9 | 926,1 |
| Autres | 0,3 | 153,6 | 0,0 | 7,3 | 0,0 | 12,4 |
| Retraits | 0,8 | 107,0 | 0,0 | 0,0 | 0,3 | 107,3 |
| Cartes perdues ou volées | 0,4 | 61,4 | 0,0 | 0,0 | 0,0 | 0,0 |
| Cartes non parvenues | 0,4 | 41,1 | 0,0 | 0,0 | 0,0 | 0,0 |
| Cartes altérées ou contrefaites | 0,0 | 0,0 | 0,0 | 0,0 | 0,3 | 103,1 |
| Numéros de cartes usurpés | 0,0 | 4,5 | 0,0 | 0,0 | 0,0 | 0,0 |
| Autres | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 4,2 |
| **Total** | **11,8** | **3 256,2** | **2,4** | **1 032,5** | **9,2** | **3 511,0** |

Source : Observatoire de la sécurité des moyens de paiement.

## Statistiques de fraude sur le virement

### T15 Répartition de la fraude au virement par zone géographique

(montant en euros, part en pourcentage)

| | 2018 | |
|---|---|---|
| | Montant | Part |
| France | 31 359 143 | 32 |
| SEPA hors France | 56 882 385 | 58 |
| Hors SEPA | 9 065 580 | 10 |
| **Total** | **97 307 108** | **100** |

Source : Observatoire de la sécurité des moyens de paiement.

## Statistiques de fraude sur les prélèvements

### T16 Répartition de la fraude au prélèvement par zone géographique

(montant en euros, part en pourcentage)

| | 2017 | |
|---|---|---|
| | Montant | Part |
| France | 44 399 031 | 76 |
| SEPA hors France | 13 946 376 | 24 |
| **Total** | **58 346 253** | **100** |

Source : Observatoire de la sécurité des moyens de paiement.

## Statistiques de fraude sur le chèque

### T17 Répartition par typologie de fraude en 2018

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

| | Montant | Part | Volume | Montant moyen |
|---|---|---|---|---|
| Détournement, rejeu | 14 741 262 | 3 | 2 793 | 5 277 |
| Vol, perte (faux, apocryphe) | 252 890 727 | 56 | 138 358 | 1 827 |
| Contrefaçon | 36 739 051 | 8 | 8 092 | 4 540 |
| Falsification | 145 737 424 | 33 | 17 178 | 8 483 |
| **Total** | **450 108 464** | **100** | **166 421** | **2 704** |

Source : Observatoire de la sécurité des moyens de paiement.

## Rectificatif des données de fraude à la carte, 2015-2017

Du fait d'une interprétation erronée de la méthodologie de l'Observatoire par un établissement déclarant, certaines données publiées précédemment dans les rapports annuels de l'Observatoire ont été corrigées. Ces corrections portent sur les données de la fraude nationale (carte française, accepteur français) dont les montants sont révisés à la hausse de + 19,4 millions d'euros pour 2015, de + 27,4 millions d'euros pour 2016 et de + 26,8 millions d'euros pour 2017. Les tableaux et graphiques qui suivent font état des différentes corrections apportées sur les données publiées pour les années 2015 à 2017 suite à la révision des montants de la fraude nationale.

### T18 Montants de la fraude corrigés de 2015 à 2017

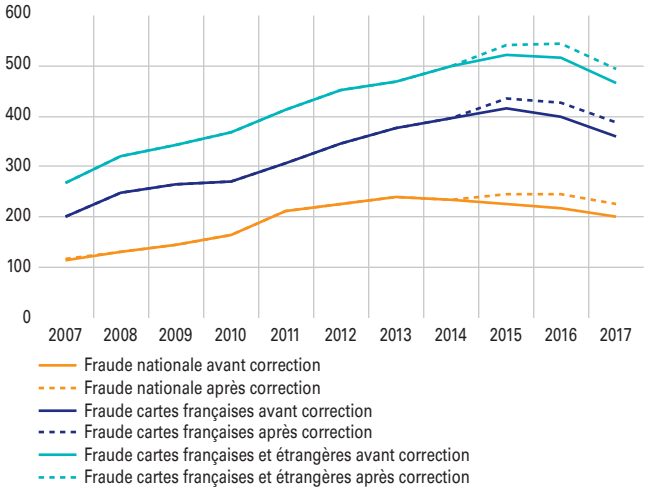
(en millions d'euros)

| | 2015 | 2016 | 2017 |
|---|---|---|---|
| **Carte française – accepteur français** | **244,4** | **244,5** | **226,5** |
| *dont paiements de proximité et sur automate* | *43,4* | *33,6* | *35,8* |
| *dont paiements à distance hors internet* | *9,1* | *9,3* | *7,4* |
| *dont paiements à distance sur internet* | *152,0* | *165,7* | *148,7* |
| *dont retraits* | *39,9* | *35,9* | *34,6* |
| **Carte française – accepteurs français, étranger SEPA, étranger hors SEPA** | **435,7** | **426,4** | **387,4** |
| **Cartes française et étrangère – accepteurs français, étranger SEPA, étranger hors SEPA** | **542,3** | **544,8** | **493,8** |

Source : Observatoire de la sécurité des moyens de paiement.

### G1 Évolution des montants de la fraude, avec correction de 2015 à 2017

(en millions d'euros)




Source : Observatoire de la sécurité des moyens de paiement.

## T19 Taux de fraude corrigés de 2015 à 2017

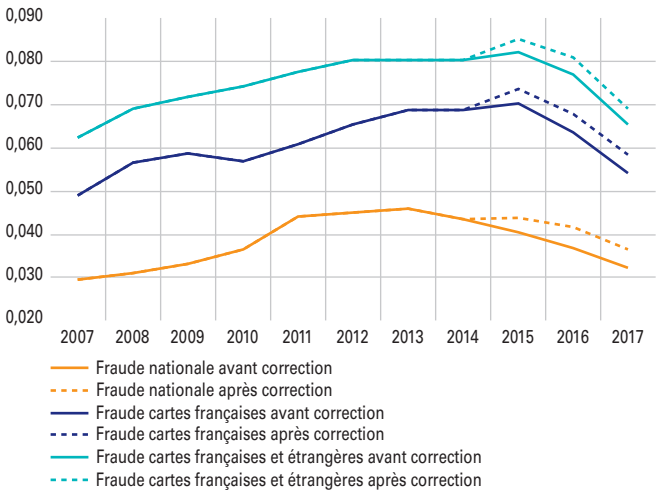
(en %)

| | 2015 | 2016 | 2017 |
|---|---|---|---|
| **Taux de fraude nationale – carte française, accepteur français** | **0,044** | **0,042** | **0,037** |
| *dont paiements de proximité et sur automate* | *0,012* | *0,009* | *0,009* |
| *dont paiements à distance* | *0,244* | *0,241* | *0,190* |
| *dont retraits* | *0,033* | *0,029* | *0,027* |
| **Taux de fraude carte française, accepteurs français, étranger SEPA, étranger hors SEPA** | **0,074** | **0,068** | **0,058** |
| **Taux de fraude cartes française et étrangère, accepteurs français, étranger SEPA, étranger hors SEPA** | **0,085** | **0,081** | **0,069** |

Source : Observatoire de la sécurité des moyens de paiement.

## G2 Évolution du taux de fraude, avec correction de 2015 à 2017

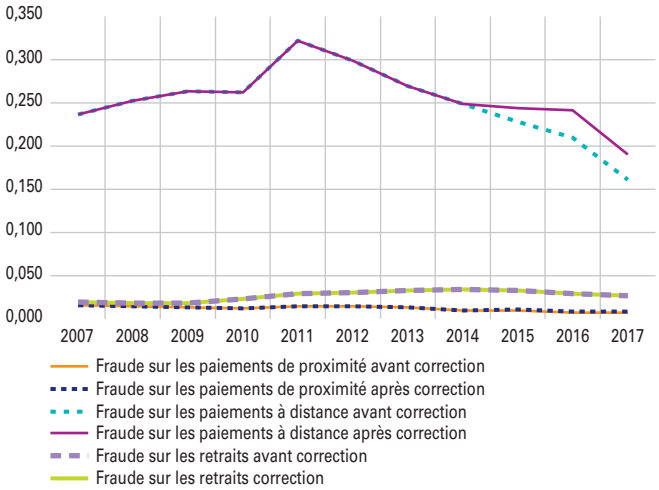
(en %)




Source : Observatoire de la sécurité des moyens de paiement.

## G3 Évolution du taux de fraude nationale par type de transaction, avec correction de 2015 à 2017

(en %)




Source : Observatoire de la sécurité des moyens de paiement.

**Éditeur**
Banque de France
39 rue Croix-des-Petits-Champs
75001 Paris

**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 Systèmes de paiement
et Infrastructures de marché
Banque de France

**Secrétariat de rédaction**
Véronique Bugaj, Olivier Catau, Guylène Chotard,
Caroline Corcy, Bernard Darrius, Florian Dintilhac,
Christelle Guiheneuc, Trân Huynh, Lucas Nozahic,
Alexandre Stervinou, Mathieu Vileyn

**Réalisation**
Studio Création
Direction de la Communication
de la Banque de France

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

**Impression**
Banque de France – SG - DISG

**Dépôt légal**
Juillet 2019
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).*