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

2016

BANQUE DE FRANCE
EUROSYSTÈME

bservatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

Rapport annuel 2016
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 L141-4 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.

Le mot du président

La stratégie nationale des paiements lancée en octobre 2015 par le ministre de l'Économie a pour objectif de promouvoir l'utilisation de moyens de paiement innovants, sûrs et efficaces sur le territoire. L'innovation est particulièrement bienvenue car elle améliore l'efficacité des processus de paiement ; mais l'innovation technologique n'est profitable pour l'écosystème des paiements et l'économie dans son ensemble que si elle s'exerce dans un environnement sécurisé, quels que soient les technologies utilisées et les acteurs impliqués. C'est une condition sine qua non *pour permettre d'assurer la confiance des utilisateurs dans leurs moyens de paiement.*

Le législateur vient d'élargir le mandat de l'Observatoire de la sécurité des cartes de paiement (OSCP) à l'ensemble des moyens de paiement scripturaux, il a ainsi pris acte du succès de la contribution de l'OSCP au renforcement de la sécurité des paiements par cartes, mais également du caractère particulièrement protéiforme de l'innovation dans le domaine des paiements, qui ne touche plus la seule carte : ce sont de nouveaux canaux d'initiation de paiement, de nouveaux supports de paiements, et de nouveaux prestataires de paiements.

L'OSMP reprend ainsi les missions de l'OSCP – suivi des mesures de sécurisation entreprises par les émetteurs, les commerçants et les entreprises, établissement de statistiques de la fraude et veille technologique en matière de moyens de paiement – sur un périmètre désormais élargi à l'ensemble des moyens de paiement scripturaux. Cet élargissement lui permettra notamment de réaliser les analyses de sécurité indispensables aux travaux conduits par le Comité national des paiements scripturaux (CNPS), en charge de veiller à la mise en œuvre de la stratégie nationale des paiements, et qui porteront notamment sur la mise en place de solutions de virement instantané ou la promotion du recours aux moyens de paiement électroniques comme alternatives au chèque.

Dans un contexte réglementaire en pleine évolution, avec l'entrée en vigueur en janvier 2018 de la deuxième directive européenne sur les services de paiement, l'Observatoire sera également une instance essentielle dans la mise en œuvre des dispositions de sécurité, d'ordre légal. Cela sera d'autant plus naturel que certaines de ces dispositions ont constitué de longue date le socle des recommandations de l'OSCP, notamment la généralisation du recours à des dispositifs d'authentification forte du payeur pour l'utilisation de moyens de paiement électronique. Les actions prioritaires porteront également sur la sécurisation de

l'accès aux comptes de paiement par les acteurs tiers que sont les initiateurs de paiement et les agrégateurs d'information sur les comptes. L'OSMP conduira ces travaux en les nourrissant d'un dialogue permanent entre les différentes parties prenantes : fournisseurs et utilisateurs de services de paiement (entreprises et consommateurs), autorités publiques.

Ce premier rapport annuel apporte un éclairage statistique sur la fraude aux paiements scripturaux en 2016. La carte représente la moitié du montant global de fraude compte tenu de son fort usage, mais il est important de noter que cette fraude s'inscrit depuis plusieurs années en retrait sur les transactions nationales, et pour la première fois sur l'ensemble des transactions, y compris internationales.

Par ailleurs, les chiffres de fraude de l'année 2016 confortent le choix des axes de la stratégie nationale, concernant la promotion du virement et de la carte pour les paiements aux points de vente comme alternatives sécurisées au paiement par chèque en France. En effet, le taux de fraude des paiements par carte en proximité s'établit à 0,008 % (soit 1 euro de fraude pour 12 500 euros de montant de transaction), avec notamment des paiements par carte sans contact en plein essor et à la fraude maîtrisée (0,020 %), celui du virement est encore inférieur (1 pour 275 000 euros), alors que le chèque présente un taux de fraude de 0,025 % (1 pour 4 000 euros).

Dans ce contexte, la contribution de l'Observatoire de la sécurité des moyens de paiement sera, à n'en pas douter, déterminante pour continuer à garantir la confiance des utilisateurs dans leurs moyens de paiement actuels et futurs. J'en remercie tous les membres de l'Observatoire et les services de la Banque de France, engagés dans cette maîtrise de la fraude.

François Villeroy de Galhau
Président de l'Observatoire

Synthèse

Ce premier rapport annuel de l'Observatoire de la sécurité des moyens de paiement permet au grand public de disposer, pour la première fois, de données et d'informations relatives à la fraude sur les différents moyens de paiement scripturaux, jusqu'à présent disponibles pour les seules cartes de paiement. Il en ressort les principaux constats suivants.

• *La fraude aux moyens de paiement scripturaux émis en France représente un montant global d'environ 800 millions d'euros. Si cette somme peut sembler relativement modeste au regard des flux de paiement échangés annuellement en France, de l'ordre de 27 000 milliards d'euros, elle représente une charge substantielle supportée par les utilisateurs et les fournisseurs de services de paiement.*

• *La carte de paiement, qui reste le moyen de paiement privilégié des Français (utilisé dans près de la moitié des transactions scripturales), supporte plus de la moitié de la fraude aux moyens de paiement scripturaux émis en France, soit un montant de l'ordre de 400 millions d'euros en 2016 pour les cartes françaises (pour un taux de fraude de 0,064 %). Cette fraude présente deux caractéristiques principales : d'une part, elle est concentrée sur les paiements à distance, essentiellement sur internet, qui supportent les deux tiers du montant de la fraude alors qu'ils ne représentent que 12 % des transactions ; d'autre part, elle affecte plus fortement les transactions transfrontalières que les transactions nationales, les premières supportant plus de 60 % du montant de la fraude alors que leur poids n'est que de 15 % des transactions réalisées.*

Au niveau national et pour la première fois depuis le début des années 2000, le montant de fraude sur les transactions diminue, d'environ 4 %, alors que l'usage de ce moyen de paiement continue à croître de 6 %, porté notamment par le développement du paiement sans contact. Le taux de fraude sur les cartes est en repli pour la seconde année consécutive sur l'ensemble des usages : paiement de proximité (à 0,008 %, dont 0,020 % pour les paiements sans contact), paiement à distance (0,199 %) et retraits aux distributeurs automatiques (0,029 %). Cette meilleure maîtrise de la fraude est notamment le fruit des efforts consentis par l'ensemble des acteurs pour développer le recours à des solutions d'authentification forte du payeur pour les paiements sur internet, mais également à la mise en œuvre de solutions de scoring *des transactions par les émetteurs et les systèmes de paiement carte.*

Au niveau international, il est à noter que la fraude sur les transactions au sein de l'espace européen SEPA est globalement mieux maîtrisée, du fait du renforcement progressif des règlementations européennes concernant la sécurité des paiements. Le recours croissant aux solutions d'authentification forte pour les paiements à distance, ainsi que la mise en œuvre progressive de la carte à puce aussi bien en Europe qu'au-delà, permettent de stabiliser la fraude dans un contexte de développement de ces transactions transfrontalières.

• Le chèque est le second moyen de paiement le plus touché par la fraude, à hauteur de près de 272 millions d'euros en 2016 (soit un taux de fraude de 0,025 %). Deux catégories de fraude se distinguent à parts quasiment équivalentes : d'une part, l'utilisation frauduleuse de chèques perdus ou volés, qui représente 44 % de la fraude totale ; d'autre part, la fraude par falsification d'un chèque, c'est-à-dire la modification frauduleuse du montant ou du bénéficiaire d'un chèque valide, qui représente 42 % de la fraude.

Du fait des caractéristiques du chèque, la prévention de ces fraudes repose en premier lieu sur la vigilance de ses utilisateurs, qu'il s'agisse des utilisateurs tirés ou des bénéficiaires, afin de prévenir les risques de vol et de perte, et de falsification.

• Les virements supportent un montant de fraude plus faible, de l'ordre de 86 millions d'euros en 2016, et sont proportionnellement beaucoup moins touchés que la carte ou le chèque avec des taux de fraude plus de soixante fois inférieurs à ces derniers.

*La fraude au virement présente certaines similitudes avec la fraude carte, dans la mesure où les transactions sur internet (*via *l'espace de banque en ligne du titulaire du compte) et les transactions transfrontalières sont davantage affectées par la fraude. Les modalités de fraude diffèrent selon le statut du titulaire de compte : les particuliers sont généralement visés par des logiciels malveillants ou des campagnes d'envoi de faux mails visant pour les fraudeurs à collecter les identifiants de banque en ligne en vue d'usurper l'identité du titulaire du compte et initier ainsi des virements frauduleux ; si elles subissent aussi ce type d'attaques, les entreprises sont également visées par des attaques d'ingénierie sociale, dans lesquelles le fraudeur usurpe l'identité d'un interlocuteur habituel de l'entreprise (un fournisseur, un dirigeant de l'entreprise…) pour amener cette dernière à émettre dûment un ordre de paiement illégitime.*

La prévention de la fraude au virement s'appuie, au niveau des établissements teneurs de compte, sur la mise en place de dispositifs d'analyse des transactions qui permettent d'identifier celles à caractère inhabituel et d'alerter le titulaire de compte pour validation, ainsi que sur le recours à des dispositifs d'authentification forte pour la validation des ordres de paiement. La vigilance des entreprises et des particuliers reste toutefois nécessaire, d'une part pour identifier les demandes frauduleuses qui leur sont adressées et d'autre part pour protéger leurs outils et environnements informatiques (mise en place d'anti-virus et pare-feu, suppression des pièces jointes douteuses, etc.).

- *Enfin, la fraude sur les prélèvements et les effets de commerce représente des montants plus faibles, de l'ordre respectivement de 40 millions d'euros et 1 million d'euros en 2016. Cette fraude est presqu'exclusivement nationale, en dépit du caractère européen du prélèvement SEPA. Les mesures de prévention sur ces moyens de paiement portent en premier lieu sur la connaissance par la banque du profil d'utilisation des moyens de paiement de ses clients, qu'ils soient créanciers ou payeurs, et de mécanismes d'alerte en cas de transaction atypique ou inattendue, telle qu'une nouvelle référence de mandat de prélèvement.*

L'ensemble de ces données s'appuie sur une méthodologie statistique harmonisée entre les différents moyens de paiement, présentée en détail dans le premier chapitre du présent rapport et cohérente avec le cadre méthodologique précédemment mis en place par l'Observatoire de la sécurité des cartes de paiement. La continuité qui en résulte permet d'exploiter pleinement l'historique statistique de la fraude aux cartes de paiement depuis le début des années 2000.

Enfin, dans le prolongement des actions conduites par l'Observatoire de la sécurité des cartes de paiement en matière de veille technologique, le présent rapport annuel présente également une étude sur la sécurité des terminaux de paiement mobiles dits « m-POS », reposant sur l'utilisation d'un smartphone ou d'une tablette pour l'encaissement de paiements par carte. L'Observatoire note en particulier la nécessité de soumettre ces nouveaux types de terminaux aux exigences applicables aux terminaux de paiement électroniques en matière de protection de la saisie du code confidentiel, tout en assurant une protection par chiffrement des données afin de parer à toute vulnérabilité liée à la présence d'un terminal non certifié (le smartphone ou la tablette) dans la réalisation de la transaction.

1 Méthodologie de mesure de la fraude aux moyens de paiement scripturaux

1.1 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,…) ;
– 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,…) ;
– 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…). 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 cinq typologies de fraude, étant précisé que celles-ci ne s'appliquent pas de la même manière aux différents instruments de paiement :

• perte/vol : fraude par l'utilisation d'un instrument de paiement physique (carte, chéquier…) obtenu par vol ou perte ;

• contrefaçon : fraude par l'utilisation d'un instrument de paiement contrefait ou par l'utilisation de données de paiement détournées ;

• 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.

1 *https://observatoire.banque-france.fr/fileadmin/user_upload/Observatoire/pdf/rapport_et_communique_de_presse/2015/OSCP-rapport-annuel-2015-Chapitre-1.pdf*

1.2 Mesure de la fraude à la carte de paiement

Transactions couvertes

La fraude sur 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 établissement acquéreur de la transaction domicilié 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.

Origine des données de fraude

Les données de fraude sur 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 sur 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.

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

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

Typologie de fraude sur 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.

Canaux 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'acquéreur sont, tous deux, établis en France. Pour les paiements à distance, le fraudeur peut toutefois opérer depuis l'étranger.
Transaction internationale FR ➔ SEPA	L'émetteur est établi en France et l'acquéreur est établi à l'étranger dans l'espace SEPA.
Transaction internationale FR ➔ hors SEPA	L'émetteur est établi en France et l'acquéreur est établi à l'étranger hors espace SEPA.
Transaction internationale SEPA ➔ FR	L'émetteur est établi à l'étranger dans l'espace SEPA et l'acquéreur est établi en France.
Transaction internationale hors SEPA ➔ FR	L'émetteur est établi à l'étranger hors espace SEPA et l'acquéreur est établi en France.
Secteur d'activité du commerçant pour les paiements à distance	**Description du secteur d'activité**
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.
Equipement de la maison	Vente de produits d'ameublement et de bricolage.
Jeu en ligne	Sites de jeu 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	

1.3 Mesure de la fraude au virement

Instruments de paiement couverts

La fraude sur le 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 Transfer*) 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 sur le 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. Afin d'éviter tout risque de double déclaration de la fraude, celle-ci est effectuée uniquement par l'établissement qui a exécuté le virement.

Éléments d'analyse de la fraude

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

4 Établissements habilités à tenir des comptes de paiement pour le compte de leur clientèle et à 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 L518-1 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.

Typologies de fraude sur le 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*…) 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…), 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 la zone SEPA.
Virements hors zone SEPA	Virement émis depuis un compte tenu en France vers un compte tenu dans un pays étranger hors zone SEPA.
Canaux d'initiation utilisés	**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 (canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque).

1.4 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*) ainsi que, jusqu'au 1er février 2016, des paiements par TIP (Titre interbancaire de paiement) et télérèglement, moyens de paiement nationaux non SEPA assimilés à des prélèvements qui avaient cours jusqu'à cette date.

Origine des données de fraude

Les données de fraude sur le 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. La déclaration de fraude au prélèvement est effectuée, selon la typologie de fraude, par le prestataire de services de paiement du créancier (faux, détournement)

Typologies de fraude sur le prélèvement	Forme de la fraude
Faux	Fraude côté créancier : le fraudeur émet des prélèvements vers des numéros de compte qu'il a obtenus illégalement et sans aucune autorisation ou réalité économique sous-jacente. Fraude côté débité : le fraudeur usurpe l'identité et l'IBAN d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien.
Détournement	Le fraudeur modifie le numéro de compte à créditer associé à des fichiers de prélèvement émis régulièrement, ou usurpe un identifiant créancier SEPA qui n'est pas le sien pour émettre à son bénéfice des prélèvements visant des comptes pour lesquels ce créancier dispose de mandats légitimes.
Rejeu	Le créancier émet sciemment des prélèvements déjà émis (qui ont soit déjà été réglés, soit ont fait l'objet de rejets pour opposition du débiteur par exemple).
Zones géographiques d'émission et de destination du prélèvement	**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 la zone SEPA.
Prélèvement hors zone SEPA	Prélèvement émis par un créancier dont le compte est domicilié en France vers un compte tenu dans un pays étranger, hors zone SEPA.
Canaux d'autorisation utilisés	**Modalités d'utilisation**
Papier	Mandat de prélèvement collecté par courrier, formulaire, courriel, télécopie et 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.

ou par celui du débiteur (rejeu), afin d'éviter tout risque de double comptage ou de sous-évaluation des données de fraude.

Éléments d'analyse de la fraude

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

1.5 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 sur le 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 L131-1 à 88 du *Code monétaire et financier*. Plus précisément, il s'agit des chèques tirés par la clientèle de l'établissement bancaire sur des

Typologie de fraude au chèque	Forme de la fraude	Établissement déclarant
Vol/perte (faux 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).	Établissement remettant
Contrefaçon	Faux chèque créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque.	
Falsification	Chèque régulier intercepté par un fraudeur qui l'altère volontairement par grattage, gommage ou effacement.	
Détournement/rejeu	Chèque perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l'encaissement. Chèque régulièrement émis, perdu ou volé, intercepté dans le circuit d'acheminement vers le bénéficiaire et encaissé sur un compte différent de celui du bénéficiaire légitime. La formule est correcte, le nom du bénéficiaire est inchangé et la ligne magnétique située en bas du chèque est valide, tout comme la signature du client. Émission volontaire d'un chèque par le titulaire après sa mise en opposition.	Établissement tiré

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

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 L525-4 du *Code monétaire et financier*, tels que les chèques-vacances, les chèques ou titres restaurant, les chèques culture, les chèques emploi-service universels… qui recouvrent des catégories variées de titres dont l'usage est restreint, soit à l'acquisition d'un nombre limité de biens ou de services, soit à un réseau limité d'accepteurs.

Origine des données de fraude

Les données de fraude sur le 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 (on parlera alors d'établissement remettant), soit en qualité d'établissement qui tient le compte du payeur (on parlera alors d'établissement tiré).

- Pour les catégories de « vol, perte (faux, apocryphe) », « contrefaçon », et « falsification », la déclaration est effectuée par l'établissement remettant.

- Pour la catégorie « détournement, rejeu », qui correspond à la présentation au paiement une seconde fois d'un chèque déjà payé, la déclaration est effectuée par l'établissement tiré dans la mesure où c'est son service fraude qui détecte généralement ce cas de figure.

Cette répartition vise à prévenir tout risque de double comptage ou de sous-évaluation dans les données de fraude collectées.

Éléments d'analyse des données de fraude

Les données de fraude sur le chèque sont analysées à partir des grandes typologies de fraude définies par l'Observatoire.

Pour le chèque, le tableau précédent récapitule les formes de la fraude les plus couramment observées, la typologie à laquelle elles se rattachent ainsi que l'établissement soumis à la déclaration de la fraude.

1.6 Mesure de la fraude aux effets de commerce

Instruments de paiement couverts

La fraude sur les 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 typologies de fraude sur les effets de commerce sont les mêmes que celles définies 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).

- Pour les catégories de « vol, perte (faux, apocryphe) », « contrefaçon », et « falsification », la déclaration est effectuée par l'établissement remettant.

- Pour la catégorie « détournement, rejeu », qui correspond à la présentation au paiement une seconde fois d'un effet déjà payé, la déclaration est effectuée par l'établissement tiré dans la mesure où c'est son service fraude qui détecte généralement ce cas de figure.

Cette répartition vise à prévenir tout risque de double comptage ou de sous-évaluation dans les données de fraude collectées.

1.7 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 pré-alimentée 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.

2 État de la fraude en 2016

2.1 Vue d'ensemble

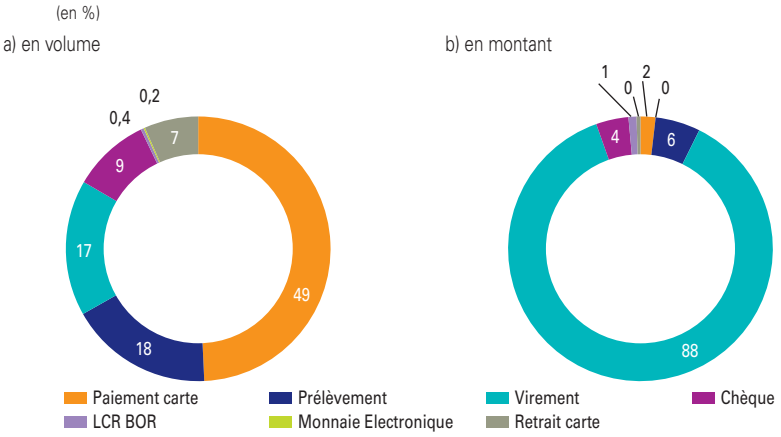
Cartographie des moyens de paiement

En 2016, 22,6 milliards de transactions scripturales ont été réalisées par les clients (particuliers et entreprises) des banques et prestataires de services de paiement français pour un montant total de 27 161 milliards d'euros, ce qui représente une progression de 5 % du nombre de transactions et de 3 % des montants échangés par rapport à 2015.

Le paiement par carte s'affiche comme le mode de paiement privilégié des français, avec une utilisation dans près de la moitié des transactions scripturales en volume (49 %) pour un montant total de 499 milliards d'euros en 2016. Par ailleurs, les retraits par carte ont représenté 1 491 millions d'opérations pour un montant total de 129 milliards d'euros.

G1 Usage des moyens de paiement scripturaux en France en 2016

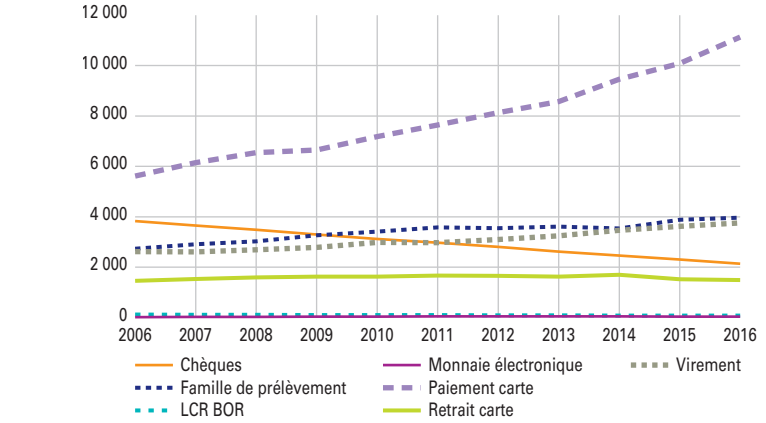
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

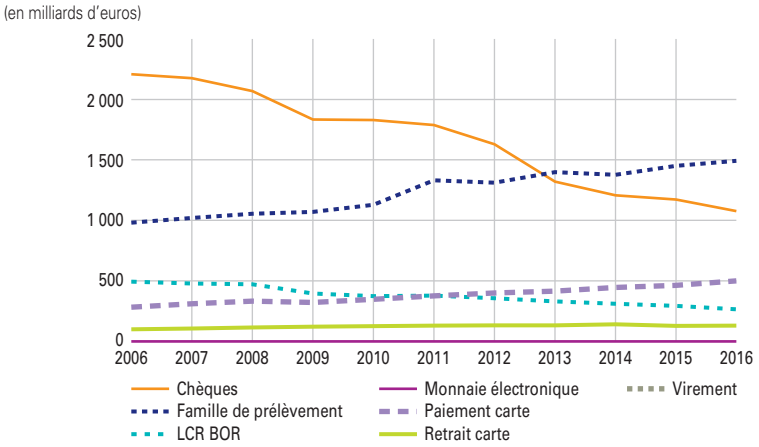
G2 Usage des moyens de paiement en France depuis 2006

(en millions d'opérations)



Source : Observatoire de la sécurité des moyens de paiement.

G3 Montant des transactions hors virements en France



Source : Observatoire de la sécurité des moyens de paiement.

Le virement demeure l'instrument de prédilection pour les paiements de montant élevé (paiements des salaires et pensions, paiements interentreprises…) et représente ainsi 88 % du montant total des transactions scripturales. En nombre d'opérations, il se situe en troisième position (17 %), juste après le prélèvement et loin derrière la carte. Les virements sont principalement émis au niveau national (77 % des virements globaux), contre 18 % à destination de l'espace SEPA et 4 % en dehors.

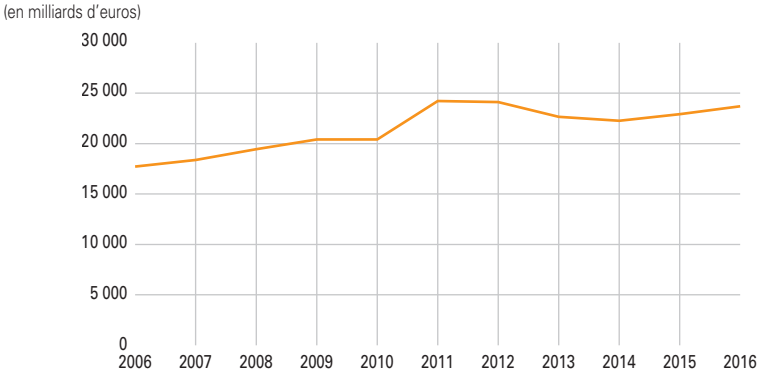
Le prélèvement arrive au deuxième rang des instruments de paiement scripturaux les plus utilisés en nombre (18 %) et en montant (6 %). Ces transactions sont presqu'exclusivement nationales, les prélèvements SEPA transfrontaliers représentant moins de 1 % de l'ensemble des flux émis.

Le chèque connaît depuis plusieurs années un déclin régulier qui se confirme en 2016 tant en nombre d'opérations (– 8 %) qu'en valeur (– 8 %). 2,1 milliards de chèques ont ainsi été émis en 2016 pour un montant global de 1 077 milliards d'euros, soit une part dans les paiements scripturaux de 9,5 % en volume et 4 % en valeur.

Les lettres de change relevé et les billets à ordre, qui représentent moins de 1 % des transactions scripturales tant en volume qu'en valeur, connaissent un repli continu qui se confirme en 2016, tant en montant (– 9 %) qu'en nombre d'opérations (– 3 %).

Enfin, l'utilisation de **la monnaie électronique** reste marginale en France avec 38 millions de transactions pour une valeur totale de 591 millions d'euros.

G4 Montant des virements en France



Source : Observatoire de la sécurité des moyens de paiement.

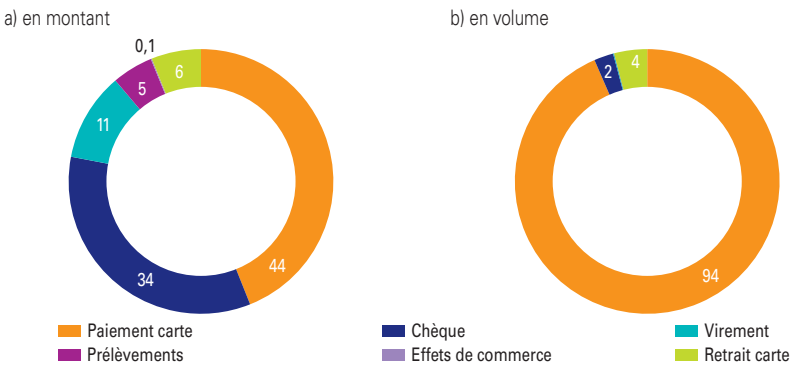
Fraude aux moyens de paiement

En 2016, la fraude aux transactions scripturales représente un montant global d'environ 800 millions d'euros pour 4,8 millions de transactions frauduleuses.

La carte de paiement [1] concentre la moitié de la fraude en montant, soit près de 400 millions d'euros en cumulant les transactions de paiement et de retrait, et représente la quasi-totalité (97 %) du nombre de transactions frauduleuses. Néanmoins, le montant de fraude global sur les cartes émises en France diminue en 2016 pour la première fois après plusieurs années de progression ; cela permet au taux de fraude de diminuer, après plusieurs années de stagnation, pour s'établir à 0,064 % soit environ un euro de fraude pour 1 600 euros de transactions. Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,008 % soit un euro de fraude pour 12 500 euros de transactions) mais plus significative sur les paiements à distance (0,199 %, soit un euro de fraude pour 500 euros de paiements).

G5 Répartition de la fraude sur les moyens de paiement scripturaux en 2016

(en %)



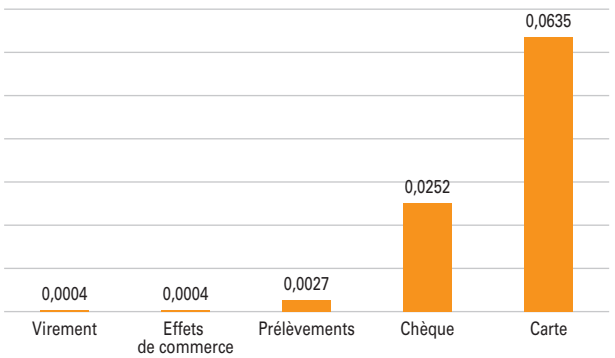
Source : Observatoire de la sécurité des moyens de paiement.

Le chèque est le second moyen de paiement le plus fraudé en France en 2016, avec un montant de fraude qui s'élève à près de 272 millions d'euros, et ce alors qu'il n'est que le quatrième moyen de paiement en termes d'usage. Son taux de fraude s'établit à 0,025 %, soit un niveau légèrement inférieur à celui des transactions par carte et l'équivalent d'un euro de fraude pour 4 000 euros de paiement.

Le montant annuel de fraude au **virement** est significativement inférieur à celui de la carte et du chèque,

G6 Taux de fraude- par moyen de paiement

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

1 Cartes émises en France, utilisées en France et à l'étranger.

et s'établit à 86 millions d'euros en 2016. Compte tenu des montants élevés échangés par ce moyen de paiement, son taux de fraude est le plus faible parmi les moyens de paiement scripturaux, à 0,0004 % soit l'équivalent d'un euro de fraude pour 275 000 euros de paiement.

Le **prélèvement** enregistre un montant plus limité de fraude, soit environ 40 millions d'euros en 2016, pour un taux de fraude dont l'ordre de grandeur est à un niveau intermédiaire, à 0,003 %, soit l'équivalent d'un euro de fraude pour 37 000 euros de prélèvements émis.

Les effets de commerce sont relativement épargnés par la fraude, avec un montant de l'ordre d'un million d'euros en 2016, pour un taux de fraude équivalent à celui des virements, soit 0,0004 %.

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 2016 portent ainsi sur :

- 612,1 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 73,4 millions de cartes de type « interbancaire » émises en France (dont 44,5 millions de cartes sans contact) ;
- 16,3 milliards d'euros de transactions réalisées (principalement en France) avec 10,9 millions de cartes de type « privatif » émises en France ;
- 44,8 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».

Les données recueillies proviennent :

- des 120 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 9 émetteurs de cartes privatives : American Express, Oney Bank, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance, Cofidis, Diners Club, 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

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

Depuis 2003, l'Observatoire de la sécurité des cartes de paiement (OSCP) établit des statistiques de fraude sur les cartes de paiement de type « interbancaire » et de type « privatif », sur la base de données recueillies auprès des émetteurs et des accepteurs. Ce recensement statistique suit une méthodologie commune, dont les définitions et typologies sont décrites en annexe 6 du présent rapport, qui a été établie dès la première année de fonctionnement de l'OSCP et dont la pertinence a été revue et confirmée récemment par une étude qualitative conduite par le groupe de travail Statistiques de fraude (voir chapitre précédent). L'Observatoire de la sécurité des moyens de paiement s'inscrit dans la continuité de ces travaux (cf. chapitre 1).

Vue d'ensemble

En 2016, le montant total de la fraude affectant les cartes de paiement françaises sur les transactions de paiement et de retrait réalisées en France et à l'étranger s'élève à 399,1 millions d'euros, en baisse de 4,1 % par rapport à 2015, pour un montant total de transactions qui atteint 628,3 milliards d'euros, en augmentation de 6,1 % par rapport à 2015.

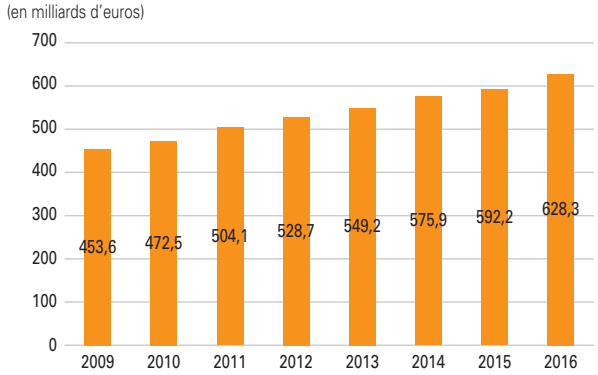
En conséquence, le **taux de fraude sur les cartes de paiement françaises baisse sensiblement à 0,064 % contre 0,070 % en 2015** (cf. graphique 9).

Le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2016 s'élève à 1 138 200, ce qui constitue une hausse de 31 % par rapport à 2015.

En incluant également les transactions réalisées en France avec des cartes émises dans d'autres pays, le montant total de la fraude s'élève à 517,5 millions d'euros en 2016, en baisse de 1,0 % par rapport à 2015, pour un montant total des transactions qui atteint 673,1 milliards d'euros, en augmentation de 5,8 %.

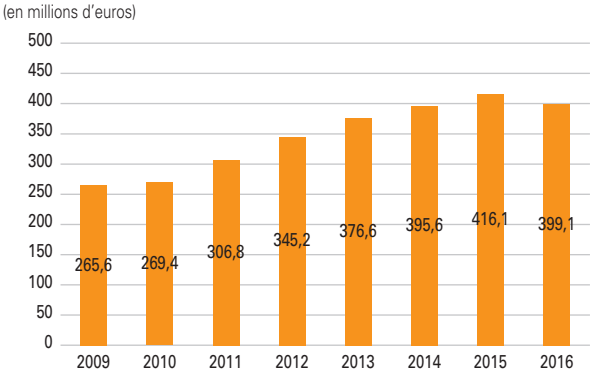
Compte tenu de ces éléments, le **taux de fraude global sur les transactions traitées dans les systèmes français**, comprenant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises

G7 Montant des transactions des cartes françaises



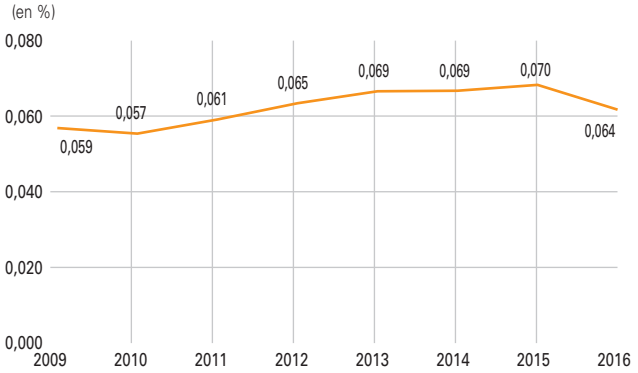
Source : Observatoire de la sécurité des moyens de paiement.

G8 Montant de la fraude des cartes françaises



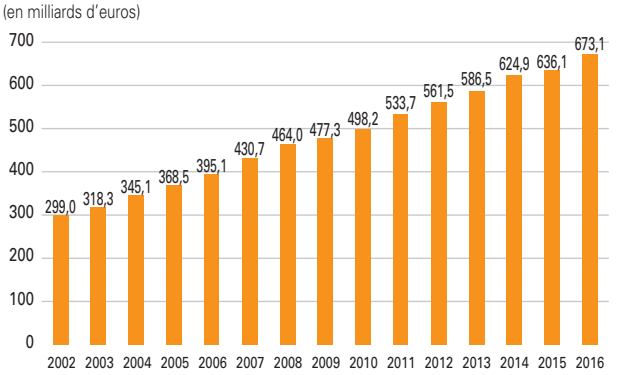
Source : Observatoire de la sécurité des moyens de paiement.

G9 Taux de fraude des cartes françaises



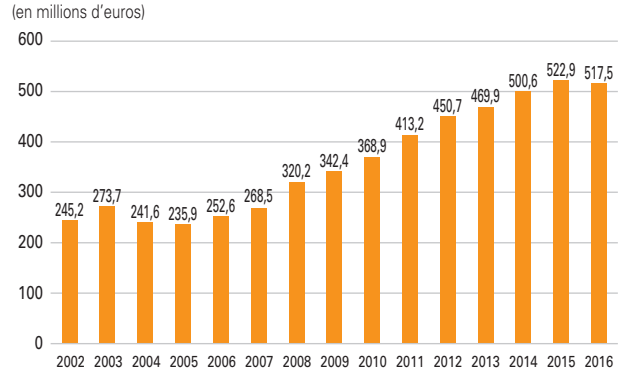
Source : Observatoire de la sécurité des moyens de paiement.

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



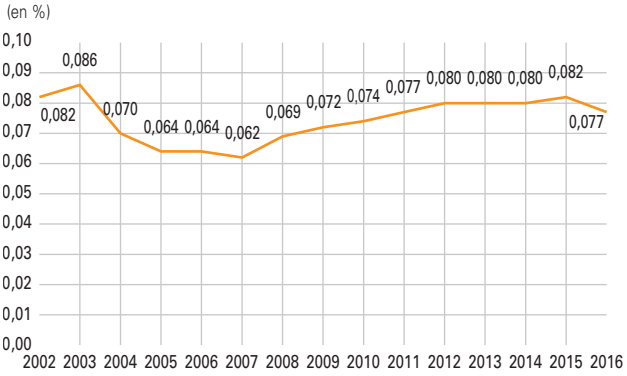
Source : Observatoire de la sécurité des moyens de paiement.

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.

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



Source : Observatoire de la sécurité des moyens de paiement

et les paiements et les retraits réalisés en France avec des cartes étrangères, **baisse sensiblement à 0,077 %, contre 0,082 % en 2015.**

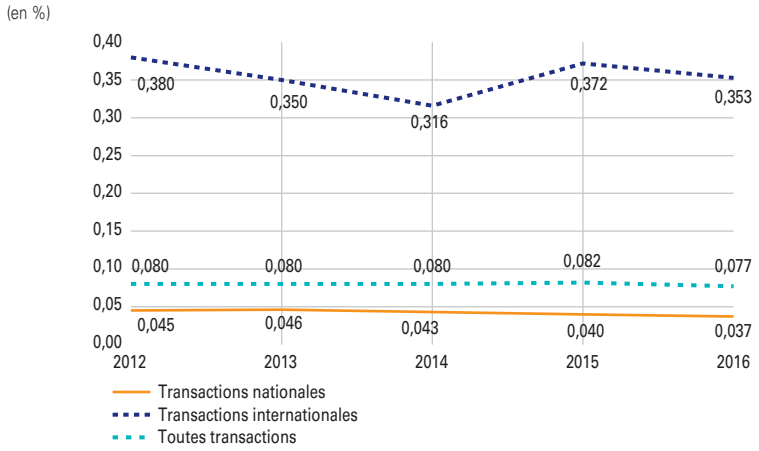
Le montant moyen d'une transaction frauduleuse baisse pour s'établir à 95 euros contre 113 euros en 2015.

Répartition de la fraude par zone géographique

La tendance à la baisse de la fraude sur les transactions nationales, observée depuis 2014, se confirme en 2016 puisque **le montant de la fraude sur les transactions nationales se réduit de près de 8 millions d'euros pour s'établir** à 217,2 millions d'euros. Le taux de fraude est également en baisse à 0,037 % contre 0,040 % en 2015.

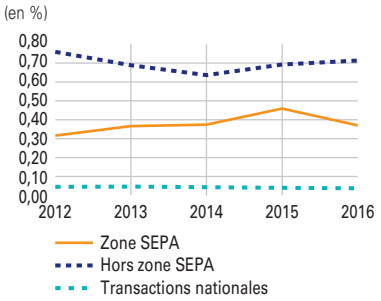
Le taux de fraude sur les transactions internationales est

G13 Taux de fraude par zone géographique



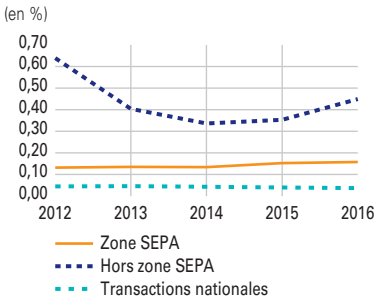
Source : Observatoire de la sécurité des moyens de paiement

G14 Taux de fraude par zone géographique – porteurs français



Source : Observatoire de la sécurité des moyens de paiement

G15 Taux de fraude par zone géographique – commerçants français



Source : Observatoire de la sécurité des moyens de paiement

également en baisse pour s'établir à 0,353 %. Le taux de fraude sur les transactions internationales demeure cependant toujours près de dix fois supérieur à celui des transactions nationales. Compte tenu de la croissance des transactions internationales, le montant de fraude reste orienté légèrement à la hausse à 300,3 millions d'euros contre 297,9 millions d'euros en 2015.

Ainsi les transactions internationales représentent 58,0 % du montant total de la fraude alors qu'elles ne comptent que **pour 12,6 % de la valeur totale des transactions.**

On continue à observer, parmi ces transactions internationales, une meilleure maîtrise de la fraude sur les transactions réalisées avec la zone SEPA [2] que sur celles réalisées avec les pays situés hors de la zone SEPA :

- pour les cartes françaises, le taux de fraude sur les transactions effectuées hors zone SEPA (0,713 %) est près de deux fois supérieur à celui des transactions effectuées au sein de la zone SEPA (0,370 %) ;

- pour les cartes étrangères, le taux de fraude sur les transactions effectuées en France avec des cartes émises hors de la zone SEPA (0,449 %) est près de trois fois supérieur à celui des cartes émises au sein de la zone SEPA (0,158 %).

Ces résultats récompensent les efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et des terminaux de paiements vers le standard EMV et pour renforcer la sécurité des paiements sur internet [3].

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

3 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 2

Fraude aux paiements par carte sans contact

L'Observatoire a collecté, pour la troisième année consécutive, les données permettant de mesurer le taux de fraude sur les paiements sans contact. Ainsi, sur l'ensemble de l'année 2016, 628,5 millions de paiements sans contact ont été enregistrés pour un montant total de 6 450,7 millions d'euros, représentant respectivement 6,5 % en volume et 1,6 % en valeur des paiements de proximité, pour un montant moyen de 12,5 euros par opération. Par ailleurs, environ 119 000 paiements frauduleux ont été recensés sur la même période pour un montant total de 1,298 million d'euros. **Le taux de fraude sur les transactions sans contact** s'élève par conséquent **à 0,020 %** sur cette période. Il se maintient, comme en 2015 où il s'établissait à 0,019 %, à un niveau intermédiaire entre le taux de fraude des paiements de proximité tous modes confondus (0,008 %) et celui des retraits (0,029 %), et se situe par conséquent à un niveau très inférieur à celui des paiements à distance (0,199 %).

Comme en 2015, la fraude aux paiements sans contact résulte quasi exclusivement du vol ou de la perte de la carte. Dans un contexte de très forte croissance des paiements sans contact où l'on observe une activité multipliée par 2,5 entre 2015 et 2016, la part de la fraude ayant pour origine la perte ou le vol de la carte continue cependant de diminuer régulièrement. La fixation par les émetteurs de carte de plafonds sur le montant maximum d'une transaction unitaire (généralement fixé à 20 ou 25 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (généralement fixé à 100 euros), permet en effet de limiter le préjudice subi en cas de perte ou de vol d'une carte.

Pour rappel, le porteur est protégé par la loi en cas de fraude. Il dispose en France de treize mois [1] pour contester les transactions non autorisées auprès de son prestataire de services de paiement, qui doit alors le rembourser dans les plus brefs délais. Les porteurs sont par ailleurs invités à faire opposition le plus rapidement possible auprès de l'établissement émetteur de la carte lorsque celle-ci est perdue ou volée. Dans le cas de fraudes résultant d'un paiement effectué en sans contact suite à une perte ou un vol de sa carte, on notera que le porteur ne supportera aucune perte liée à cette opération de paiement non autorisée [2].

1 Voir détails en annexe 2.

2 Voir annexe 1 : une opération de paiement par carte en mode sans contact est en effet effectuée sans l'utilisation du dispositif personnalisé de sécurité de la carte (absence de saisie de code), ce qui signifie que même avant opposition suite à la perte ou vol du moyen de paiement, le porteur ne peut pas supporter de pertes liées à un paiement non autorisé.

.../...

Dans un contexte continu de fort développement du taux d'équipement des porteurs, avec désormais près de 45 millions de cartes disposant de la fonctionnalité de paiement sans contact en circulation à fin décembre 2016, l'Observatoire appelle les émetteurs à maintenir toute la vigilance nécessaire, et rappelle les engagements pris par les émetteurs concernant la possibilité de désactiver la fonction sans contact des cartes, (i) en mettant des étuis de protection [3] à la disposition des utilisateurs, ou (ii) en mettant en œuvre la désactivation à distance de la fonction sans contact [4], ou enfin (iii) en permettant le remplacement, à la demande du porteur, d'une carte sans contact par une carte dépourvue de cette fonctionnalité.

La Banque de France dans son rôle de surveillant des moyens de paiement scripturaux assure un suivi de la mise en œuvre de ces mesures.

3 Étuis de carte bloquant les ondes de communications de type NFC, permettant d'éviter toute activation non sollicitée de la carte.

4 La fonction sans contact est alors désactivée par l'exécution d'un script EMV sur la carte, qui est réalisée au moment de l'insertion dans un distributeur automatique de billets ou un terminal de paiement électronique.

Répartition de la fraude par type de transaction

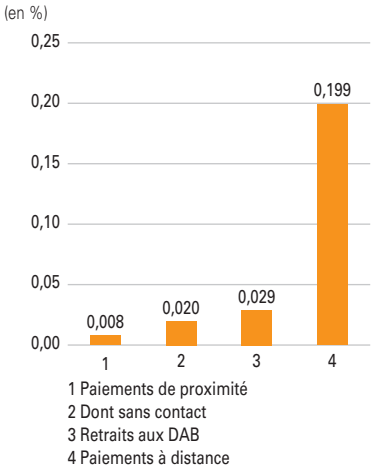
Fraude sur les transactions nationales

Le **taux de fraude sur les paiements de proximité et sur automate [4] est en baisse à 0,008 %, contre 0,009 % en 2015**. Ces paiements représentent 66,2 %, soit près des deux tiers du montant des transactions nationales, pour seulement 13,5 % du montant de la fraude.

Le **taux de fraude sur les retraits est en légère baisse pour s'établir à 0,029 %, contre 0,034 % en 2015**. Cette baisse s'explique principalement par la diminution du nombre de piratages de distributeurs automatiques de billets (301 en 2016 contre 640 en 2015) et de points de vente (434 en 2016 contre 575 en 2015). Ces appareils restant cependant des cibles toujours privilégiées pour les réseaux de fraude organisée, l'Observatoire maintient ses conseils de prudence aux porteurs et rappelle les bonnes pratiques à suivre lors d'une opération de paiement chez un commerçant ou lors d'un retrait (cf. annexe 1).

Le taux de fraude sur les paiements à distance, qui s'élève à 0,199 % contre 0,229 % en 2015, est également en baisse sensible pour la cinquième année consécutive.

G16 Comparaison des taux de fraude par type de transaction, transactions nationales



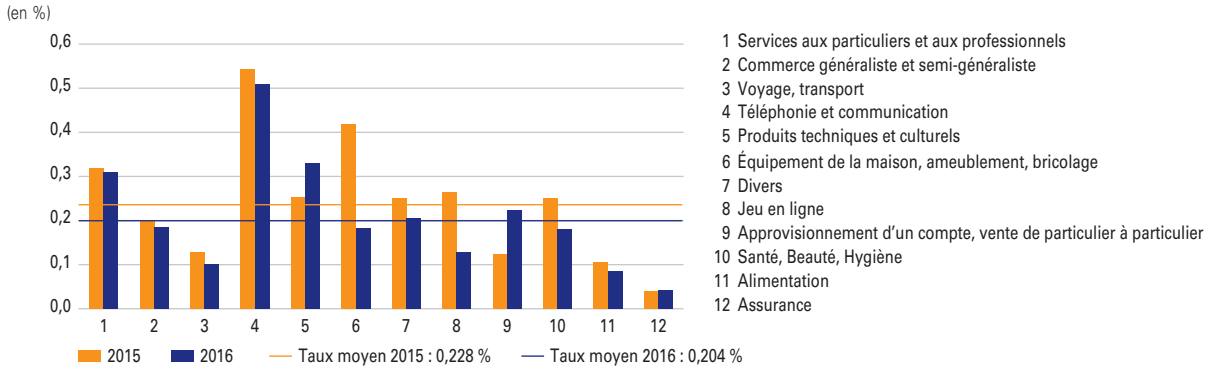
Source : Observatoire de la sécurité des moyens de paiement.

4 Comprenant notamment les distributeurs automatiques de carburant, les caisses automatiques de parking, les bornes de péage

Encadré 3

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

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



Source : Observatoire de la sécurité des moyens de paiement.

L'Observatoire a collecté des données permettant de fournir des indications sur la répartition [1] de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions nationales.

Secteur	Montant de fraude (en millions d'euros)	Part du secteur dans la fraude
Services aux particuliers et aux professionnels	40,6	26,6 %
Commerce généraliste et semi-généraliste	32,8	21,5 %
Voyage, transport	23,7	15,5 %
Téléphonie et communication	23,1	15,1 %
Produits techniques et culturels	11,9	7,8 %
Équipement de la maison, ameublement, bricolage	8,2	5,4 %
Divers	4,8	3,1 %
Jeu en ligne	2,6	1,7 %
Approvisionnement d'un compte, vente de particulier à particulier	2,2	1,4 %
Santé, Beauté, Hygiène	1,2	0,8 %
Alimentation	0,8	0,5 %
Assurance	0,4	0,3 %
Total	**152,3**	**100,0 %**

Les secteurs « Services aux particuliers et aux professionnels », « Commerce généraliste et semi-généraliste », « Voyage/transport » et « Téléphonie et communication » demeurent les plus exposés, concentrant 78,7 % du montant de la fraude en vente à distance.

Malgré une légère baisse en 2016, le secteur « Téléphonie et communication » se maintient à un taux de fraude très supérieur à la moyenne (voir graphique ci-dessous). L'Observatoire appelle tout particulièrement les acteurs de ce secteur à renforcer les mesures visant à lutter contre la fraude.

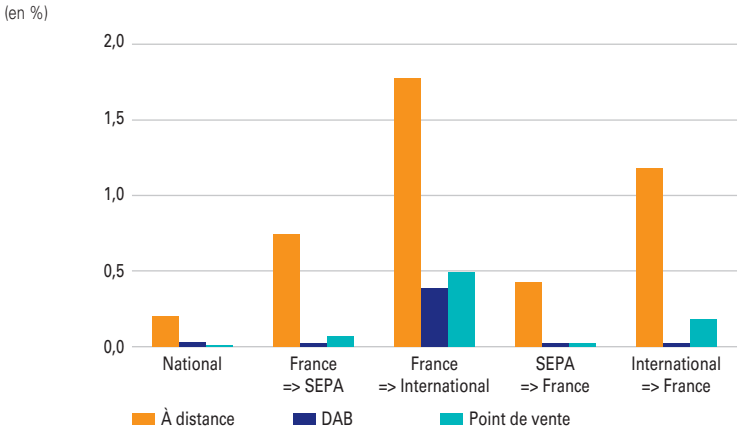
La comparaison des taux moyens de chacun des secteurs d'activité permet de constater que certains secteurs, tels les Produits techniques et culturels, qui comptent pour une plus faible part du total de la fraude, subissent néanmoins un taux de fraude largement supérieur à la moyenne.

1 Voir annexe 6 pour une description des secteurs retenus

Cependant, ce taux demeure plus de vingt fois plus élevé que le taux de fraude sur les paiements de proximité.

Ainsi, **les paiements à distance, qui ne représentent que 13 % de la valeur des transactions nationales, comptent pour plus de 70 % du montant de la fraude**. Cette situation justifie le maintien des efforts d'équipement des commerçants et des porteurs en dispositif d'authentification du payeur (cf. rubrique 2– 7).

G17 Taux de fraude par type de transaction et origine géographique



Source : Observatoire de la sécurité des moyens de paiement.

Fraude sur les transactions internationales

En ce qui concerne les transactions réalisées par les cartes françaises à l'étranger, le montant total de la fraude baisse pour celles effectuées au sein de la zone SEPA (113,8 millions d'euros contre 116,8 millions en 2015) après plusieurs années d'augmentation importante ; les taux de fraude baissent également pour chaque type d'opérations (paiements de proximité, paiements à distance et retraits). Ce phénomène peut s'expliquer par la perspective de l'entrée en vigueur, en janvier 2018, de la deuxième directive sur les services de paiement, qui prévoit l'authentification forte du porteur pour toutes les opérations de paiement électronique, et plus particulièrement dans le cas des paiements électroniques sur internet, une authentification forte du porteur comprenant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire.

Par ailleurs, on note également une baisse de la fraude pour les opérations réalisées hors zone SEPA, qui s'explique principalement par l'amélioration des outils de détection des tentatives de fraude par contrefaçon de piste magnétique.

Répartition de la fraude selon son origine

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux à distance reste la principale origine de la fraude (70,1 % en montant), en augmentation par rapport à 2015 (66,8 %).

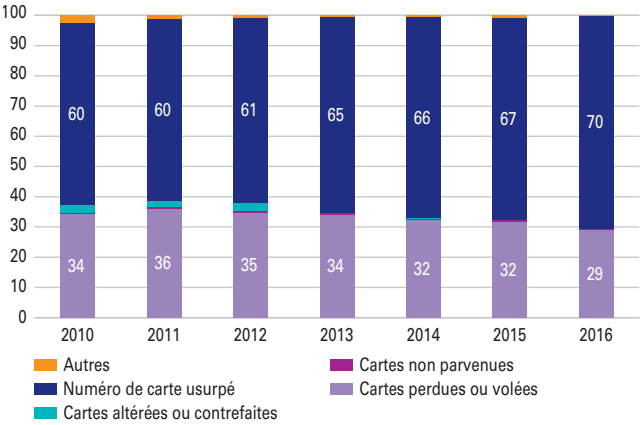
La fraude liée aux pertes et vols de cartes représente toujours près du tiers de la fraude sur les transactions nationales (29,0 %). Cette part est en diminution continue depuis cinq années (36,1 % en 2011).

La contrefaçon de cartes n'est à l'origine que de 0,2 % des paiements nationaux frauduleux. Ce niveau très bas s'explique principalement par

5 Migration de la technologie d'authentification des cartes du SDA – *Static Data Authentication* vers le DDA – *Dynamic Data Authentication*.

G18 Répartition de la fraude aux paiements par carte selon son origine

(transactions nationales, en valeur, hors retraits)



Source : Observatoire de la sécurité des moyens de paiement.

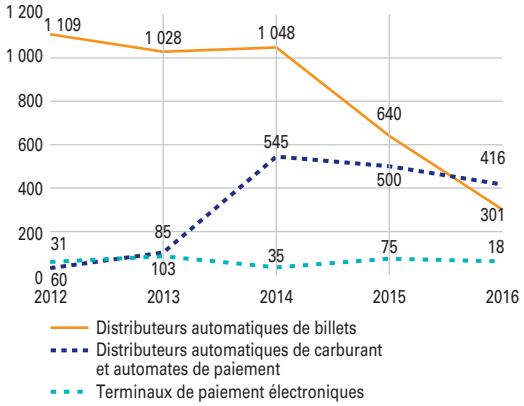
l'adoption de technologies de cartes à puce par le plus grand nombre de systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes [5].

Encadré 4

Indicateurs des services de police et de gendarmerie

Le nombre de piratages de distributeurs automatiques de billets (DAB) est à nouveau en baisse sensible en 2016 avec 301 cas (contre 640 en 2015) après s'être maintenu à des niveaux plus élevés les années précédentes (environ 1 000 cas par an entre 2012 et 2014, autour de 500 cas par an entre 2011 et 2006, 200 en 2005 et seulement 80 cas en 2004). À ceux-ci s'ajoutent 434 piratages ciblant les points de vente (contre 575 en 2015), dont 354 piratages de distributeurs automatiques de carburant (DAC), 18 compromissions de terminaux de paiement chez les commerçants et 62 piratages d'automates de paiement (telles les bornes de parking). Malgré une baisse encourageante, en particulier pour les DAB, ces chiffres demeurent élevés et confirment dans les faits l'intérêt constant que portent les réseaux criminels à la collecte des données de carte. Ces données 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 encore mis en œuvre l'authentification renforcée du porteur de la carte.

Nombre d'infractions constatées sur les distributeurs et terminaux



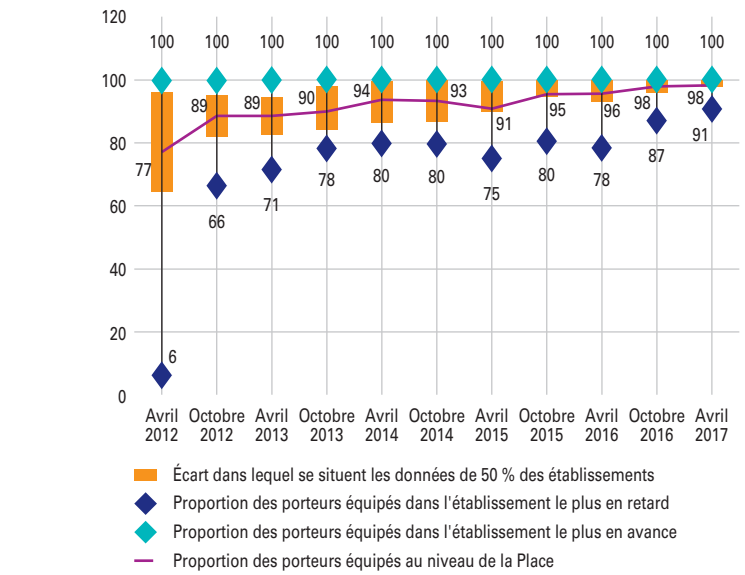
Source : Observatoire de la sécurité des moyens de paiement.

Suivi du déploiement de l'authentification forte

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 protection des transactions. Dans ce contexte, les recommandations émises dès 2008 par l'Observatoire de la sécurité des cartes de paiement afin de renforcer la sécurité du paiement à distance portent sur la généralisation des dispositifs d'authentification forte ; ces recommandations font l'objet d'un suivi statistique depuis 2011.

G19 Distribution du taux d'équipement des porteurs en dispositif d'authentification forte

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

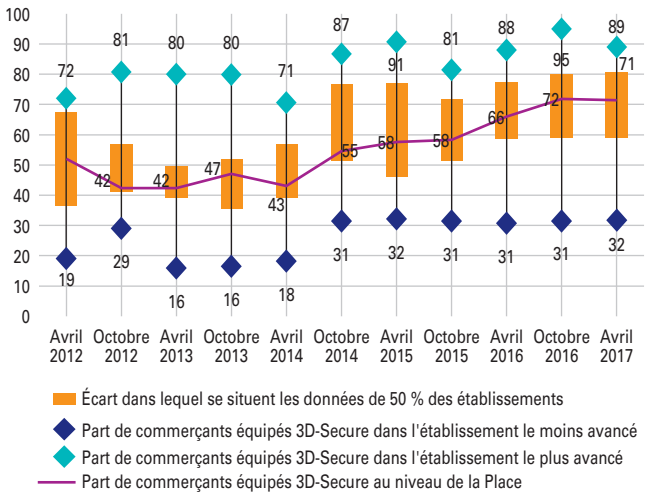
Pour la période de novembre 2016 à avril 2017, le suivi statistique du déploiement des solutions d'authentification réalisé par l'Observatoire auprès des principaux établissements bancaires porte sur un volume de 61,6 millions de cartes de paiement et 45,1 milliards d'euros de transactions en valeur (dont 15,7 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 renforcée.

L'année 2017 vient confirmer l'achèvement du processus d'équipement des porteurs en authentification forte constaté l'année précédente, avec un taux moyen en 2016 de 98 %, permettant de couvrir la totalité des porteurs susceptibles de réaliser des transactions sur internet.

Du côté des e-commerçants, le taux d'équipement en dispositif d'authentification forte continue à progresser pour s'établir à 71 %, dans le prolongement des hausses constatées au cours des trois dernières années. L'Observatoire et la Banque de France encouragent les acteurs

G20 Distribution du taux d'équipement des commerçants en dispositif 3D-Secure

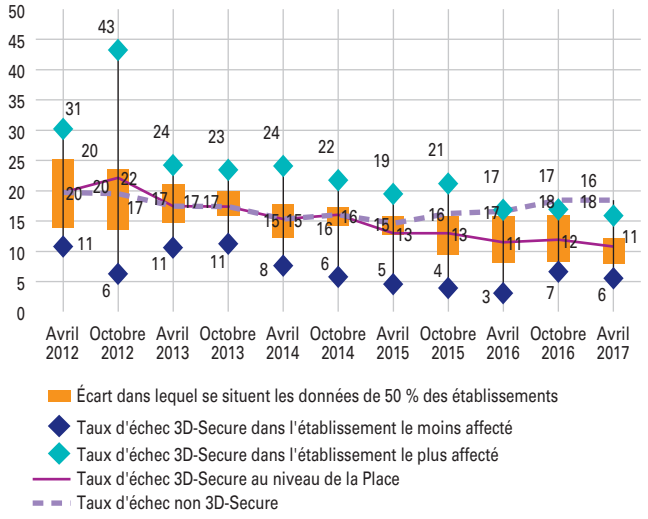
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G21 Distribution du taux d'échec 3D-Secure (3DS)

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

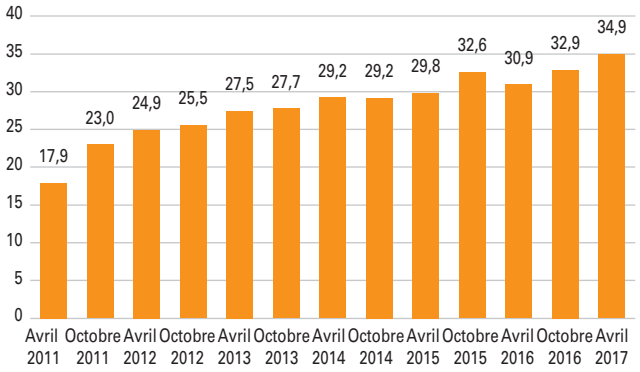
du e-commerce à adopter des dispositifs d'authentification renforcée des paiements, quelle que soit la nature de leur clientèle, d'ici l'entrée en vigueur en 2018 de la seconde direction européenne sur les services de paiement.

L'Observatoire constate une poursuite de la baisse du taux d'échec sur les transactions authentifiées qui passe en dessous de 11 % et reste sensiblement inférieur à celui des transactions non authentifiées, permettant 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 forte, laquelle pousse les fraudeurs à privilégier par défaut des sites non équipés.

Compte-tenu de ces différentes évolutions favorables au développement du recours à l'authentification forte, la proportion de paiements en ligne authentifiés 3D-Secure poursuit une progression continue depuis 2011, pour s'approcher de 35 % des montants de paiement par carte à distance.

G22 Part des paiements en ligne authentifiés par 3D-Secure

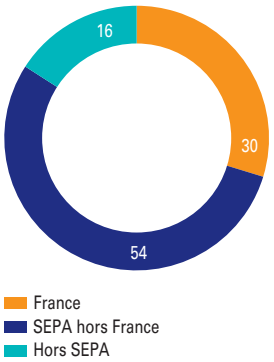
(en %)



Note : Compte-tenu d'un changement de périmètre dans la collecte de ces données statistiques, les valeurs relatives aux exercices 2015 et 2016 ont été ré-estimées par rapport aux données publiées dans le rapport annuel 2015 de l'Observatoire de la Sécurité des cartes de paiement.
Source : Observatoire de la sécurité des moyens de paiement.

G23 Répartition de la fraude au virement en montant par zone géographique

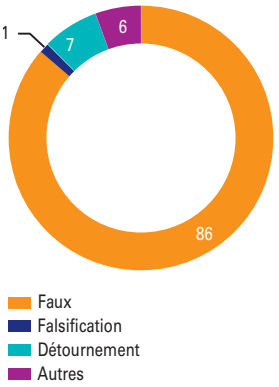
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G24 Répartition de la fraude au virement en montant par typologie de fraude

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

2.3 État de la fraude sur le virement

Vue d'ensemble

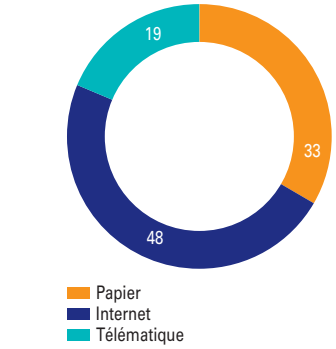
En 2016, le montant total de la fraude sur les virements émis depuis un compte tenu en France s'élève à 86 millions d'euros pour près de 23 700 milliards d'euros de transactions. Ainsi, le taux de fraude en montant pour ce moyen de paiement s'établit à 0,00036 %, soit l'équivalent d'un euro de fraude pour environ 275 000 euros de virements émis. Ces données positionnent le virement comme le moyen de paiement scriptural le moins fraudé en proportion, alors qu'il est le plus utilisé en montant d'opérations (89 %). Le montant moyen d'un virement frauduleux se situe à 15 500 euros.

Les virements transfrontaliers subissent en proportion une fraude plus importante que les virements nationaux, et représentent 70 % des montants fraudés alors que les transactions transfrontalières ne comptent que pour 23 % des virements émis en montant.

Les virements frauduleux ont essentiellement pour origine le faux virement, qui représente à lui seul 86 % du montant total de la

G25 Répartition de la fraude au virement en montant par canal de transmission

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

fraude. La seconde forme de fraude rencontrée est le détournement (7 % en valeur) [6].

L'initiation de virement depuis l'espace de banque en ligne (sur internet ou *via* application mobile) est le canal le plus vulnérable et concentre près de la moitié de la fraude globale (48 % en valeur). La fraude sur support papier (courrier, fax) représente un tiers de la fraude, et celle initiée par des canaux télématiques sécurisés 19 %.

Principaux cas de fraude en 2016 et mesures de prévention

Les principales techniques de fraude sur le virement constatées en 2016 sont, d'une part, la fraude par ingénierie sociale [7] et, d'autre part, les attaques informatiques par *malware* et *phishing*.

6 Les typologies de fraude au virement sont présentées au chapitre 1, paragraphe 3

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

Cas de fraude rencontrés en 2016 sur le virement

En 2016, la fraude par **ingénierie sociale** a revêtu essentiellement les formes suivantes :

- **la fraude au président** : le fraudeur usurpe l'identité d'un haut responsable de l'entreprise pour obtenir d'un collaborateur la réalisation d'un virement urgent et confidentiel à destination de l'étranger. Pour ce faire, le fraudeur utilise des informations recueillies sur l'entreprise et ses dirigeants sur internet ou directement auprès des services de l'entreprise ;
- **la fraude aux coordonnées bancaires :** le fraudeur usurpe l'identité d'un fournisseur, bailleur ou autre créancier et prétexte auprès du client, locataire ou débiteur un changement de coordonnées bancaires aux fins de détourner le paiement des factures ou loyers. Le fraudeur envoie les nouvelles coordonnées bancaires par courrier électronique ou avec un courrier en bonne et due forme du créancier ;
- **la fraude au faux technicien** : le fraudeur usurpe l'identité d'un technicien informatique (de la banque, par exemple) pour effectuer des faux tests dans le but de récupérer des identifiants de connexion, provoquer des virements frauduleux ou encore procéder à l'installation de logiciels malveillants.

Mesures de prévention

Outils de surveillance et de détection des transactions à caractère inhabituel qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison par exemple de son montant ou du pays destinataire des fonds eu égard à l'activité habituelle du client. Un contre-appel auprès du client peut alors être fait afin de vérifier le bien-fondé de l'ordre de virement.

Actions d'information et de sensibilisation menées par les banques et les prestataires de services de paiement auprès des entreprises.

Cas de fraude rencontrés en 2016 sur le virement

Les attaques informatiques ont principalement visé en 2016 les sites de banque en ligne et les canaux télématiques, tels que par exemple le système EBICS (canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque) et ont été réalisées essentiellement par :

- ***malwares*** : des logiciels malveillants (tels que les troyens, les *spammeurs*, les virus,…) 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 compromis 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 à titre d'exemple, lors de la connexion au site de banque en ligne d'un client, le *malware* récupère les identifiant et mot de passe que le client a saisis puis les réutilise pour s'y connecter lui-même, faire une demande d'ajout de bénéficiaire et initier un ordre de virement frauduleux.

- ***phishing* ou hameçonnage** : technique permettant de collecter des données personnelles et bancaires à partir de courriels non sollicités invitant leurs destinataires à cliquer sur un lien renvoyant vers un faux site (celui d'une banque en ligne ou d'un marchand en ligne) lequel le plus souvent demande à l'internaute de communiquer ses coordonnées bancaires. Ces courriels sont le plus souvent à connotation alarmiste et demandent à leur destinataire une intervention rapide (facture à régler sous peine de la suspension d'un service, régularisation d'une interdiction bancaire ou encore une mise à jour sécuritaire). Des variantes du *phishing* sur d'autres canaux sont également mises en œuvre, on parle alors de *vishing* pour le téléphone ou de *smishing* pour le SMS.

Mesures de prévention

Déploiement d'un dispositif d'authentification forte pour la validation des ordres de virement saisis en ligne.

Mise en place d'une temporisation ou d'une authentification forte du client pour l'ajout de nouveaux bénéficiaires de virement depuis le site de banque en ligne.

Fixation de plafonds maximaux de virements sur le site de banque en ligne.

Mise à disposition de la clientèle de solutions informatiques de sécurisation permettant la recherche d'infections de type *malware* sur ses terminaux.

Outils de surveillance et de détection des transactions à caractère inhabituel qui permettent de suspendre l'exécution d'un virement analysé comme suspect en raison par exemple de son montant ou du pays destinataire des fonds eu égard à l'activité habituelle du client. Une alerte peut être adressée au client pour lui permettre de faire opposition à la transaction le cas échéant pendant la durée de temporisation.

Actions d'information et de sensibilisation menées par les banques et les prestataires de services de paiement auprès des particuliers.

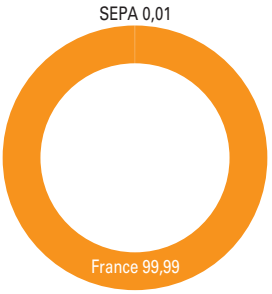
2.4 État de la fraude sur le prélèvement

Vue d'ensemble

En 2016, la fraude sur le prélèvement émis au débit d'un compte tenu en France représente 40 millions d'euros pour un montant total de transactions de 1 492 milliards d'euros. Le taux de fraude en montant pour ce moyen de paiement s'établit à 0,003 % ce qui représente l'équivalent d'un euro

G26 Répartition de la fraude au prélèvement en montant par zone géographique

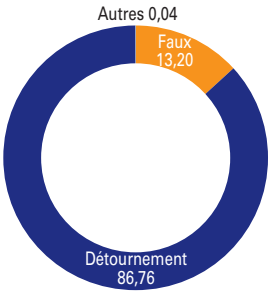
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G27 Répartition de la fraude au prélèvement en montant par typologie de fraude

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

de fraude pour environ 37 000 euros de prélèvements émis. Le montant moyen d'un prélèvement frauduleux s'établit à 34 000 euros.

La fraude sur le prélèvement est concentrée sur les transactions nationales, et est très marginale sur les transactions transfrontalières avec la zone SEPA.

Le détournement [8] constitue la forme de fraude sur le prélèvement la plus répandue, puisqu'il représente 87 % du montant total de la fraude. La fraude est également imputable mais dans une moindre mesure (13 % en valeur) à l'émission de faux prélèvements.

8 Les typologies de fraude au prélèvement sont présentées au chapitre 1, paragraphe 4.

Cas de fraude rencontrés en 2016 sur le prélèvement	Mesures de prévention
Émission illégitime d'ordres de 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. **Envoi d'une alerte aux clients débiteur** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelée aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelée aussi « listes noires »)
Usurpation d'IBAN pour la souscription de service : 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 débiteur** lors de la première occurrence d'ordre de prélèvement émise par un créancier sur son compte. **Services optionnels** proposés à la clientèle permettant notamment de fixer des limitations de montant par créancier et par pays ou encore de dresser des listes de créanciers autorisés à effectuer des prélèvements sur le compte du client (appelée aussi « listes blanches ») ou, *a contrario*, des listes de créanciers qui ne sont pas autorisés à le faire (appelée 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.

Enfin, la fraude au prélèvement n'a affecté en 2016 que le prélèvement SEPA, aucun cas de fraude n'ayant été déclaré sur le TIP (Titre Interbancaire de Paiement) et le télérèglement, qui avaient cours jusqu'au 1er février 2016 et étaient apparentés à cette catégorie de moyens de paiement.

2.5 État de la fraude sur le chèque

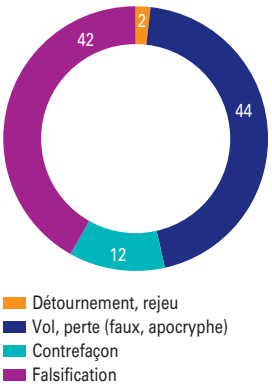
Vue d'ensemble

En 2016, le montant total de la fraude sur les chèques payés en France s'élève à 272 millions d'euros pour un volume d'activité de 1 077 milliards d'euros, soit un taux de fraude de 0,0252 %. Ces données placent le chèque comme le deuxième moyen de paiement le plus fraudé après la carte de paiement alors qu'il est le quatrième moyen de paiement en termes d'utilisation. Le montant moyen d'un chèque fraudé est de 2 300 euros.

Deux catégories de fraude représentent la majeure partie des cas rencontrés en 2016, à parts quasiment égales : d'un côté, l'utilisation frauduleuse de chèques perdus ou volés représente 45 % du total de la fraude sur le chèque, pour un montant unitaire moyen de l'ordre de 1 300 euros ; de l'autre, la falsification d'un chèque régulièrement émis représente 42 % des montants fraudés, pour un montant unitaire moyen plus élevé, à 7 400 euros. Enfin, la fraude par contrefaçon de chèques et par détournement/rejeu représentent des portions moindres (respectivement 12 % et 2 % de la fraude chèque).

G28 Répartition de la fraude par chèque en montant par typologie de fraude

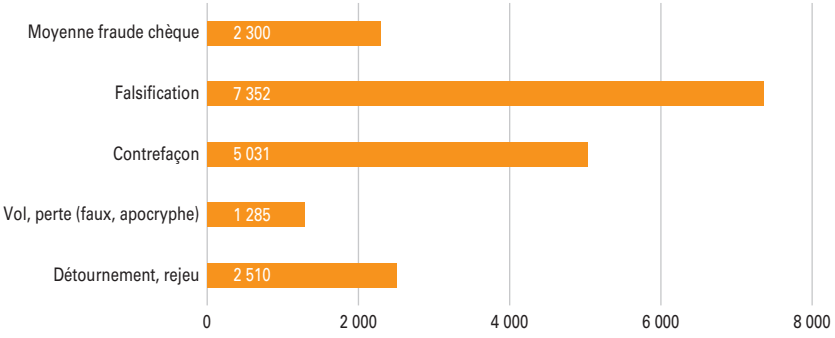
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

G29 Montants unitaires de fraude chèque par typologie de fraude

(en euros)



Source : Observatoire de la sécurité des moyens de paiement.

Principaux cas de fraude en 2016 sur le chèque	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 trois niveaux : • en amont de la délivrance au client : chez les prestataires fabricants et/ou expéditeurs, chez les prestataires transporteurs ou distributeurs vers les agences bancaires, dans les boîtes à lettres des clients bénéficiaires. • lors de la remise en agences bancaires, les fraudeurs utilisent des pièces d'identité volées ou falsifiées pour se faire remettre un chéquier. **Vol de chéquiers lors de la détention par le client lui-même** faisant suite à un cambriolage, au vol ou la perte de son chéquier.	**Traçabilité des envois** de chéquiers et lettres chèques durant les phases de transport **Information par la banque de la mise à disposition d'un chéquier**, soit en agence bancaire, soit par pli postal selon l'option définie par le client lors de la souscription au moyen de paiement et indication d'un délai attendu de mise à disposition permettant au client d'informer sa banque en cas de retard constaté. **Rappel régulier par les banques des obligations de vigilance** des détenteurs de chéquiers et lettres chèques et de l'obligation de déclaration en cas de perte ou de vol, même en cas de souscription d'une assurance couvrant ces évènements.
Falsification d'un chèque régulier intercepté par les fraudeurs, consistant à altérer le chèque subtilisé par grattage, gommage ou effacement se manifeste par le fait que concrètement, les fraudeurs tirent profit des vulnérabilités présentes sur le chèque subtilisé pour le modifier, par exemple : • En substituant, par grattage ou gommage, le nom du bénéficiaire légitime inscrit avec une encre faible, • En réécrivant un nom de bénéficiaire sur celui du bénéficiaire légitime, • En ajoutant une mention (par exemple nom ou sigle, tampon de société etc.) après celui du bénéficiaire légitime sur l'espace libre de la ligne non rempli. • En ajoutant un montant en lettres et/ou en chiffres sur l'espace libre laissé avant ou après la mention manuscrite.	**Examen systématique du chèque et des mentions portées, ainsi que de leur cohérence avec l'identité du payeur.** Il s'agit de réaliser un examen physique du chèque afin d'identifier les éventuelles altérations avant son acceptation, ainsi que de contrôler l'identité du payeur, *via* la demande par exemple d'une pièce d'identité ou d'un justificatif de domicile. **Les commerçants peuvent se prémunir des chèques irréguliers en accédant au Fichier national des chèques irréguliers (FNCI)** de la Banque de France, service officiel de prévention des impayés chèques [1].
Contrefaçon de chèque, en créant un faux chèque de toutes pièces, émis sur une banque existante ou une fausse banque.	**Examen physique approfondi du chèque et des documents d'identité du payeur** (voir 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 consécutifs à une remise de chèques.

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

3 L'acceptation des paiements par carte en situation de mobilité

3.1 Introduction

L'innovation technologique joue un rôle clef dans le développement des paiements électroniques, notamment par carte bancaire, en enrichissant l'offre de paiement disponible. Ainsi, alors que la carte est à l'origine un instrument de paiement conçu pour une utilisation au point de vente au travers d'un dispositif de lecture physique, les développements technologiques qu'elle a connus lui permettent d'initier des paiements par d'autres canaux, tels que les transactions par internet ou en mode sans contact.

Au-delà de ces développements, plusieurs fois abordés dans les travaux de l'Observatoire [1], les acteurs du marché se sont également attachés à s'appuyer sur l'innovation technologique pour enrichir l'offre de paiement au point de vente, pour apporter des solutions adaptées à leur acquisition par les professionnels amenés à gérer des situations de vente ou de prestation en mobilité (artisans et services à domicile, professions libérales, taxis…). Cette piste d'évolution constitue d'ailleurs un des axes de développement identifiés au titre de la Stratégie nationale des paiements, en réponse aux objectifs visant à « faciliter l'acceptation des paiements par carte » et à « proposer des solutions alternatives à l'usage du chèque ».

Pour mémoire, l'Observatoire avait conduit dès 2011 une analyse de veille portant sur « le mobile comme terminal de paiement », qui concluait :

« L'utilisation d'un terminal de paiement mobile dans la chaîne d'acceptation ne peut donc être actuellement envisagée que concomitamment à l'adoption de mesures permettant de garantir un niveau de sécurité équivalent à celui prévalant pour les terminaux de paiement traditionnels.

La rapide évolution de ces solutions et leur faible degré de maturité sur le marché français appellent toutefois l'ensemble des acteurs à examiner de plus près les usages possibles et à venir pour ces terminaux de paiement, dont la majorité [ne répondait pas en 2011] aux exigences en vigueur. Cette analyse devra être menée en tenant compte de l'internationalisation croissante de la filière d'acquisition et du développement d'offres similaires en Europe. Il conviendra, dans ce contexte, de disposer de conditions sécuritaires adéquates et d'un cadre juridique adapté à ces modes d'acceptation, en précisant notamment la nature des relations contractuelles et en identifiant les responsabilités de chacun dans la chaîne de paiement. L'Observatoire sera attentif à ces futures évolutions. »

1 Notamment, études de veille technologique du rapport annuel 2014 sur les paiements sans contact, et du rapport annuel 2015 sur les paiements par mobile et les nouvelles solutions d'authentification des paiements à distance.

La présente étude de veille technologique sur les solutions d'acceptation des paiements en situation de mobilité vise à actualiser et compléter les conclusions de cette étude, en tenant compte des innovations technologiques survenues depuis et de la plus grande maturité des acteurs du marché pour le développement d'offres commerciales abouties et sécurisées.

3.2 État des lieux des solutions d'acceptation mobile ou en situation de mobilité

Périmètre

Il existe deux grandes familles de solutions d'acceptation de paiements de proximité par carte adaptées aux besoins de professionnels mobiles :

• Les solutions sur terminaux autonomes qui sont en capacité de se connecter au réseau d'un opérateur téléphonique pour échanger avec l'acquéreur. Ces solutions, similaires à celles des terminaux de paiement traditionnels des commerçants, se distinguent de ces dernières par leur capacité de connexion aux réseaux mobiles des opérateurs de téléphonie, se substituant à l'usage des lignes téléphoniques fixes (lignes de téléphonie classiques de type RTC ou haut-débit par ADSL ou fibre optique).

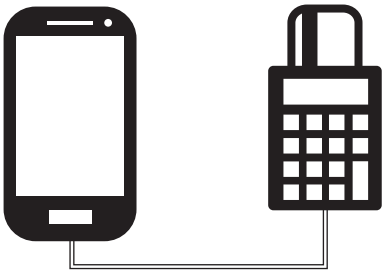
• Les solutions reposant sur l'appairage d'un module de lecture de carte avec un smartphone ou une tablette au moyen d'une connexion filaire (câble USB ou *Lightning*…) ou sans fil (*Bluetooth*, WiFi…), couramment dénommées sous l'acronyme m-POS pour « *mobile point of sale* ». Dans ce cas de figure, le module dédié est équipé d'une ou de plusieurs interfaces pour les cartes de paiement permettant de lire une piste ou d'échanger des données avec une puce EMV (*Europay Mastercard Visa*) en mode contact ou sans contact ; l'appairage avec un appareil connecté de type smartphone ou tablette permet au module de lecture de carte de disposer d'un modem de communication sur les réseaux

Illustration de solutions de type terminal autonome

Illustrations de solutions de type m-POS

En connexion sans fil

En connexion filaire



de téléphonie mobile avec l'établissement acquéreur. Selon les cas le dispositif peut être équipé d'une imprimante connectée pour l'édition du ticket de transaction ; dans le cas contraire, le dispositif permet l'envoi du ticket sous forme numérique, par SMS ou e-mail, systématiquement ou à la demande du client.

Solutions de type vente à distance (exclues du champ de l'étude)

En alternative au recours à un matériel dédié (terminal autonome ou m-POS), certains professionnels peuvent être tentés de recourir à une solution de paiement de type vente à distance. Cette dernière consiste en une application ou un site web permettant d'initier un paiement à partir de la saisie des données de la carte, de façon similaire à celle d'un paiement sur un site d'e-commerce. Dans ce cadre, des technologies d'aide à la saisie, telles que la reconnaissance de caractères par photographie de la carte ou la lecture des données par interface NFC (*near field communication*), peuvent être mises en œuvre.

Ces solutions logicielles ne sont pas assimilables à une transaction au point de vente, dans la mesure où elles ne s'appuient pas sur les dispositifs de sécurité physiques embarqués par la carte (notamment, les propriétés cryptographiques intégrées à la puce).

La sécurité de ces solutions est donc d'un niveau intrinsèquement plus faible, le taux de fraude sur les paiements à distance étant près de 20 fois supérieur à celui des transactions de proximité. *Leur usage pour les situations de vente en présence physique du porteur et du professionnel est donc à proscrire*.

L'Observatoire ayant déjà émis des recommandations relatives à la sécurité des paiements à distance [2], ce type de dispositif est exclu de la présente étude de veille technologique.

3.3 État des lieux du déploiement de solution d'acceptation m-POS

L'Observatoire a collecté auprès des principaux établissements et groupes bancaires de la Place française des données de suivi du déploiement des terminaux de paiement mobiles de type m-POS. Certains établissements ont également communiqué des données relatives aux transactions de type TPE (terminal de paiement électronique) connecté à un réseau de téléphonie mobile.

État de l'offre

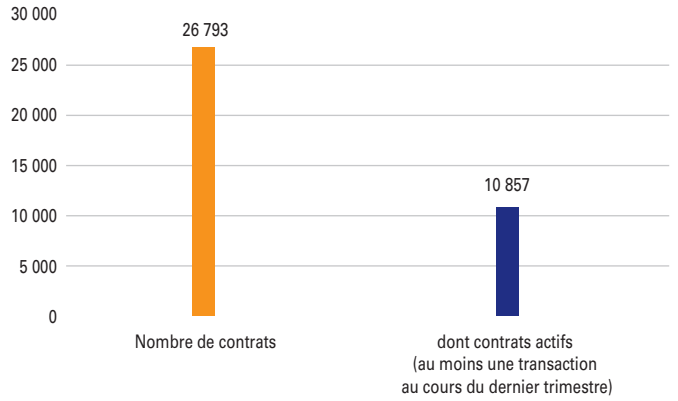
Les matériels actuellement commercialisés par les établissements interrogés sont constitués de boîtiers de lecture de carte permettant la lecture de la puce et de la piste magnétique, et connectés à un smartphone ou une tablette en utilisant la technologie sans fil Bluetooth. La plupart de ces solutions font toutefois l'objet de projets d'évolution, en vue de permettre l'acceptation des paiements en mode sans contact à horizon 2017 ; des projets de développement de

2 Notamment, rapport annuel 2009 de l'Observatoire : ces recommandations, visant à promouvoir l'authentification forte du porteur pour les paiements à distance, ont par ailleurs été reprises dans les recommandations publiées par la Banque centrale européenne en 2013, puis dans les orientations émises par l'Autorité bancaire européenne en 2014. Le recours systématique à l'authentification forte pour les paiements électroniques fait partie des dispositions phares de la deuxième directive européenne sur les services de paiement, qui entrera en vigueur en janvier 2018 dans l'ensemble de l'Union européenne.

connexion filaire sont également envisagés sur certaines de ces solutions. Par ailleurs, il est à noter que les solutions commercialisées en France respectent toutes les règles de sécurité établies par le PCI SSC (*Payment Card Industry Security Standard Council*) et sont certifiées par les principaux réseaux de paiement interbancaires (CB, Visa, Mastercard).

À noter que la date de lancement commercial pour les équipements de type m-POS varie sensiblement d'un établissement à l'autre, puisque les premières offres ont été commercialisées dès la mi-2014 tandis que certains établissements élaborent encore leur offre en vue d'une commercialisation à l'horizon 2017.

G1 Commercialisation des solutions m-POS en France



Source : OSMP – Données à septembre 2016.

Paiements

À mi-2016, le nombre de paiements par carte en situation de mobilité sur des matériels de type m-POS enregistrés chez des accepteurs clients des principaux établissements bancaires français s'élevait à près de 450.000 transactions par trimestre, pour un montant d'environ 22,5 millions d'euros.

En comparaison des transactions sur des terminaux classiques de type TPE-GPRS, ce mode d'acceptation demeure toutefois un épiphénomène dans le domaine de la vente en situation de mobilité. En effet, les données collectées, par les groupes bancaires ayant rapporté les données relatives aux deux types de terminaux révèlent un ratio de 1 paiement m-POS pour 250 paiements sur des terminaux GPRS.

Fraude

Les principaux groupes bancaires français ont indiqué ne pas subir de fraude significative sur les paiements aux terminaux de type m-POS. Ainsi, le montant trimestriel des transactions frauduleuses s'élève à environ un millier d'euros (pour 35 cas de fraude), soit un taux de fraude de 0,004 % en montant. Ce niveau reste globalement inférieur à celui des paiements de proximité (0,009 % en moyenne).

L'Observatoire note que ces données de fraude ont été mesurées sur la base d'un faible volume de ce type de transactions, et sont donc non représentatives d'une utilisation généralisée de ce type de terminal. Ces chiffres attestent toutefois qu'aucune faille de sécurité n'a vraisemblablement pu être identifiée et exploitée à ce stade par les fraudeurs.

3.4 Enjeux attachés au niveau de sécurité du m-POS

Solutions de type terminal autonome

Ces solutions bénéficient d'un environnement contrôlé exactement similaire aux terminaux de paiement utilisés en magasin, et qui ont fait l'objet des recommandations passées de l'Observatoire visant à en assurer la sécurité.

Pour mémoire, les principales exigences vis-à-vis de ces terminaux portent sur le respect des standards EMV (rapport annuel 2009 de l'Observatoire) et des règles PCI-PTS (*Payment Card Industry - Pin Transaction Security*) développées par le PCI SSC et visant à assurer la sécurité des dispositifs permettant la saisie du code confidentiel pour les transactions par carte au point de vente.

Solutions de type m-POS

L'évaluation du niveau de sécurité des solutions m-POS doit prendre en compte l'ensemble des composants intervenant dans leur mise en œuvre : le smartphone ou la tablette, le module de lecture de carte dédié, le serveur de gestion centralisé et leurs interfaces d'échange respectives. Si le module de lecture de carte et le serveur de gestion monétique sont dédiés à cette activité et peuvent donc bénéficier de mêmes certifications contraignantes en matière de sécurité que les terminaux de paiement traditionnels, le smartphone ou la tablette ne peut raisonnablement pas être soumis à ces mêmes contraintes, et constitue donc la principale source de risque pour ces solutions.

Les principes de sécurité applicables en Europe[3] aux terminaux de paiement par carte visent à protéger les données de la carte, le code confidentiel et sa saisie, et d'éviter ainsi tout risque de détournement. Ces principes impliquent la présence d'un dispositif de saisie du code confidentiel de la carte protégé techniquement contre le risque d'interception des données, et disposant à ce titre d'une certification de type PCI-PTS. *Un tel niveau de sécurité requiert, en l'état actuel des technologies, la présence d'un clavier physique dédié et certifié sur le module de lecture de carte*[4] ; en effet, une saisie sur l'écran ou le clavier du smartphone appairé serait vulnérable à une interception des données par un logiciel malveillant installé sur le smartphone.

À l'autre extrémité du dispositif, *le serveur de gestion doit être en mesure de protéger les données des opérations dans un environnement distant et sécurisé*, et doit être soumis à ce titre à une obligation de certification de type PCI-DSS (*Payment Card Industry - Data Security Standard*).

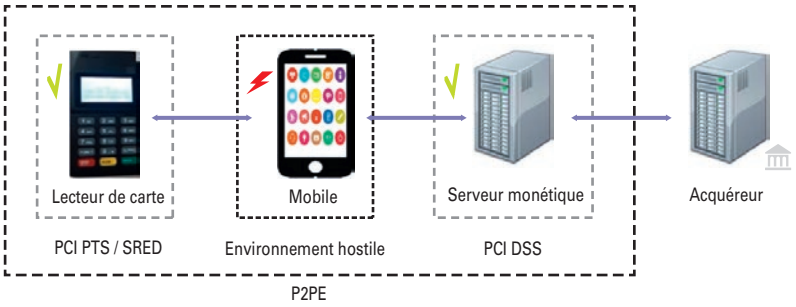
Entre ces deux éléments dédiés du dispositif de paiement, le smartphone constitue un point de vulnérabilité central : en effet, s'agissant d'un matériel appartenant au commerçant et utilisé pour des fonctions autres que le paiement, la sécurité de l'environnement logiciel du smartphone ne peut être assurée de manière certaine par l'établissement acquéreur. Cette exposition potentielle à des failles de sécurité justifie la mise en

3 Notamment, *SEPA Cards Framework* de l'*European Payments Council* (EPC) et cadre de surveillance des systèmes de paiement par carte de l'Eurosystème.

4 Si d'autres zones géographiques, du fait d'exigences sécuritaires moindres, autorisent l'utilisation de terminaux de type m-POS équipés d'un simple lecteur de carte sans clavier de saisie (la saisie du code confidentiel se faisant alors sur le smartphone), les systèmes de paiement par carte opérant en Europe sont tenus de bloquer l'acquisition de paiement par ce type de dispositif allégé non conforme aux cadres de surveillance applicables dans l'Espace SEPA.

Encadré 1

Les différents composants d'une solution de type m-POS et les certifications de sécurité associées



Module de lecture de carte : dispositif technique de confiance qui permet l'acceptation de moyens de paiement par carte afin de réaliser des paiements de proximité. Il permet d'échanger des informations avec le moyen de paiement, de réaliser des contrôles (sécurité, validité, risques, etc.) et de transmettre les données des transactions à l'acquéreur. Le niveau de sécurité requis impose qu'il dispose d'un écran, d'un clavier et d'un dispositif de lecture de données carte. Il doit garantir la confidentialité et l'intégrité des données (code PIN, données de compte) et être certifié PCI-PTS (*Payment Card Industry - PIN Transaction Security*) and SRED (*Secure Reading and Exchange of Data*).

Mobile : équipement de communication nomade (smartphone, tablette, etc.) de l'accepteur (commerçant, etc.) hébergeant une application qui combinée avec un terminal permet d'accepter les paiements carte (avec une carte ou un appareil compatible NFC tel qu'un téléphone mobile). Cet élément ne propose pas de mécanismes de sécurité et des éléments d'assurance (évaluation, certification…) permettant de garantir la confidentialité et l'intégrité des données des transactions de paiement. Il est considéré comme « l'environnement hostile » de la solution.

Serveur monétique ou serveur de gestion : équipement informatique chargé de la gestion des demandes d'autorisation et de la gestion des données de transactions de paiement avant transmission à l'acquéreur. Cet équipement doit proposer des éléments de sécurité et d'assurance permettant de garantir la confidentialité et l'intégrité des données des transactions de paiement. Il doit être certifié PCI-DSS (*Payment Card Industry - Data Security Standard*).

Sécurisation de la solution : les protocoles de communication entre le terminal et le serveur monétique doivent garantir la confidentialité et l'intégrité des données des transactions de paiement circulant *via* des réseaux potentiellement ouverts (internet, GSM, etc.). La solution doit garantir une solution de chiffrement de bout en bout telle que P2PE (*point-to-point encryption*).

œuvre de mesures visant à confiner le rôle du smartphone dans le dispositif à celui de machine de caisse et de modem de communication, en ne lui permettant pas d'accéder aux données élémentaires de la transaction.

• Les protocoles de communication entre les différents appareils physiques doivent viser à assurer de façon continue la confidentialité et l'intégrité des données des transactions de bout en bout, ce qui nécessite la mise en œuvre de mécanismes de chiffrement entre le module de lecture de carte et le serveur de gestion. De ce fait, les données échangées ne peuvent être exploitées par un tiers car elles circulent chiffrées lors de leur transfert *via* le smartphone et les réseaux de télécommunication publics.

• Le smartphone ne doit disposer d'aucune fonction permettant de piloter le fonctionnement interne du module autre que celles prévues pour l'acceptation de paiements par carte, afin d'éviter tout risque de manipulation de ce dernier par une application malveillante. Cette condition est nécessaire pour assurer la résistance du dispositif face à des menaces dues à un *malware* sur le smartphone, qui pourrait tenter par exemple de :

- générer des transactions frauduleuses ;
- voler des données liées à la carte de paiement ;
- modifier les données d'une transaction en cours,
- valider une transaction en contournant certaines étapes sécuritaires telles que l'authentification du porteur par exemple.

Pour se prémunir contre certains procédés visant notamment à récupérer les codes PIN, l'écran utilisé lors de la transaction doit être intégré à un environnement sécurisé, c'est pourquoi celui-ci doit être embarqué dans le module de lecture de carte.

Par ailleurs, le recours à un serveur de gestion permet à ces solutions de ne pas être contraintes d'éditer des tickets papier à destination de l'accepteur, puisque ce dernier peut accéder à ses tickets dématérialisés à partir des données stockées, ce qui limite le risque de compromission des données qui y figurent.

3.5 Conclusion et recommandations de l'Observatoire

Le développement de solutions d'acceptation des paiements au point de vente en situation de mobilité constitue une opportunité pour les acteurs du marché, et fait écho aux besoins exprimés dans le cadre de la Stratégie nationale des paiements.

L'Observatoire note l'émergence de deux grandes familles de solutions répondant à ce besoin : d'une part, le développement de terminaux de paiement autonomes semblables à ceux équipant les commerçants et disposant d'une connectivité aux réseaux de téléphonie mobile (GPRS, 3G ou 4G) ; et d'autre part, des dispositifs dits m-POS fondés sur l'appairage d'un boîtier de lecture de carte et d'un appareil mobile (smartphone, tablette, etc.) ce dernier assurant principalement le rôle de modem.

Afin que l'émergence de ces nouvelles solutions, d'ores et déjà commercialisées par certains acquéreurs, ne vienne pas affecter le haut niveau de sécurité proposé par les terminaux de paiement traditionnels, l'Observatoire souligne la

nécessité de mettre en œuvre des mesures de sécurité adaptées :

- concernant les terminaux dits autonomes : veiller au respect des principes de sécurité applicables aux terminaux de paiement de proximité tels que définis par l'Observatoire, notamment le respect des standards EMV et PCI-PTS permettant d'assurer la résilience des dispositifs à la fraude.

- Concernant les solutions de type m-POS : permettre à ces solutions d'évoluer dans un cadre sécuritaire équivalent à celui des terminaux autonomes. Le boîtier de lecture de la carte et de saisie du code confidentiel doit ainsi être soumis au respect des exigences applicables aux terminaux classiques (EMV, PCI-PTS et SRED) ; en outre, les protocoles de communication entre les différents composants de la solution doivent limiter au strict nécessaire la capacité d'accès de l'appareil mobile aux données de transaction. Sur ce second point, le cadre de référence doit s'attacher en particulier à préserver la sécurité et l'intégrité des données de bout en bout par des méthodes de chiffrement, en tenant compte des risques liés à la présence d'un composant non dédié au paiement – l'appareil mobile chargé d'assurer la fonction de modem – dans le traitement de la transaction.

À cet effet, l'Observatoire invite les acteurs du marché à appliquer les procédures d'agrément mises en place pour ces solutions, et permettant d'assurer le respect de ces exigences.

L'Observatoire rappelle que les conseils de prudence à l'usage des porteurs restent pleinement applicables dans le cas d'un paiement sur un terminal mobile. Compte tenu de la multiplication des solutions d'acceptation, l'Observatoire invite les porteurs à être attentifs lors du paiement sur des terminaux inhabituels :

- En France et en Europe, le recours à la piste magnétique des cartes n'est toléré que sur dérogation et dans des environnements de paiement spécifiques. Si la carte de paiement est équipée d'une puce EMV, les seuls modes de paiement autorisés sont soit par lecture de la puce (auquel cas la carte doit être insérée de façon statique dans le terminal au moment de la saisie du code confidentiel), soit en mode sans contact (carte posée contre le lecteur NFC du terminal).

- Il est recommandé de demander au commerçant le ticket-client attestant du paiement, de s'assurer de l'avoir bien reçu (notamment dans le cas d'un ticket dématérialisé envoyé par SMS ou email) et de le conserver comme justificatif, en vue de vérifier la bonne imputation de la dépense sur le relevé de compte du titulaire de la carte.

Enfin, l'Observatoire souligne le caractère innovant de l'industrie du m-POS, et restera par conséquent attentif à l'émergence de nouvelles catégories de solutions, qui pourraient l'amener à actualiser les recommandations présentement émises.

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, 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…) ;

- 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 fraude 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…).

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, même pas 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…), 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…).

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 vérifier 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 sur les 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…), 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 courrier électronique, 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…) 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-mêmes 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 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…) à un tiers qui vous parait douteux.

- En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 150 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, courrier électronique 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 13 mois à compter de la date de débit de l'opération contestée (délai fixé par la loi), vous déposez une réclamation auprès de votre établissement teneur de compte, les sommes contestées doivent vous être immédiatement remboursées 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). Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l'opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir néanmoins dépasser 120 jours.

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 directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 1er novembre 2009, a modifié les règles relatives à la responsabilité du payeur en cas d'opération de paiement non autorisée.

La charge de la preuve incombe au prestataire de services de paiement. Ainsi, lorsqu'un client nie avoir autorisé une opération, il incombe à son prestataire de services de paiement de prouver que l'opération 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 prestataire de services de paiement 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.

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 afin de déterminer l'étendue de la responsabilité du payeur.

Opérations nationales ou intracommunautaires

Ces dispositions de protection du payeur couvrent :

- les opérations effectuées en euros ou en francs CFP sur le territoire de la République française [1],

- les opérations intracommunautaires dans lesquelles le prestataire de service de paiement du bénéficiaire et celui du payeur sont situés :

  – l'un sur le territoire de la France métropolitaine, dans les départements d'outre-mer, à Saint-Martin ou à Saint-Barthélemy ;
  – l'autre dans un autre État partie à l'accord sur l'Espace économique européen [2],

et réalisées en euros ou dans la devise nationale de l'un de ces États.

1 L'ordonnance d'extension à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna des dispositions de l'ordonnance de transposition est entrée en vigueur le 8 juillet 2010.

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

Concernant les opérations 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 devra contester, auprès de son prestataire de services de paiement et dans un délai de 13 mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son prestataire devra alors rembourser immédiatement l'opération non autorisée au payeur et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Une indemnisation complémentaire pourra aussi éventuellement être versée. Nonobstant l'extension du délai maximal de contestation à 13 mois, le porteur devra, 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 prestataire de services de paiement.

Une dérogation à ces règles de remboursement est cependant prévue pour les opérations de paiement réalisées en utilisant un dispositif de sécurité personnalisé, par exemple la frappe d'un code secret ou l'utilisation d'un code non rejouable pour initier un virement en ligne.

Avant information aux fins de blocage de l'instrument de paiement

Avant l'information aux fins de blocage de l'instrument, le payeur pourra supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de l'instrument de paiement si l'opération est effectuée avec l'utilisation du dispositif personnalisé de sécurité. En revanche, si l'opération est effectuée sans l'utilisation du dispositif personnalisé de sécurité, le payeur ne voit pas sa responsabilité engagée.

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 elle 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, convenues avec son prestataire de services de paiement.

Enfin, si le prestataire de services de paiement 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 prestataire, 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 prestataire de services de paiement 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 prestataire de services de paiement de la perte, du vol, du détournement ou de la contrefaçon de l'instrument de paiement, ce dernier lui fournit sur demande et pendant 18 mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

Opérations extra-européennes

La directive sur les services de paiement n'est applicable qu'aux opérations intracommunautaires. Cependant la législation française existant avant l'adoption de cette directive protégeait les titulaires de cartes sans distinction de la localisation du bénéficiaire de l'opération non autorisée. Il a été décidé de maintenir une protection équivalente à celle à laquelle le client avait droit auparavant. À cette fin, les règles applicables aux opérations nationales ou intracommunautaires sont applicables avec des adaptations.

Ainsi, les opérations de paiement concernées par ces adaptations sont les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer [3], à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un État non européen [4], quelle que soit la devise dans laquelle l'opération est réalisée. Sont également concernées les opérations effectuées avec une carte dont l'émetteur est situé à Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française ou à Wallis et Futuna, au profit d'un bénéficiaire dont le prestataire est situé dans un État autre que la République française, quelle que soit la devise utilisée.

3 Y compris Mayotte depuis le 31 mars 2011.

4 Qui n'est pas partie à l'accord sur l'Espace économique européen.

Dans ces cas, le plafond de 150 euros trouve à s'appliquer pour les opérations non autorisées en cas de perte ou de vol de la carte, même si l'opération a été réalisée sans utilisation du dispositif personnalisé de sécurité.

Par ailleurs, le délai maximal de contestation de l'opération est ramené à 70 jours et peut être conventionnellement étendu à 120 jours. Le remboursement d'une opération non autorisée doit toujours être immédiat.

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 R141-1, R141-2 et R142-22 à R142-27 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 L141-4 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 L311-3 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 L141-4 et R141-1 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 R141-2 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 R142-22 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 R142-23 et suivants du *Code monétaire et financier*, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté un règlement intérieur qui précise les conditions de son fonctionnement.

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

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

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat sont tenus au secret professionnel par l'article R142-25 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 R142-22 du *Code monétaire et financier*, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre de l'Économie et des Finances. Le dernier arrêté de nomination date du 16 juin 2017.

Président
François VILLEROY de GALHAU
Gouverneur de la Banque de France

Représentants des assemblées

Sénat
Assemblée nationale

Représentant du secrétaire général de l'Autorité de contrôle prudentiel et de résolution

Edouard FERNANDEZ-BOLLO
Secrétariat général

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

Sur proposition du ministre de l'Économie et des Finances :

- Le haut fonctionnaire de défense et de sécurité ou son représentant :
  Christian DUFOUR

- Le directeur général du Trésor ou son représentant :
  Odile RENAUD-BASSO
  Isabelle BUI

- Le directeur général des Entreprises ou son représentant :
  Pascal FAURE
  Loïc DUFLOT

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

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

- Le directeur des Affaires criminelles et des Grâces ou son représentant :
  Nicolas BARRET

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

- Le directeur général de la gendarmerie nationale ou son représentant :
  Nicolas DUVINAGE

Sur proposition de la Commission nationale de l'Informatique et des Libertés

- Le chef du service des affaires économiques
  Clémence SCOTTEZ

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
Responsable communication
et relations institutionnelles
Association française
du multimédia mobile (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
Directeur général
American Express France (AMEX)

Solveig HONORE-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

Gérard NEBOUY
Directeur régional
Visa Europe France

Jérôme RAGUENES
Directeur - Systèmes et Moyens de paiement
Fédération bancaire française (FBF)

Caroline SELLIER
Directeur - *Risk management* et lutte
contre la fraude
Natixis Payment Solutions

Jean-Marie VALLEE
Directeur général
STET

Narinda YOU
Directeur - Stratégie et relations de place
Crédit Agricole

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)

Robin MATHIEU
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 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)

Christophe LESOBRE
Président de la Commission monétique
et moyens de paiement
Association française
des trésoriers d'entreprises (AFTE)

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 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 Dossier statistique

Vue d'ensemble

T1 Cartographie des moyens de paiement en 2016

(variation en pourcentage)

Paiements scripturaux	Nombre de transactions (en millions)		Montants des transactions (en Md€)		Montants moyens en €
	2016	Variation 2016/2015	2016	Variation 2016/2015	
Paiement carte (*)	11 134	+ 10	499	+ 8	45
Prélèvements	3 963	+ 2	1 492	+ 3	377
Virement	3 753	+ 4	23 697	+ 3	6 314
Chèque	2 137	- 8	1 077	- 8	504
LCR BOR	82	- 3	266	- 9	3 236
Monnaie Électronique	38	+ 5	1	+ 47	16
Total	**21 107**	**+ 5**	**27 032**	**+ 3**	**1 281**
Retrait carte (*)	1 491	- 2	129	+ 1	87
Total transactions	**22 598**	**+ 5**	**27 161**	**+ 3**	**1 202**

(*) cartes émises en France uniquement

T2 Répartition de la fraude sur les moyens de paiement en montant et en volume en 2016

(part en pourcentage)

	Montant		Volume		Montant moyen en €
	2016 (en €)	Part en montant	2016 (en unités)	Part en volume	
Paiement Carte (*)	350 694 173	44	4 675 093	93	75
Chèque	271 706 352	34	118 299	2	2 296
Virement	86 284 101	11	5 585	0	12 226
Prélèvements	39 935 882	5	1 176	0	33 959
LCR-BOR	1 018 149	0	4	0	254 537
Total Paiements	**749 638 657**	**94**	**4 800 157**	**96**	**156**
Retrait carte (*)	48 384 911	6	201 193	4	240
Total transactions	**798 023 568**	**100**	**5 001 350**	**100**	**159**

(*) cartes émises en France uniquement

Statistiques de fraude sur les cartes de paiement

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

- des 120 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 2016, le nombre de cartes en circulation s'élève à 84,3 millions dont :

- 73,4 millions de cartes de type « interbancaire »(« CB », MasterCard, Visa) ;
- 10,9 millions de cartes de type « privatif ».

Le nombre de cartes [1] mises en opposition en 2016 est d'environ 1 138 000.

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 et 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	9 528,76	381,65	224,79	12,02	46,11	3,84
Paiements à distance hors Internet	32,00	2,88	25,30	1,34	1,65	0,29
Paiements à distance sur Internet	918,02	67,92	198,30	11,76	19,39	1,29
Retraits	1 432,56	122,07	35,54	3,95	20,34	3,03
Total	**11 911,34**	**574,53**	**483,94**	**29,07**	**87,49**	**8,45**
Cartes de type « privatif »						
Paiements de proximité et sur automate	80,02	7,41	3,79	0,68	4,98	0,81
Paiements à distance hors Internet	29,94	4,52	6,09	0,38	0,55	0,13
Paiements à distance sur Internet	10,15	1,37	3,41	0,60	0,89	0,16
Retraits	2,68	0,24	0,00	0,00	0,00	0,00
Total	**122,78**	**13,53**	**13,30**	**1,66**	**6,42**	**1,09**
Total général	**12 034,13**	**588,06**	**497,23**	**30,74**	**93,91**	**9,55**

Source : Observatoire de la sécurité des moyens de paiement.

T4 Le marché des cartes de paiement en France - Acceptation

(volume en millions et 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	9 528,76	381,65	239,96	14,20	61,86	6,39
Paiements à distance hors Internet	32,00	2,88	9,66	1,55	3,89	1,02
Paiements à distance sur Internet	918,02	67,92	64,74	6,94	17,71	2,95
Retraits	1 432,56	122,07	23,33	3,81	6,92	1,68
Total	**11 911,34**	**574,53**	**337,69**	**26,50**	**90,38**	**12,04**
Cartes de type « privatif »						
Paiements de proximité et sur automate	80,02	7,41	6,09	0,89	8,13	3,32
Paiements à distance hors Internet	29,94	4,52	3,23	0,70	1,16	0,59
Paiements à distance sur Internet	10,15	1,37	2,01	0,26	0,77	0,17
Retraits	2,68	0,24	0,00	0,00	0,68	0,29
Total	**122,78**	**13,53**	**11,34**	**1,85**	**10,74**	**4,38**
Total général	**12 034,13**	**588,06**	**349,03**	**28,34**	**101,12**	**16,42**

Source : Observatoire de la sécurité des moyens de paiement.

T5 Répartition de la fraude par type de carte

(montant de la fraude en millions d'euros)

	Taux de fraude				
	2012	2013	2014	2015	2016
Cartes de type « interbancaire »	0,080 % (434,4)	0,080 % (455,8)	0,080 % (486,4)	0,083 % (507,2)	0,077 % (504,0)
Cartes de type « privatif »	0,076 % (16,3)	0,065 % (14,0)	0,062 % (14,2)	0,068 % (15,5)	0,060 % (13,5)
Total	**0,080 % (450,7)**	**0,080 % (469,9)**	**0,080 % (500,6)**	**0,082 % (522,7)**	**0,077 % (517,5)**

Source : Observatoire de la sécurité des moyens de paiement.

T6 Répartition de la fraude par zone géographique

(montant de la fraude en millions d'euros)

	Taux de fraude				
	2012	2013	2014	2015	2016
Transactions nationales	0,045 % (226,4)	0,046 % (238,6)	0,043 % (234,6)	0,040 % (225,0)	0,037 % (217,2)
Transactions internationales	0,380 % (224,3)	0,350 % (231,3)	0,316 % (266,0)	0,372 % (297,9)	0,353 % (300,3)
dont carte française et accepteur hors SEPA	*0,759 % (62,5)*	*0,688 % (70,2)*	*0,636 % (70,0)*	*0,692 % (74,5)*	*0,713 % (68,0)*
dont carte française et accepteur SEPA	*0,316 % (56,3)*	*0,366 % (67,9)*	*0,374 % (91,0)*	*0,459 % (116,8)*	*0,370 % (113,9)*
dont carte étrangère hors SEPA et accepteur français	*0,639 % (78,2)*	*0,404 % (64,1)*	*0,336 % (65,6)*	*0,353 % (69,7)*	*0,449 % (73,7)*
dont carte étrangère SEPA et accepteur français	*0,132 % (27,3)*	*0,135 % (29,1)*	*0,134 % (39,3)*	*0,153 % (36,9)*	*0,158 % (44,7)*
Total	**0,080 % (450,7)**	**0,080 % (469,9)**	**0,080 % (500,6)**	**0,082 % (522,9)**	**0,077 % (517,5)**

Source : Observatoire de la sécurité des moyens de paiement.

T7 Répartition de la fraude nationale par type de transaction

(montant de la fraude en millions d'euros)

	Taux de fraude				
	2012	2013	2014	2015	2016
Paiements	0,049 % (190,0)	0,050 % (199,9)	0,046 % (193,2)	0,043 % (185,1)	0,039 % (181,5)
dont paiements de proximité et sur automate	*0,015 % (51,2)*	*0,013 % (45,8)*	*0,010 % (37,1)*	*0,009 % (34,7)*	*0,008 % (29,2)*
dont paiements à distance	*0,299 % (138,8)*	*0,269 % (154,2)*	*0,248 % (156,0)*	*0,228 % (150,4)*	*0,199 % (152,3)*
dont par courrier / téléphone	*0,338 % (29,4)*	*1,122 % (29,2)*	*0,147 % (2,8 [2])*	*0,208 % (5,1)*	*0,079 % (5,8)*
dont sur Internet	*0,290 % (109,4)*	*0,229 % (125,0)*	*0,251 % (153,2 [3])*	*0,229 % (145,3)*	*0,211 % (146,5)*
Retraits	0,031 % (36,4)	0,033 % (38,6)	0,034 % (41,5)	0,033 % (39,9)	0,029 % (35,7)
Total	**0,045 % (226,4)**	**0,046 % (238,6)**	**0,043 % (234,6)**	**0,040 % (225,0)**	**0,037 % (217,2)**

2) 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.
3) Voir note précédente.
Source : Observatoire de la sécurité des moyens de paiement

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

(montant de la fraude en millions d'euros)

	Taux de fraude			
	2013	2014	2015	2016
Carte française – Accepteur étranger hors SEPA				
Paiements	0,547 % (40,3)	0,532 % (41,7)	0,735 % (56,3)	0,862 % (56,2)
dont paiements de proximité et sur automate	*0,377 % (17,7)*	*0,350 % (19,2)*	*0,509 % (25,8)*	*0,494 % (23,0)*
dont paiements à distance	*0,848 % (22,6)*	*0,960 % (22,5)*	*1,174 % (30,5)*	*1,781 % (33,3)*
– par courrier / téléphone	*1,234 % (6,4)*	*4,955 % (7,5)*	*2,345 % (9,5)*	*2,239 % (9,4)*
– sur Internet	*0,755 % (16,2)*	*0,682 % (14,9)*	*0,959 % (21,1)*	*1,648 % (23,9)*
Retraits	1,054 % (29,9)	0,890 % (28,3)	0,586 % (18,1)	0,390 % (11,8)
Total	**0,688 % (70,2)**	**0,636 % (70,0)**	**0,692 % (74,5)**	**0,713 % (68,0)**
Carte française – Accepteur étranger SEPA				
Paiements	0,434 % (66,8)	0,434 % (89,8)	0,526 % (115,7)	0,422 % (112,9)
dont paiements de proximité et sur automate	*0,089 % (8,2)*	*0,067 % (7,8)*	*0,071 % (8,0)*	*0,066 % (8,4)*
dont paiements à distance	*0,937 % (58,6)*	*0,910 % (82,0)*	*1,004 % (107,7)*	*0,742 % (104,5)*
– par courrier / téléphone	*1,566 % (11,3)*	*1,317 % (13,9)*	*1,399 % (18,7)*	*1,142 % (19,7)*
– sur Internet	*0,856 % (47,3)*	*0,856 % (68,1)*	*0,948 % (89,0)*	*0,687 % (84,9)*
Retraits	0,036 % (1,1)	0,033 % (1,2)	0,033 % (1,1)	0,024 % (0,9)
Total	**0,366 % (67,9)**	**0,374 % (91,0)**	**0,459 % (116,8)**	**0,370 % (113,8)**

Source : Observatoire de la sécurité des moyens de paiement.

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

(montant de la fraude en millions d'euros)

	Taux de fraude			
	2013	2014	2015	2016
Carte étrangère hors SEPA – Accepteur français				
Paiements	0,451 % (63,2)	0,380 % (65,0)	0,391 % (68,1)	0,507 % (73,2)
dont paiements de proximité et sur automate	*0,230 % (25,3)*	*0,162 % (21,9)*	*0,168 % (22,8)*	*0,179 % (17,4)*
dont paiements à distance	*1,268 % (37,9)*	*1,213 % (43,1)*	*1,185 % (45,3)*	*1,179 % (55,8)*
– par courrier / téléphone	*0,930 % (9,2)*	*1,018 % (7,7)*	*1,159 % (10,8)*	*1,127 % (18,2)*
– sur Internet	*1,436 % (28,7)*	*1,265 % (35,4)*	*1,193 % (34,5)*	*1,206 % (37,7)*
Retraits	0,051 % (0,9)	0,026 % (0,6)	0,069 % (1,6)	0,024 % (0,5)
Total	**0,404 % (64,1)**	**0,336 % (65,6)**	**0,353 % (69,7)**	**0,449 % (73,7)**
Carte étrangère SEPA – Accepteur français				
Paiements	0,158 % (28,2)	0,156 % (38,5)	0,175 % (36,0)	0,178 % (43,8)
dont paiements de proximité et sur automate	*0,039 % (4,9)*	*0,026 % (5,1)*	*0,033 % (4,8)*	*0,025 % (3,7)*
dont paiements à distance	*0,458 % (23,2)*	*0,476 % (33,1)*	*0,528 % (31,3)*	*0,424 % (40,0)*
– par courrier / téléphone	*0,308 % (3,8)*	*0,397 % (4,8)*	*0,734 % (7,7)*	*0,490 % (11,0)*
– sur Internet	*0,506 % (19,4)*	*0,492 % (28,6)*	*0,484 % (23,6)*	*0,403 % (29,0)*
Retraits	0,025 % (0,9)	0,018 % (0,9)	0,025 % (0,9)	0,024 % (0,9)
Total	**0,135 % (29,1)**	**0,134 % (39,3)**	**0,153 % (36,9)**	**0,158 % (44,7)**

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 %)

2016	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	63,0	29,0	62,5	29,2	0,5	16,3
Carte non parvenue	0,8	0,4	0,6	0,3	0,2	7,0
Carte altérée ou contrefaite	0,4	0,2	0,3	0,1	0,0	1,5
Numéro usurpé	152,2	70,1	150,4	70,2	1,8	63,5
Autres	0,7	0,3	0,4	0,2	0,3	11,7
Total	**217,2**	**100,0**	**214,3**	**100,0**	**2,9**	**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	586,0	28 378,7	79,8	8 003,0	124,6	22 161,5
Cartes perdues ou volées	566,0	27 378,1	46,6	4 075,7	15,9	2 985,7
Cartes non parvenues	8,6	403,8	0,4	31,6	0,1	21,1
Cartes altérées ou contrefaites	10,3	299,1	10,6	1 698,5	88,4	16 320,0
Numéro de carte usurpé	0,1	10,8	13,4	1 696,7	14,5	2 121,3
Autres	1,2	286,8	5,7	500,6	5,8	713,5
Paiements à distance hors Internet	43,5	4 979,8	242,1	19 349,9	62,9	9 114,3
Cartes perdues ou volées	0,5	18,0	21,5	2 619,1	6,9	1 344,0
Cartes non parvenues	0,0	0,1	0,1	4,8	0,0	2,3
Cartes altérées ou contrefaites	0,0	1,0	5,0	398,4	2,5	400,7
Numéro de carte usurpé	42,9	4 955,1	214,9	16 285,3	52,5	7 313,1
Autres	0,1	5,6	0,6	42,2	1,0	54,1
Paiements à distance sur Internet	1 915,5	145 465,8	1 350,7	83 643,9	231,4	23 470,1
Cartes perdues ou volées	0,2	10,1	85,3	5 967,0	15,9	1 670,4
Cartes non parvenues	0,0	0,0	0,3	19,3	0,1	22,3
Cartes altérées ou contrefaites	0,0	2,0	20,7	1 532,3	6,1	639,3
Numéro de carte usurpé	1 915,3	145 442,3	1 242,5	75 983,5	208,6	21 069,5
Autres	0,1	11,6	1,9	141,7	0,8	68,5
Retraits	119,7	35 445,3	4,4	932,3	75,9	11 802,2
Cartes perdues ou volées	118,0	35 098,1	3,0	696,9	4,8	291,6
Cartes non parvenues	0,7	232,4	0,1	46,9	0,0	3,0
Cartes altérées ou contrefaites	0,0	12,6	0,9	132,9	48,1	11 165,9
Numéro de carte usurpé	0,0	0,9	0,1	10,0	8,5	140,8
Autres	0,9	101,3	0,3	45,6	0,9	200,9
Total	**2 665,0**	**214 269,6**	**1 677,1**	**111 929,1**	**494,9**	**66 548,1**

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	586,0	28 378,7	26,8	3 499,7	77,4	14 912,1
Cartes perdues ou volées	566,0	27 378,1	12,3	1 827,3	18,8	4 634,5
Cartes non parvenues	8,6	403,8	0,8	171,5	0,3	147,3
Cartes altérées ou contrefaites	10,3	299,1	7,3	432,6	48,9	7 754,2
Numéro de carte usurpé	0,1	10,8	5,8	937,8	8,5	1 763,4
Autres	1,2	286,8	0,6	130,6	0,9	612,7
Paiements à distance hors Internet	43,5	4 979,8	42,0	10 511,3	48,1	16 800,0
Cartes perdues ou volées	0,5	18,0	1,2	213,9	1,9	444,7
Cartes non parvenues	0,0	0,1	0,1	5,5	0,1	7,6
Cartes altérées ou contrefaites	0,0	1,0	1,5	492,2	3,4	1 284,5
Numéro de carte usurpé	42,9	4 955,1	39,1	9 764,1	42,3	14 869,5
Autres	0,1	5,6	0,2	35,6	0,4	193,7
Paiements à distance sur Internet	1 915,5	145 465,8	158,1	28 234,4	191,6	35 909,8
Cartes perdues ou volées	0,2	10,1	2,9	532,7	5,5	1 029,6
Cartes non parvenues	0,0	0,0	0,1	18,5	0,1	19,4
Cartes altérées ou contrefaites	0,0	2,0	2,4	403,6	13,4	2 322,4
Numéro de carte usurpé	1 915,3	145 442,3	151,6	27 078,3	171,3	35 056,9
Autres	0,1	11,6	1,1	201,3	1,4	481,5
Retraits	119,7	35 445,3	3,9	918,7	1,7	450,3
Cartes perdues ou volées	118,0	35 098,1	3,4	822,1	0,8	231,0
Cartes non parvenues	0,7	232,4	0,0	11,7	0,0	8,9
Cartes altérées ou contrefaites	0,0	12,6	0,2	46,0	0,8	190,1
Numéro de carte usurpé	0,0	0,9	0,1	25,1	0,1	16,7
Autres	0,9	101,3	0,1	13,7	0,0	3,6
Total	**2 665,0**	**214 269,6**	**230,8**	**43 164,0**	**318,8**	**68 072,2**

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	2,63	855,95	0,85	418,76	3,70	801,00
Cartes perdues ou volées	0,75	272,75	0,11	80,64	0,33	128,21
Cartes non parvenues	0,47	159,22	0,05	16,47	0,02	1,74
Cartes altérées ou contrefaites	0,14	23,85	0,15	84,02	2,20	364,38
Numéro de carte usurpé	0,44	200,23	0,49	218,32	1,15	305,87
Autres	0,84	199,89	0,05	19,31	0,01	0,80
Paiements à distance hors Internet	2,98	849,91	4,70	300,49	1,78	269,82
Cartes perdues ou volées	0,08	6,86	0,49	2,30	0,02	6,66
Cartes non parvenues	0,02	6,63	0,06	0,84	0,01	1,97
Cartes altérées ou contrefaites	0,06	13,26	0,13	11,15	0,06	40,20
Numéro de carte usurpé	2,75	766,49	4,00	281,10	1,70	220,51
Autres	0,07	56,66	0,02	5,10	0,00	0,48
Paiements à distance sur Internet	2,80	984,49	16,04	1 232,32	2,65	414,48
Cartes perdues ou volées	0,14	24,81	0,14	3,20	0,04	3,22
Cartes non parvenues	0,02	2,09	0,01	0,04	0,00	0,20
Cartes altérées ou contrefaites	0,02	5,15	0,07	16,44	0,05	14,87
Numéro de carte usurpé	2,52	871,05	15,67	1 182,28	2,55	391,22
Autres	0,11	81,39	0,16	30,36	0,01	4,97
Retraits	1,25	205,13				
Cartes perdues ou volées	1,05	168,96				
Cartes non parvenues	0,19	33,46				
Cartes altérées ou contrefaites	0,00	0,00				
Numéro de carte usurpé	0,00	2,26				
Autres	0,01	0,44				
Total	**9,65**	**2 895,47**	**21,59**	**1 951,57**	**8,12**	**1 485,30**

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	2,63	855,95	0,99	248,34	3,90	2 473,08
Cartes perdues ou volées	0,75	272,75	0,16	45,13	0,65	388,49
Cartes non parvenues	0,47	159,22	0,39	38,69	0,02	5,33
Cartes altérées ou contrefaites	0,14	23,85	0,16	81,00	2,70	1 551,92
Numéro de carte usurpé	0,44	200,23	0,12	49,80	0,28	119,76
Autres	0,84	199,89	0,16	33,72	0,24	407,58
Paiements à distance hors Internet	2,98	849,91	1,27	530,04	3,15	1 358,85
Cartes perdues ou volées	0,08	6,86	0,01	14,21	0,11	38,41
Cartes non parvenues	0,02	6,63	0,00	0,86	0,11	21,82
Cartes altérées ou contrefaites	0,06	13,26	0,04	21,51	0,41	111,55
Numéro de carte usurpé	2,75	766,49	1,21	482,47	2,45	1 543,20
Autres	0,07	56,66	0,01	0,99	0,07	49,77
Paiements à distance sur Internet	2,80	984,49	2,45	749,73	7,42	1 758,76
Cartes perdues ou volées	0,14	24,81	0,01	1,67	0,23	47,29
Cartes non parvenues	0,02	2,09	0,01	3,36	0,18	24,35
Cartes altérées ou contrefaites	0,02	5,15	0,11	24,98	0,47	94,16
Numéro de carte usurpé	2,52	871,05	2,26	671,14	6,43	1 543,20
Autres	0,11	81,39	0,07	48,57	0,13	49,77
Retraits	1,25	205,13			0,11	33,12
Cartes perdues ou volées	1,05	168,96			0,09	27,40
Cartes non parvenues	0,19	33,46			0,00	0,00
Cartes altérées ou contrefaites	0,00	0,00			0,00	0,00
Numéro de carte usurpé	0,00	2,26			0,00	0,00
Autres	0,01	0,44			0,02	5,72
Total	**9,65**	**2 895,47**	**4,71**	**1 528,11**	**14,59**	**5 623,81**

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

(valeur en euros, part en %)

	Montant	
	Valeur	Part
France	25 671 275	29,7
SEPA hors France	46 943 345	54,4
Hors SEPA	13 744 853	15,9
Total	**86 359 473**	**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

(valeur en euros, part en %)

	Montant	
	Valeur	Part
France	39 930 322	99,99
SEPA hors France	5 560	0,01
Total	**39 935 882**	**100**

Source : Observatoire de la sécurité des moyens de paiement.

Statistiques de fraude sur le chèque

T17 Répartition par typologie de fraude en 2016

(montant en euros, part en % et volume en unité)

	Montant		Volume	Montant
	Valeur	Part		
Détournement, rejeu	5 010 202	1,8	1 996	2 510
Vol, perte (faux, apocryphe)	123 537 940	44,7	96 112	1 285
Contrefaçon	32 418 849	11,7	6 444	5 030
Falsification	115 749 563	41,8	15 743	7 352
Total	**276 716 554**	**100**	120295	2 300

Source : Observatoire de la sécurité des moyens de paiement.

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

Directeur de la publication
Denis Beau,
Directeur général de la Stabilité financière
et des Opérations de marché
Banque de France

Rédacteur en chef
Emmanuelle Assouan,
Directeur des Systèmes de paiement
et Infrastructures de marché
Banque de France

Secrétariat de rédaction
Véronique Bugaj, Guylène Chotard,
Christine Collomb-Jost, Bernard Darrius,
Florian Dintilhac, Christelle Guiheneuc, Julien Lasalle,
Antoine Lhuissier, Lucas Nozahic, Eloïse Senkur,
Alexandre Stervinou, Mathieu Vileyn

Réalisation
Direction de la Communication
de la Banque de France

Opérateurs PAO
Studio Création
Direction de la Communication
de la Banque de France

Version papier
Observatoire de la sécurité des moyens de paiement
011-2323
Téléphone : +1 42 92 96 13
Télécopie : +1 42 92 31 74

Impression
Banque de France

Dépôt légal
Dès parution

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 l'Observatoire *(www.banque-france.fr).*

Une version imprimée peut être obtenue gratuitement, jusqu'à épuisement du stock, sur simple demande (cf. adresse ci-contre).

L'Observatoire de la sécurité des moyens de paiement se réserve le droit de suspendre le service de la diffusion et de restreindre le nombre de copies attribuées par personne.