2013

RAPPORT ANNUEL
DE L'OBSERVATOIRE DE LA SÉCURITÉ DES CARTES DE PAIEMENT

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

Observatoire
de la sécurité
des cartes de paiement

31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01
Code Courrier : 11-2323

Rapport annuel 2013
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Monsieur le ministre de l'Économie,
du Redressement productif et du Numérique
Monsieur le ministre des Finances et des Comptes publics
Monsieur le président du Sénat
Monsieur le président de l'Assemblée nationale

par

Christian Noyer,
gouverneur de la Banque de France,
président de l'Observatoire de la sécurité des cartes de paiement

L'Observatoire de la sécurité des cartes de paiement, mentionné au I de l'article L141-4 du Code monétaire et financier*, a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des systèmes de paiement par carte.*

Conformément à l'alinéa 6 de cet article, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'économie et au ministre chargé des finances et transmis au Parlement.

NB : Pour ses travaux, l'Observatoire distingue les systèmes de paiement par carte de type « interbancaire » et ceux de type « privatif ». Les premiers correspondent à ceux dans lesquels il existe un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs. Les seconds correspondent à ceux dans lesquels il existe un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs.

Sommaire

Le onzième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2013, comprend cette année quatre parties dont les principales conclusions sont reprises ci-après.

1re partie : état des lieux de la sécurisation des paiements par carte sur Internet

La baisse très prononcée en 2013 du taux de fraude sur les paiements par carte sur Internet montre les importants progrès de sécurisation qui ont lieu dans ce domaine.

La quasi-totalité des porteurs dispose aujourd'hui de cartes équipées de dispositifs d'authentification renforcée.

Parallèlement, le taux d'échec sur les transactions authentifiées connaît une baisse significative, et atteint un niveau similaire à celui du taux d'échec des transactions non authentifiées.

Ceci constitue un signal très positif pour les commerçants et montre que la mise en œuvre de l'authentification renforcée ne constitue plus un obstacle au développement du commerce électronique.

Ces évolutions encourageantes restent toutefois encore limitées par le faible taux de commerçants en ligne équipés de dispositifs d'authentification renforcée, qui atteint seulement 43 %.

Dans ce contexte, l'Observatoire appelle l'ensemble des acteurs concernés à généraliser au plus vite ces dispositifs d'authentification renforcée d'ici au 1er février 2015, date de la mise en œuvre des recommandations relatives à la sécurité des paiements sur Internet émises par le forum européen sur la sécurité des moyens de paiement « SecuRe Pay *».*

2e partie : statistiques de fraude pour l'année 2013

Le taux de fraude sur les paiements et les retraits par carte reste en 2013 stable à 0,080 %.

Cette stabilisation du taux de fraude recouvre toutefois plusieurs dynamiques différentes :

- *une hausse contenue de la fraude sur les transactions nationales, qui se caractérise par la diminution simultanée des taux de fraude sur les paiements de proximité et sur les paiements à distance. Pour la deuxième année consécutive, le taux de fraude sur les paiements par Internet continue de baisser, à 0,229 % (contre 0,290 % en 2012), bien qu'un tiers de cette baisse soit imputable à une révision de la méthodologie de collecte des données [1].*

1 Une modification de la méthodologie utilisée par le Groupement des Cartes Bancaires pour évaluer la répartition au sein des paiements à distance entre ceux effectués sur Internet et ceux réalisés par courrier ou téléphone a conduit à revoir à la baisse le montant de ces derniers et à en effectuer le report sur les paiements sur Internet. Ceci entraîne logiquement une baisse du taux de fraude sur ce dernier canal, le montant de l'activité totale augmentant.

Toutefois, les montants concernés par la fraude sur les paiements à distance, notamment sur les paiements par Internet, continuent d'augmenter. Les paiements à distance représentent toujours la majeure partie de la fraude en montant (64,6 %) alors qu'ils ne représentent que 11 % du montant total des paiements. Dans ce contexte, l'Observatoire appelle l'ensemble des acteurs à poursuivre leurs efforts pour mieux sécuriser ces paiements, et renouvelle ses recommandations à destination des commerçants en ligne afin que tous adoptent au plus vite des dispositifs d'authentification renforcée pour les transactions les plus risquées.

- *une baisse prononcée du taux de fraude sur les transactions internationales, qui masque toutefois des tendances contrastées.*

  Ainsi, le taux de fraude sur les paiements en France impliquant des cartes émises hors zone SEPA a connu une chute importante depuis 2012, grâce notamment à l'adoption du standard EMV par un nombre croissant de pays à l'exception notable des États-Unis. C'est cette même raison qui explique la baisse régulière depuis 2011 des taux de fraude sur les paiements de proximité au sein de la zone SEPA.

  À l'inverse, le taux de fraude sur les paiements à distance impliquant des cartes françaises dans la zone SEPA a crû de manière significative. La mise en œuvre au plus tard le 1er février 2015 des recommandations relatives à la sécurité des paiements sur Internet émises par le forum européen sur la sécurité des moyens de paiement « SecuRe Pay *» devrait permettre de lutter plus efficacement contre la fraude sur les paiements à distance dans la zone SEPA.*

3e partie : travaux de veille technologique autour de la sécurité des terminaux de paiement et des techniques d'authentification renforcée par porteur

Sécurité des terminaux de paiement *: le nombre de cas de compromission de terminaux de paiement ayant fortement augmenté au cours des deux dernières années, l'Observatoire a souhaité faire un état des lieux de la mise en œuvre des recommandations qu'il avait formulées précédemment sur la sécurité des terminaux de paiement et actualiser ses analyses au regard de l'évolution des techniques de fraude telles que présentées dans son rapport 2012.*

À la lumière de la tendance haussière des attaques visant les terminaux de paiement, l'Observatoire appelle l'ensemble des acteurs à une vigilance accrue. Il recommande plus particulièrement que les processus d'agrément des dispositifs d'acceptation par les systèmes de paiement par carte soient renforcés afin de mieux gérer les terminaux défaillants ou en fin de vie. L'Observatoire souligne également que les efforts engagés pour disposer d'une meilleure traçabilité des équipements doivent se poursuivre et aboutir dans les meilleurs délais.

Techniques d'authentification renforcée du porteur *: le secteur de vente à distance continuant à être particulièrement exposé à la fraude, l'Observatoire a souhaité faire un état des lieux des techniques d'authentification renforcée mises en œuvre par les systèmes de paiement par carte et les émetteurs français.*

Constatant que l'envoi d'un code non rejouable par SMS sur un téléphone mobile ou smartphone *est actuellement la solution la plus utilisée en France, l'Observatoire appelle à la poursuite*

des efforts de sécurisation des téléphones mobiles en tant que support d'authentification non rejouable. Il relève cependant que l'essor du paiement en ligne effectué depuis un téléphone mobile pourrait soutenir le développement d'autres solutions, l'envoi d'un SMS apparaissant dans ce contexte peu ergonomique. Il s'agirait notamment des portefeuilles électroniques dont le niveau de sécurité a fait l'objet de recommandations par l'Observatoire en 2011 et plus récemment par le forum européen « SecuRe Pay *».*

Enfin, l'Observatoire note que les récentes évolutions technologiques visant à intégrer des dispositifs biométriques sur les smartphones *pourraient à l'avenir jouer un rôle dans la sécurisation des paiements mobiles, dans la mesure où les dispositifs d'authentification retenus s'avéreraient particulièrement robustes d'un point de vue sécuritaire et ne pourraient être aisément contournés par l'exploitation de failles de sécurité du dispositif biométrique ou des composants périphériques qui lui sont attachés. La mise en place de processus d'évaluation et de certification sécuritaires de ces éléments pourrait œuvrer en ce sens.*

4e partie : protection des données personnelles dans le cadre des traitements de lutte contre la fraude

Dans un contexte d'évolution rapide des technologies relatives à la lutte contre la fraude à distance, l'Observatoire a souhaité comprendre les conséquences de la réglementation applicable en matière de traitement de données à caractère personnel dans le cadre de la lutte contre la fraude.

En l'absence d'un équivalent au standard EMV pour protéger les paiements par carte à distance, les dispositifs de lutte contre la fraude ont élargi le nombre et la nature de données à caractère personnel collectées lors d'un paiement par carte sur Internet afin d'augmenter le degré de certitude quant à la personne initiant une transaction de paiement. Si cette évolution a permis la mise en place de traitements de lutte contre la fraude plus élaborés et efficaces, elle pose la question du risque d'atteinte à la vie privée. C'est la raison pour laquelle ces nouveaux traitements font l'objet d'un contrôle de la CNIL conformément à la loi « Informatique et libertés ».

La CNIL a récemment engagé des travaux en vue de simplifier les formalités déclaratives relatives aux traitements de lutte contre la fraude utilisant des données à caractère personnel. Ces travaux seront ainsi l'occasion de prendre en compte le besoin de clarifier la responsabilité des acteurs ayant recours à des prestataires externalisés, celui de l'éventuelle mutualisation des données de fraude entre les acteurs afin de gagner en efficacité, la possibilité le cas échéant d'avoir recours à de nouvelles données d'identification issues des nouvelles technologies ou encore le besoin de clarifier les règles relatives à la durée de protection des données personnelles dans le cadre des traitements de lutte contre la fraude. Ils devraient déboucher sur l'adoption d'une autorisation dite unique qui permettra de mieux encadrer la collecte et le traitement des données afin que la lutte contre la fraude, qui correspond à un intérêt légitime des professionnels, soit proportionnée au respect des droits des personnes.

En vue de préserver cet équilibre, il convient de rappeler que le recours à des dispositifs permettant l'authentification renforcée du porteur au moment du paiement, dont notamment « 3D-Secure », peut être de nature à limiter le besoin de recourir à une collecte de données personnelles qui pourrait être jugée excessive.

État des lieux de la sécurisation des paiements par carte sur Internet

La fraude sur les paiements à distance et les moyens mis en œuvre par les acteurs de la chaîne de paiement afin de s'en prémunir, font l'objet d'un suivi régulier par l'Observatoire.

Parmi les mesures recommandées par ce dernier, la généralisation progressive de l'authentification renforcée du porteur par l'utilisation d'un code de validation non rejouable, à chaque fois que cela est possible et pertinent, occupe une place prépondérante.

Le présent chapitre rend compte du suivi de la mise en œuvre de cette recommandation (partie 1|) ainsi que les actions menées par l'Observatoire et la Banque de France pour sensibiliser les e-commerçants au renforcement de la sécurité des paiements sur Internet (partie 2|).

1| État d'avancement de la sécurisation des paiements par carte sur Internet

L'année 2013 a été marquée par une amélioration sensible de la sécurisation des paiements par carte sur Internet, puisque le taux de fraude sur ce canal a subi une diminution de 21 % [1] pour atteindre 0,229 % du montant des transactions (cf. le chapitre 2 du présent rapport). Si la baisse du taux de fraude, qui confirme le mouvement engagé en 2012, est encourageante, ce dernier demeure plus de vingt fois supérieur au taux de fraude constaté sur les paiements de proximité.

Dans ce contexte, la généralisation de l'authentification renforcée du porteur, à chaque fois que cela est possible et pertinent, reste une priorité de l'Observatoire. Il est à noter que cette priorité s'inscrit désormais dans un contexte européen puisque les recommandations du forum européen sur la sécurité des moyens de paiement *SecuRe Pay* [2] ont préconisé la généralisation de l'authentification renforcée pour les paiements par carte sur Internet les plus risqués d'ici le 1er février 2015.

Dans ce contexte, un suivi statistique semestriel du déploiement des solutions d'authentification est réalisé par l'Observatoire auprès des principaux établissements bancaires et de leurs prestataires techniques.

Ce suivi statistique, portant sur un périmètre de 57,3 millions de cartes de paiement et 34,3 milliards d'euros de paiements (dont 10,1 milliards sécurisés par le dispositif « 3D-Secure » [3]) permet de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification renforcée.

La septième campagne de collecte, qui portait sur la période 1er novembre 2013 au 30 avril 2014, met en évidence trois principaux enseignements.

1|1 La quasi-totalité des porteurs est désormais équipée d'au moins un dispositif d'authentification renforcée

En deux ans, le taux moyen de porteurs équipés d'au moins un dispositif d'authentification renforcée « opérationnel » a fortement progressé, passant de 77,0 % à 93,7 %, et s'est largement harmonisé entre les établissements sondés.

En considérant le périmètre des porteurs ayant effectivement réalisé une opération de paiement par Internet sur les six derniers mois, le taux est proche de 100 %.

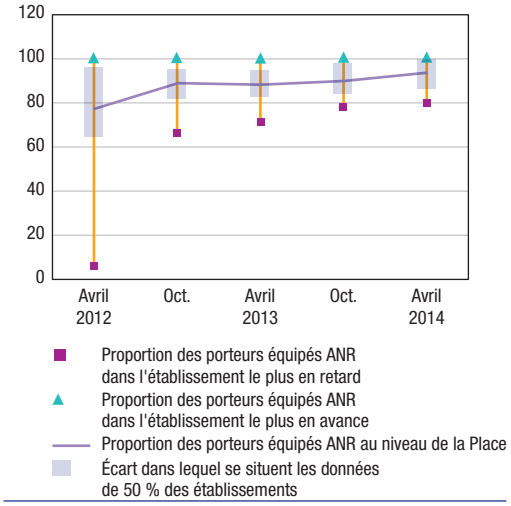
Parmi les dispositifs d'authentification proposés, le SMS [4] reste toujours largement majoritaire.

1 Une partie de cette baisse résulte cependant d'un changement de méthodologie de calcul (cf. chapitre 2 du présent rapport).
2 https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf
3 Protocole interbancaire de sécurisation des paiements par carte en ligne permettant l'authentification du porteur.
4 Cf. le chapitre 4 du présent rapport « étude sur les dispositifs d'authentification renforcée ».

Graphique 1

Distribution des porteurs équipés ANR (authentification non rejouable)

(en %)

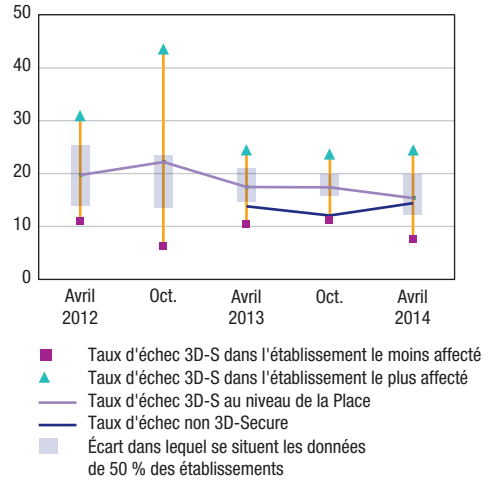


Source : Observatoire de la sécurité des cartes de paiement

Graphique 2

Distribution du taux d'échec « 3D-Secure » (3D-S)

(en %)



Source : Observatoire de la sécurité des cartes de paiement

1|2 Le taux d'échec sur les transactions authentifiées de manière renforcée se rapproche du taux d'échec sur les transactions non sécurisées

L'Observatoire a pu constater l'évolution positive du taux d'échec [5] sur les paiements authentifiés au fil des collectes réalisées, passant de 18,0 % en 2011 à 15,3 % sur la dernière collecte.

De plus, les écarts constatés sur ce taux d'échec entre les établissements sondés s'est fortement réduit, témoignant d'une meilleure compréhension des dispositifs d'authentification renforcée par les porteurs permise notamment par la généralisation de « 3D-Secure » par de grands e-commerçants.

Ainsi, ce taux d'échec se rapproche désormais du taux d'échec sur les paiements non authentifiés, collecté pour la première année par l'Observatoire, et qui se situe à 14,3 %. **L'Observatoire observe ainsi que la mise en œuvre de l'authentification renforcée du porteur, à chaque fois que cela est possible et pertinent, ne constitue plus un obstacle au développement du commerce électronique.**

L'Observatoire restera toutefois attentif à l'évolution positive du taux d'échec, et poursuivra, notamment dans le cadre de son groupe de travail e-commerce, les actions engagées au regard de la sécurisation des paiements sur Internet.

1|3 La part des transactions authentifiées *via* « 3D-Secure » continue de progresser en valeur, mais le taux d'e-commerçants équipés reste stable

La part des transactions authentifiées progresse en valeur de 27,5 % à 29,7 % en montants sur un an. Cette évolution positive peut ainsi expliquer la diminution du taux de fraude sur Internet en 2013.

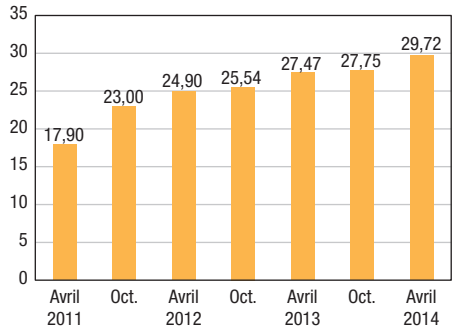
Pour autant, le taux de e-commerçants équipés en dispositif d'authentification renforcée reste pour sa part stable autour de 43 % ce qui peut

5 Sont inclus dans les motifs d'échec les abandons porteur (tous motifs confondus), les problèmes techniques (tous motifs confondus), les tentatives de fraude, les saisies erronées.

Graphique 3

Taux des paiements « 3D-Secure » (en valeur)

(en %)



Source : Observatoire de la sécurité des cartes de paiement

être considéré comme insuffisant au regard de la lutte contre la fraude.

2| Les actions menées par l'Observatoire et la Banque de France pour sensibiliser les e-commerçants au renforcement de la sécurité des paiements sur Internet

La Banque de France et le Groupement des Cartes Bancaires ont poursuivi les actions initiées en 2013, sous l'égide de l'Observatoire, notamment au travers de rencontres bilatérales avec les e-commerçants qui connaissent un montant et/ou un taux de fraude particulièrement élevé.

Cette démarche est destinée à sensibiliser les e-commerçants et leurs prestataires de services de paiement à la question de la fraude en vente à distance et à définir des plans d'action visant à diminuer le taux de fraude, notamment en déployant l'authentification renforcée du porteur pour les paiements les plus risqués.

Il ressort de ces rencontres les conclusions suivantes :

• Au-delà de son impact financier, la fraude aux paiements par Internet porte préjudice au développement du e-commerce dans son ensemble en raison d'une part, des répercussions en termes d'image et de confiance auprès des internautes et, d'autre part, de la crainte pour les professionnels de voir leur activité fragilisée en cas d'attaque organisée et de compromission massive de données de paiement. La lutte contre la fraude est ainsi considérée comme un enjeu stratégique.

• Les e-commerçants rencontrés et subissant un taux de fraude élevé se sont engagés à déployer la sécurisation des paiements par l'authentification renforcée des porteurs, *a minima* pour les transactions jugées les plus risquées. L'identification des transactions les plus risquées est le plus souvent rendue possible par l'utilisation d'outils dits de *« scoring »* [6] des transactions.

• Les e-commerçants ayant subi des pics de fraude importants ont reconnu l'efficacité de l'authentification renforcée des porteurs, notamment lorsque celle-ci est déclenchée sur la base d'une approche par les risques.

Les e-commerçants ont par ailleurs souligné trois pistes d'évolution qui permettraient de renforcer la lutte contre la fraude aux paiements par carte sur Internet.

• Les difficultés rencontrées dans la mise en œuvre de l'authentification renforcée *via* SMS sur les nouveaux canaux de vente comme le canal mobile *(smartphone)* rendent souhaitable l'émergence de nouvelles solutions d'authentification pouvant être déployées sur l'ensemble des canaux de vente. Dans l'attente de ces nouveaux dispositifs, les e-commerçants indiquent que les solutions de portefeuille électronique répondent, sous certaines conditions [7], au besoin de sécurisation du canal mobile.

• Le recours par les émetteurs à des modes d'authentification non renforcée (par exemple une authentification par mot de passe statique tel que la date de naissance), généralement pour des transactions de faible montant, peut être à l'origine de certaines fraudes. Bien que cette pratique préserve la garantie du paiement pour l'e-commerçant en cas de fraude, l'identification du type d'authentification

6 Cf. le chapitre 4 du présent rapport sur la protection des données personnelles dans le cadre des dispositifs de lutte contre la fraude.
7 Cf. chapitre 4 du rapport 2011 « portefeuille électronique et paiement par carte ».

dans les messages véhiculés au sein des systèmes de paiement permettrait cependant d'améliorer la fiabilité des systèmes d'analyse de transactions.

• Enfin, certains e-commerçants ont rappelé [8] la problématique rencontrée dans certains secteurs au regard des cartes prépayées anonymes et ont réitéré leur souhait de pouvoir les identifier afin de renforcer la vigilance sur ces dernières.

3| Conclusion

La dernière collecte statistique réalisée par l'Observatoire auprès des établissements bancaires et de leurs prestataires techniques montre **une baisse significative du taux de fraude sur les paiements par carte sur Internet, qui peut s'expliquer par la progression de la proportion en montant des paiements sécurisés par une authentification renforcée.**

Constatant d'une part que le taux d'échec sur les paiements authentifiés ne constitue plus un frein à la mise en œuvre de l'authentification renforcée et que d'autre part le taux de fraude sur les paiements par Internet demeure à un niveau près de vingt fois supérieur à celui des paiements de proximité, **l'Observatoire appelle l'ensemble des acteurs du paiement à poursuivre le renforcement de la sécurité des paiements par Internet.**

Avec seulement 43 % des sites e-commerce équipés, l'Observatoire considère que la généralisation des dispositifs d'authentification renforcée auprès des e-commerçants reste dans ce contexte une priorité qui s'inscrit désormais dans le cadre européen avec la mise en œuvre d'ici au 1er février 2015 des recommandations du forum européen sur la sécurité des moyens de paiement *SecuRe Pay* visant la généralisation de l'authentification renforcée du porteur pour les paiements sur Internet à chaque fois que cela est possible et pertinent.

8 Cf. chapitre 1 du rapport 2012 « État des lieux de la sécurisation des paiements par carte sur Internet ».

Statistiques de fraude pour 2013

Depuis 2003, l'Observatoire 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 définition et une typologie harmonisées, établies dès la première année de fonctionnement de l'Observatoire et reprises en annexe 6 du présent rapport. Une synthèse des statistiques pour 2013 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou de retrait) et l'origine de la fraude (carte perdue ou volée, carte non parvenue, carte altérée ou contrefaite, numéro de carte usurpé). En complément, une série d'indicateurs détaillés est présentée dans l'annexe 5 de ce rapport.

On notera également que la Banque centrale européenne a publié le 25 février 2014 le troisième rapport [1] de l'Eurosystème sur la fraude aux cartes de paiement au sein de l'Union européenne, couvrant les exercices 2008 à 2012.

Si, dans l'ensemble, les méthodologies retenues respectivement par l'Observatoire et par l'Eurosystème sont très proches l'une de l'autre, il importe tout de même de préciser, dans l'optique de l'examen

Encadré 1

Statistiques de fraude : 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 ».

Les statistiques calculées par l'Observatoire portent ainsi sur :

- *532,2 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 68,4 millions de cartes de type « interbancaire » émises en France (dont 1,87 million de porte-monnaie électroniques et 20,2 millions de cartes sans contact) ;*
- *17 milliards d'euros de transactions réalisées (principalement en France) avec 17,1 millions de cartes de type « privatif » émises en France ;*
- *37,3 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.*

Les données recueillies proviennent :

- *de 10 émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club, Franfinance, JCB et UnionPay International ;*
- *des 130 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 ;*
- *des émetteurs du porte-monnaie électronique Moneo.*

1 Rapport disponible en anglais sur le site de la BCE : *http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf]*

comparé des principaux indicateurs publiés, les différences existantes entre les deux méthodologies :

• le rapport de la BCE ne tient compte que de la fraude sur les transactions (paiements et retraits) effectuées avec des cartes émises au sein de la zone SEPA alors que l'Observatoire intègre, en complément, la fraude sur les transactions effectuées en France à l'aide de cartes émises hors de la zone SEPA ;

• et, dans une moindre mesure, par le fait que l'Observatoire intègre l'ouverture frauduleuse de compte (ouverture d'un compte en fournissant par exemple de fausses données personnelles et de faux justificatifs de domicile) parmi les techniques de fraude aux cartes de paiement, contrairement à la méthodologie de la BCE qui la considère comme technique de fraude à l'octroi de crédit.

1| Vue d'ensemble

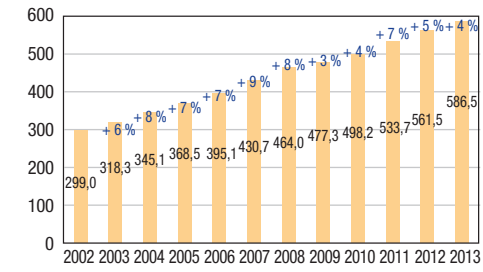
En 2013, le montant total des paiements par carte s'élève à 586,5 milliards d'euros, en croissance de 4,4 % par rapport à 2012. Le rythme de croissance annuelle de l'activité est légèrement inférieur à celui de 2012 (+ 5,2 %) ainsi qu'à la moyenne des 5 dernières années (+ 5,5 %).

Le montant total de la fraude est en augmentation similaire (+ 4,3 % par rapport à 2012) pour s'élever à 469,9 millions d'euros en 2013.

Graphique 1

Évolution du montant des transactions

(en milliards d'euros)

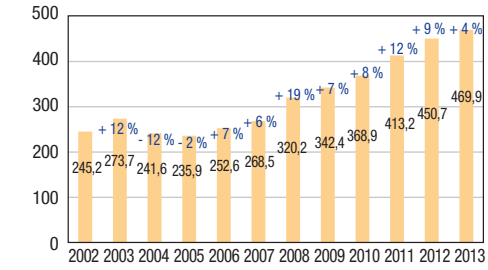


Source : Observatoire de la sécurité des cartes de paiement

Graphique 2

Évolution du montant de la fraude

(en millions d'euros)



Source : Observatoire de la sécurité des cartes de paiement

Compte tenu de ces éléments, le taux de fraude sur les paiements et les retraits par carte enregistré en 2013 dans les systèmes français reste stable à 0,080 % pour la première fois après cinq années consécutives d'augmentation.

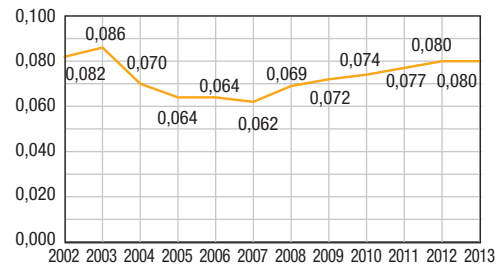
Le taux de la fraude émetteur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France s'établit en 2013 à 0,069 %, pour un montant de fraude de 376,6 millions d'euros (contre 0,065 % et 345,2 millions d'euros en 2012).

Le taux de la fraude acquéreur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France quelle que soit l'origine géographique de la carte [2], est en légère diminution. Il s'établit

Graphique 3

Évolution du taux de fraude pour tous types de cartes et transactions

(en %)



Source : Observatoire de la sécurité des cartes de paiement

2 Du fait de la prise en compte à nouveau des cartes émises en France dans le calcul de la fraude acquéreur, et du double compte en résultant, la somme de la fraude émetteur (376,6 millions d'euros) et de la fraude acquéreur (331,9 millions d'euros) est supérieure au montant total de la fraude (469,9 millions d'euros). De même, la moyenne des taux de fraude émetteur (0,069 %) et acquéreur (0,059 %) est inférieure au taux de fraude moyen (0,080 %) du fait de la prise en compte des transactions domestiques dans le calcul des deux taux de fraude, ce type de transactions connaissant par ailleurs le taux de fraude le moins élevé (0,046 % contre 0,350 % pour les transactions internationales – voir tableau 2 sur la répartition de la fraude par zone géographique).

en 2013 à 0,059 %, pour un montant de fraude de 331,9 millions d'euros (contre 0,062 % en 2012, pour un montant de fraude de 331,8 millions d'euros).

Pour autant, le nombre de cartes pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2013 s'élève à 861 000 (+ 12 % par rapport à 2012).

Le montant moyen d'une transaction frauduleuse est en diminution, pour s'établir à 116 euros contre 125 euros en 2012.

2| Répartition de la fraude par type de carte

Le taux de fraude pour les cartes de type « interbancaire » s'établit à 0,080 % en 2013, niveau stable par rapport à 2012, après cinq années consécutives d'augmentation. Le taux de fraude pour les cartes de type « privatif » s'établit à 0,065 % en 2013 (contre 0,076 % en 2012), en diminution pour la deuxième année consécutive après 4 années d'augmentation.

Tableau 1

Répartition de la fraude par type de carte

(taux en %, montants en millions d'euros)

	2009	2010	2011	2012	2013
Cartes de type « interbancaire »	0,072 (324,3)	0,074 (351,5)	0,077 (394,9)	0,080 (434,4)	**0,080 (455,8)**
Cartes de type « privatif »	0,068 (18,2)	0,080 (17,4)	0,083 (18,3)	0,076 (16,3)	**0,065 (14,0)**
Total	0,072 (342,4)	0,074 (368,9)	0,077 (413,2)	0,080 (450,7)	**0,080 (469,9)**

Source : Observatoire de la sécurité des cartes de paiement

Pour les cartes de type « interbancaire », les taux de fraude émetteur et acquéreur sont respectivement de 0,069 % [3] et de 0,060 % [4] (contre 0,066 % et 0,062 % en 2012). La valeur moyenne d'une transaction frauduleuse est de 113 euros, contre 122 euros en 2012.

Pour les cartes de type « privatif », les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,044 % [5] et à 0,057 % [6] (contre 0,051 % et 0,068 % en 2012). La valeur moyenne d'une transaction frauduleuse s'élève à 352 euros en 2013, contre 344 euros en 2012.

Tableau 2

Répartition de la fraude par zone géographique

(taux en %, montants en millions d'euros)

	2009	2010	2011	2012	2013
Transactions nationales	**0,033 (144,0)**	**0,036 (163,8)**	**0,044 (211,5)**	**0,045 (226,4)**	**0,046 (238,6)**
Transactions internationales	**0,449 (198,4)**	**0,423 (205,0)**	**0,367 (201,7)**	**0,380 (224,3)**	**0,350 (231,3)**
– dont émetteur français et acquéreur étranger [a)]	0,594 (121,6)	0,728 (54,9)	0,638 (51,0)	0,759 (62,5)	0,688 (70,2)
– dont émetteur français et acquéreur SEPA	–	0,331 (50,6)	0,255 (44,3)	0,316 (56,3)	0,366 (67,9)
– dont émetteur étranger [b)] et acquéreur français	0,324 (76,8)	0,831 (64,5)	0,892 (81,3)	0,639 (78,2)	0,404 (64,1)
– dont émetteur SEPA et acquéreur français	–	0,195 (35,0)	0,122 (25,1)	0,132 (27,3)	0,135 (29,1)
Total	**0,072 (342,4)**	**0,074 (368,9)**	**0,077 (413,2)**	**0,080 (450,7)**	**0,080 (469,9)**

a) À partir de 2010 : acquéreur hors SEPA uniquement.
b) À partir de 2010 : émetteur hors SEPA uniquement.
Source : Observatoire de la sécurité des cartes de paiement

3 Le taux de fraude émetteur des cartes de type « interbancaire » est inférieur au taux de fraude moyen des cartes de même type car ce dernier prend en compte, en complément, les transactions réalisées en France avec des cartes émises à l'étranger, ces dernières connaissant un taux de fraude plus élevé que celui des transactions réalisées avec les cartes françaises tous pays confondus.

4 Le taux de fraude acquéreur des cartes de type « interbancaire » est inférieur au taux de fraude moyen des cartes de même type car ce dernier prend en compte, en complément, les transactions réalisées à l'étranger avec les cartes émises en France, ces dernières connaissant un taux de fraude plus élevé que celui des transactions réalisées en France toutes origines de cartes confondues. Voir également les éléments de la note 2, concernant la moyenne des taux de fraude émetteur et acquéreur.

5 Voir note 3 concernant les cartes de type « interbancaires » et qui s'applique également aux cartes de type « privatif ».

6 Voir note 4 concernant les cartes de type « interbancaires » et qui s'applique également aux cartes de type « privatif ».

3| Répartition de la fraude par zone géographique

Le montant de la fraude sur les transactions internationales (231,3 millions d'euros en 2013) demeure à un niveau légèrement inférieur à celui de la fraude sur les transactions nationales (238,6 millions d'euros en 2013). Au regard du montant des opérations en jeu, le taux de fraude sur les transactions internationales (0,350 %) reste toutefois toujours près de huit fois plus élevé que le taux de fraude sur les transactions nationales (0,046 %).

Les transactions internationales représentent ainsi un peu plus de 11,3 % de la valeur totale des transactions par carte mais comptent pour 49,2 % du montant total de la fraude.

On continue à observer, parmi ces transactions internationales, une meilleure maîtrise de la fraude sur les transactions réalisées au sein de la zone SEPA que sur celles réalisées au sein des pays situés hors de la zone SEPA, même si cet écart a tendance à diminuer grâce aux efforts réalisés dans le monde entier, à l'exception notable des États-Unis, pour migrer l'ensemble des cartes et des terminaux de paiements vers le standard EMV et en France pour améliorer la détection des tentatives de fraude ciblant spécifiquement les transactions hors zone SEPA :

- le taux de fraude sur les transactions effectuées en France avec des cartes étrangères émises hors de la zone SEPA (0,404 %) est trois fois supérieur à celui des transactions effectuées avec des cartes étrangères émises dans la zone SEPA (0,135 %) ;

- le taux de fraude sur les transactions effectuées hors zone SEPA avec des cartes émises en France (0,688 %), est près de deux fois supérieur à celui des transactions effectuées au sein de la zone SEPA avec ces mêmes cartes (0,366 %).

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.

Dans ce contexte, on rappellera que Visa, MasterCard, American Express et Discover (Diners Club International) ont annoncé en 2012 un ensemble de mesures incitatives visant à encourager l'adoption du standard EMV aux États-Unis, au plus tard en octobre 2015 (voir chapitre 2|3, page 20 du rapport 2012).

4| Répartition de la fraude par type de transaction

La typologie de transaction de paiement par carte adoptée par l'Observatoire distingue les paiements de proximité et sur automate (réalisés au point de vente ou sur distributeurs de carburant, de billets de transport…) des paiements à distance (réalisés sur Internet, par courrier, par téléphone/fax, etc.) et des retraits. Pour une meilleure lisibilité, les développements qui suivent distinguent les données des transactions nationales des données des transactions internationales.

En ce qui concerne les transactions nationales (voir tableau 3), on observe que :

- le taux de fraude sur les paiements de proximité et sur automate est en diminution à 0,013 %. Ces paiements représentent plus de 66 % du montant des transactions nationales, et seulement 19 % du montant de la fraude.

Le taux de fraude sur les retraits est en augmentation de 6 % par rapport à 2012 pour s'établir à 0,033 %. Cette augmentation s'explique principalement par le nombre toujours élevé de piratages de distributeurs automatiques de billets (environ 1 000 en 2013) et de points de vente (environ 200 en 2013, soit 2 fois plus de cas qu'en 2012) qui sont devenus des cibles privilégiées pour des réseaux de fraude organisés, ainsi que par un nombre toujours important des cas de vols de carte avec code confidentiel.

Face à la confirmation de ces tendances déjà observées en 2011 et en 2012, l'Observatoire réitère 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 est quant à lui en diminution à 0,269 %, tout en demeurant vingt fois plus élevé que le taux de fraude sur les paiements de proximité. On notera en particulier que le taux de fraude sur les paiements

Tableau 3

Répartition du taux de fraude nationale par type de transaction

(taux en %, montants en millions d'euros)

	2009	2010	2011	2012	2013
Paiements	0,038	0,041	0,049	0,049	0,050
	(123,2)	(137,3)	(177,8)	(190,0)	(199,9)
dont paiements de proximité et sur automate	0,014	0,012	0,015	0,015	0,013
	(41,0)	(36,2)	(48,1)	(51,2)	(45,8)
dont paiements à distance	0,263	0,262	0,321	0,299	0,269
	(82,2)	(101,1)	(129,6)	(138,8)	(154,2)
dont par courrier/téléphone	*0,263*	*0,231*	*0,259*	*0,338*	*1,122* [a]
	(30,3)	*(27,3)*	*(25,4)*	*(29,4)*	*(29,2)*
dont sur Internet	*0,263*	*0,276*	*0,341*	*0,290*	*0,229*
	(51,9)	*(73,9)*	*(104,2)*	*(109,4)*	*(125,0)*
Retraits	0,019	0,024	0,029	0,031	0,033
	(20,8)	(26,5)	(33,7)	(36,4)	(38,6)
Total	**0,033**	**0,036**	**0,044**	**0,045**	**0,046**
	(144,0)	**(163,8)**	**(211,5)**	**(226,4)**	**(238,6)**

a) L'augmentation très importante, par rapport à 2012, du taux de fraude sur les paiements à distance effectués par courrier ou par téléphone s'explique pour grande partie par la modification de la méthodologie utilisée par le Groupement des Cartes Bancaires pour évaluer la part des transactions par courrier ou par téléphone au sein des transactions à distance. Cette correction a conduit à revoir fortement à la baisse leur montant, qui a été divisé par 3 environ, au profit des paiements sur Internet. Elle explique également environ un tiers de la baisse du taux de fraude sur les paiements par Internet, les deux autres tiers de la baisse étant liés aux efforts de lutte contre la fraude déployés par l'ensemble des acteurs en 2013.

Source : Observatoire de la sécurité des cartes de paiement

sur Internet diminue sensiblement pour s'établir à 0,229 % (contre 0,290 % en 2012) [7], alors qu'il se maintient à un niveau plus élevé pour les paiements à distance effectués par courrier ou par téléphone (1,122 % en 2013). Ces résultats obtenus pour les paiements sur Internet témoignent des efforts réalisés par les émetteurs et par les e-commerçants pour déployer des dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte pour les paiements les plus risqués. Dans un contexte de croissance toujours soutenue du commerce électronique, les paiements à distance, qui ne représentent que 11 % de la valeur des transactions nationales, comptent pour 64,6 % du montant de la fraude.

Le niveau de la fraude sur ce canal de paiement conduit l'Observatoire à renouveler ses recommandations visant au déploiement, par les e-commerçants, notamment les plus grands d'entre eux, de dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte pour les paiements les plus risqués (cf. chapitre 1 du présent rapport).

En ce qui concerne les transactions internationales (voir tableau 4), l'Observatoire ne dispose d'une répartition de la fraude par type de transaction que pour les transactions réalisées par des cartes françaises à l'étranger.

On remarque que la fraude sur les paiements à distance auprès de e-commerçants étrangers réalisés avec des cartes françaises a très fortement augmenté (81,2 millions d'euros en 2013, contre 61,6 millions d'euros en 2012), ce qui peut s'expliquer par l'adoption progressive par les sites de commerce en ligne situés en France de dispositifs de sécurisation des paiements sur Internet et par conséquent, par un report de la cible des fraudeurs vers les sites de e-commerçants étrangers.

On constate toujours un taux de fraude sur les paiements à distance particulièrement élevé hors zone SEPA (0,848 %) et une augmentation sensible du taux de fraude sur les paiements à distance réalisés avec des cartes françaises dans la zone SEPA (0,937 % en 2013, contre 0,735 % en 2012). Le déploiement de dispositifs d'authentification renforcée, sous l'impulsion notamment des recommandations du forum européen sur la sécurité des moyens de paiement (*SecuRe Pay* – cf. chapitre 1) devrait toutefois permettre d'infirmer cette tendance en zone SEPA.

7 À peu près un tiers de cette baisse est toutefois imputable à un changement méthodologique réalisé en 2013. Voir note du tableau 3.

Enfin, on remarquera une diminution de la fraude sur les paiements de proximité et les retraits réalisés par les cartes françaises dans la zone SEPA, où l'utilisation d'EMV est désormais généralisée.

Tableau 4

Répartition du taux de fraude internationale par type de transaction

(taux en %, montants en millions d'euros)

Émetteur français – Acquéreur étranger	2010	2011	2012	2013
Paiements	0,795	0,561	0,687	0,547
	(39,8)	(30,5)	(37,8)	(40,3)
dont paiements de proximité et sur automate	0,655	0,369	0,456	0,377
	(25,8)	(16,0)	(19,8)	(17,7)
dont paiements à distance	1,310	1,320	1,551	0,848
	(14,0)	(14,5)	(18,0)	(22,6)
dont par courrier/téléphone	*1,193*	*1,011*	*1,150*	*1,234*
	(3,8)	*(3,1)*	*(4,0)*	*(6,4)*
dont sur Internet	*1,360*	*1,440*	*1,720*	*0,751*
	(10,2)	*(11,4)*	*(14,1)*	*(16,2)*
Retraits	0,596	0,800	0,904	1,054
	(15,1)	(20,5)	(24,7)	(29,9)
Total	**0,728**	**0,638**	**0,759**	**0,688**
	(54,9)	**(51,0)**	**(62,5)**	**(70,2)**
Émetteur français – Acquéreur SEPA				
Paiements	0,396	0,300	0,372	0,434
	(49,1)	(43,1)	(55,3)	(66,8)
dont paiements de proximité et sur automate	0,112	0,140	0,131	0,089
	(9,2)	(12,6)	(11,7)	(8,2)
dont paiements à distance	0,944	0,571	0,735	0,937
	(40,0)	(30,5)	(43,6)	(58,6)
dont par courrier/téléphone	*0,566*	*0,643*	*0,532*	*1,566*
	(4,0)	*(5,6)*	*(6,5)*	*(11,3)*
dont sur Internet	*1,021*	*0,557*	*0,788*	*0,856*
	(36,0)	*(24,9)*	*(37,1)*	*(47,3)*
Retraits	0,052	0,040	0,036	0,036
	(1,5)	(1,2)	(1,1)	(1,1)
Total	**0,331**	**0,255**	**0,316**	**0,366**
	(50,6)	**(44,3)**	**(56,3)**	**(67,9)**
Émetteur étranger – Acquéreur français				
Paiements	0,982	1,056	0,739	0,451
	(63,2)	(80,7)	(77,7)	(63,2)
Retraits	0,103	0,042	0,033	0,051
	(1,4)	(0,6)	(0,6)	(0,9)
Total	**0,831**	**0,892**	**0,639**	**0,404**
	(64,5)	**(81,3)**	**(78,2)**	**(64,1)**
Émetteur SEPA – Acquéreur français				
Paiements	0,239	0,155	0,158	0,158
	(33,8)	(24,3)	(26,6)	(28,2)
Retraits	0,032	0,017	0,017	0,025
	(1,2)	(0,8)	(0,7)	(0,9)
Total	**0,195**	**0,122**	**0,132**	**0,135**
	(35,0)	**(25,1)**	**(27,3)**	**(29,1)**

Source : Observatoire de la sécurité des cartes de paiement

Encadré 2

Fraude nationale en vente à distance selon le secteur d'activité

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

Tableau

Ventilation de la fraude nationale sur les paiements à distance par secteur d'activité

(montants en millions d'euros, part en %)

Secteur	Montant de fraude	Part du secteur dans la fraude
Commerce généraliste et semi-généraliste	32,1	21,1
Voyage, transport	31,0	20,3
Services aux particuliers	27,6	18,1
Téléphonie et communication	17,9	11,8
Équipement de la maison, ameublement, bricolage	12,9	8,5
Approvisionnement d'un compte, vente de particulier à particulier	9,4	6,2
Produits techniques et culturels	7,1	4,7
Services aux professionnels	4,1	2,7
Alimentation	3,6	2,4
Jeu en ligne	3,4	2,3
Divers	2,5	1,6
Assurance	0,4	0,3
Santé, Beauté, Hygiène	0,2	0,1
Total	**152,3**	**100,0**

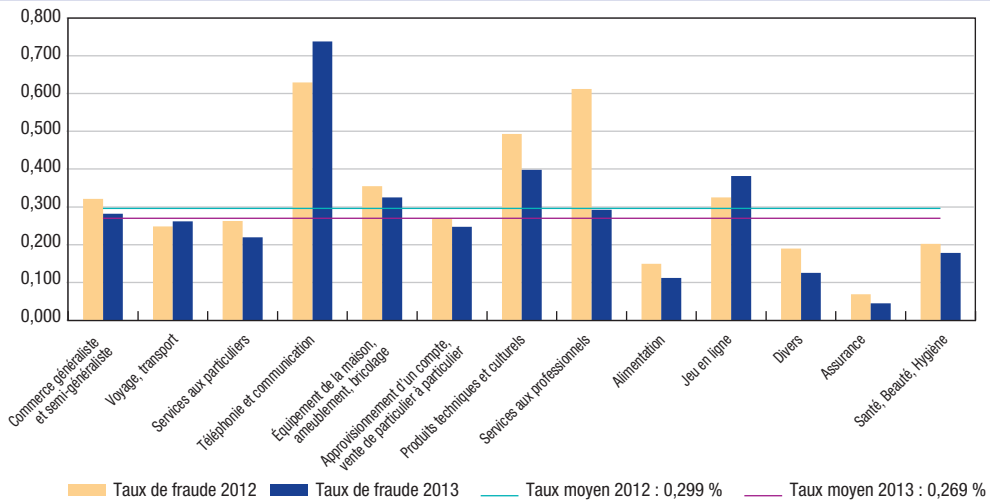
Les secteurs Commerce généraliste et semi-généraliste, Voyage/transport, Services aux particuliers et Téléphonie et communication représentent 71 % du montant de la fraude sur Internet, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Produits techniques et culturels, Jeu en ligne).

On note que les taux de fraude par secteur sont tous en baisse à l'exception notable des secteurs Téléphonie et communication et Jeu en ligne qui connaissent également de manière durable des taux de fraude supérieurs à la moyenne. L'Observatoire appelle ainsi les acteurs de ces deux secteurs à renforcer les mesures visant à lutter contre la fraude.

Graphique

Taux de fraude nationale sur les paiements à distance par secteur d'activité

(en %)



1 *Cf. annexe 6 pour une description des secteurs retenus.*

5| Répartition de la fraude selon son origine

La typologie définie par l'Observatoire distingue les origines de fraude suivantes :

• carte perdue ou volée : le fraudeur utilise une carte de paiement obtenue suite à une perte ou un vol ;

• carte non parvenue : la carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;

• carte falsifiée ou contrefaite : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation ; une carte entièrement fausse est réalisée à partir de données recueillies par le fraudeur ;

• numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé ensuite en vente à distance ;

• une catégorie « autres », qui regroupe, en particulier pour les cartes de type « privatif », la fraude liée à l'ouverture frauduleuse de compte par usurpation d'identité.

L'histogramme suivant (cf. graphique 4) indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements).

L'origine de fraude la plus importante (64,6 % des montants), en légère augmentation par rapport à 2012, est celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance.

Cette évolution conduit l'Observatoire à renouveler sa recommandation concernant la généralisation des dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte par l'ensemble des e-commerçants.

La fraude liée aux pertes et vols de cartes représente encore 34,2 % des paiements nationaux frauduleux, mais elle est de nouveau en diminution (34,9 % en 2011) après la hausse constatée en 2011.

La contrefaçon de cartes n'est à l'origine que de 0,2 % des paiements nationaux frauduleux, en diminution sensible (2,6 % en 2011). Cette diminution s'explique principalement par l'adoption de technologies de cartes à puce par certains systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes [8].

Enfin, on observe une diminution de la rubrique « autres », qui est généralement utilisée par les systèmes de carte de type « privatif » pour indiquer les fraudes par ouverture frauduleuse d'un compte ou d'un dossier de crédit (fausse identité) et qui est très significative pour ce type de carte (près de 33 %).

Tableau 5

Répartition de la fraude nationale selon son origine et par type de carte en 2013

(montants en millions d'euros, part en %)

	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	81,7	34,2	81,0	34,6	0,6	14,7
Carte non parvenue	0,9	0,4	0,6	0,3	0,3	7,4
Carte altérée ou contrefaite	0,5	0,2	0,2	0,1	0,3	6,5
Numéro usurpé	154,0	64,6	152,3	65,1	1,7	38,5
Autres	1,5	0,6	0,0	0,0	1,5	32,9
Total	238,6	100,0	234,1	100,0	4,4	100,0

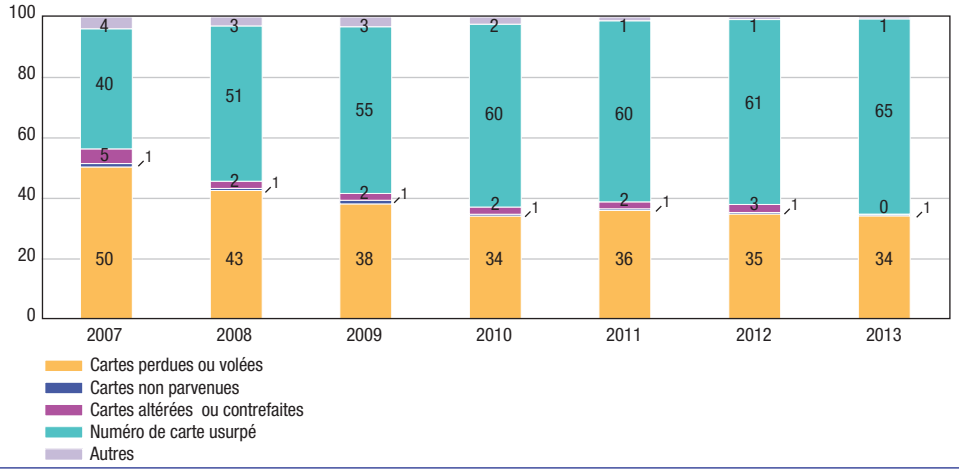
Source : Observatoire de la sécurité des cartes de paiement

8 Migration de la technologie d'authentification SDA – *Static Data Authentication* vers le DDA – *Dynamic Data Authentication*.

Graphique 4

Répartition de la fraude nationale selon son origine (transactions nationales en valeur)

(en %)



Source : Observatoire de la sécurité des cartes de paiement

Encadré 3

Indicateurs des services de police et de gendarmerie

Pour l'année 2013, les services de police et de gendarmerie enregistrent à nouveau une baisse des interpellations pour fraude à la carte bancaire, faisant état de 103 personnes interpellées contre 122 en 2012, 234 en 2011, 235 en 2010, 190 en 2009 et 154 en 2008. Cette diminution s'explique par la prononciation de peines d'emprisonnement plus sévères par la Justice ayant entrainé dès fin 2011 une chute très nette de l'activité liée aux officines de contrefaçon de cartes bancaires étrangères.

Les piratages de distributeurs automatiques de billets (DAB) sont en légère diminution avec 1 028 piratages de DAB en 2013 (contre 1 109 en 2012, 634 en 2011, 527 en 2010, 526 en 2009, 427 en 2008, 411 en 2007, 526 en 2006, 200 en 2005 et 80 en 2004). À ceux-ci s'ajoutent 188 piratages liés aux points de vente (contre 91 en 2012 et 30 en 2011) dont 85 ciblant les terminaux de paiement (contre 60 en 2012) et 103 les distributeurs automatiques de carburant (contre 31 en 2012). Ces chiffres en nette augmentation confirment dans les faits la tendance haussière des statistiques relevées par l'Observatoire concernant la fraude en retraits et paiements à distance effectués hors zone SEPA avec des cartes françaises.

Veille technologique

1| La sécurité des terminaux de paiement

Les terminaux de paiement évoluent régulièrement au gré des changements technologiques liés par exemple à la carte de paiement utilisée (notamment le support du protocole sans contact NFC – *Near Field Communication* qui tend à se généraliser), à l'utilisation de nouveaux supports pour initier les paiements tel le téléphone portable (utilisable également en mode sans contact NFC) ainsi que, plus récemment, au développement de nouveaux équipements transformant un téléphone portable en terminal de paiement et permettant de répondre à la volonté de développer les possibilités d'acceptation de paiements par carte dans des environnements où le terminal de paiement traditionnel n'avait pas encore réussi à s'implanter.

Ces dernières années, l'Observatoire a analysé plusieurs de ces évolutions, en particulier, sur les réseaux d'automates de paiement (rapport 2008, chapitre 3, p. 36), sur les nouveaux terminaux de paiement « légers » (rapport 2009, chapitre 3, p. 38) et sur le mobile comme terminal de paiement (rapport 2011, chapitre 3, p. 31).

Le nombre de cas de compromission de terminaux de paiement ayant fortement augmenté lors des deux années précédentes (on relève 188 piratages liés aux points de vente en 2013 contre seulement 30 en 2011), l'Observatoire a souhaité, dans le cadre de son programme de travail 2013-2014, d'une part, faire l'état des lieux de la mise en œuvre des recommandations qu'il avait formulées précédemment sur la sécurité des terminaux de paiement et d'autre part, actualiser ses analyses au regard de l'évolution des techniques de fraude telle que présentée dans son rapport 2012 (chapitre 3, 2|, p. 32).

1|1 Rappel sur les différents types de terminaux de paiement

Les terminaux de paiement électronique (TPE) permettent à un commerçant doté d'un point de vente physique d'accepter les paiements par carte. Ils disposent généralement de plusieurs interfaces d'échange avec l'instrument [1] de paiement du porteur : un coupleur de carte à microprocesseur, un lecteur de piste magnétique et une antenne NFC, lorsque le terminal supporte les paiements sans contact, ainsi que d'un clavier numérique pour la saisie du code PIN (*Personal Identification Number*) associé à l'instrument de paiement et d'une imprimante pour générer le reçu remis au client. Ils affichent les informations destinées au porteur et au commerçant (par exemple, le montant du paiement et le résultat de la demande d'autorisation), et ils assurent des fonctions de reconnaissance et de validation de l'instrument de paiement et des fonctions de transmission des données de transaction vers les serveurs de l'acquéreur.

Certains modèles de terminaux permettent également d'intégrer la signature manuelle du porteur, voire offrent des moyens de reconnaissance biométrique du porteur.

On distingue généralement deux types de terminaux de paiement :

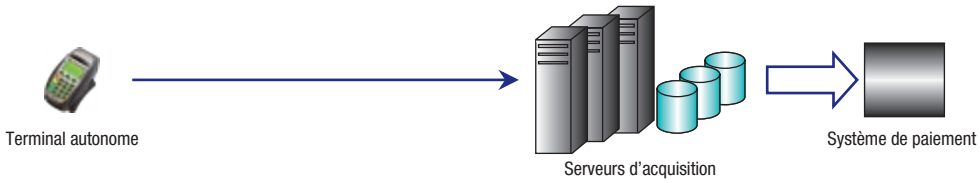
- les TPE autonomes : il s'agit d'équipements dédiés aux seules opérations de paiement. Ce sont des matériels sophistiqués permettant de réaliser de nombreux contrôles monétiques afin de vérifier l'authenticité de la carte et du porteur. Ils interagissent avec la puce de l'instrument de paiement et mettent en jeu des mécanismes de contrôles cryptographiques complexes, pour indiquer si l'instrument est valide et si le porteur est bien le titulaire de celui-ci. Ils mettent également en œuvre l'ensemble des traitements monétiques qui permettent de valider un paiement, y compris en mode hors-ligne, et ils échangent directement avec les serveurs d'acquisition de l'établissement acquéreur du commerçant ;

- les TPE en mode « grappe » ou concentrés : il s'agit d'équipements qui assurent principalement les fonctions d'interfaçage avec l'instrument de paiement et avec le porteur, y compris les mécanismes de contrôles cryptographiques. Ils font

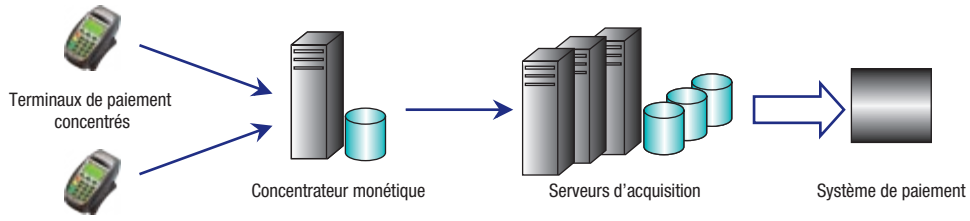
1 Une carte le plus fréquemment ou, le cas échéant, un téléphone portable.

Encadré 1

Principe de fonctionnement d'un terminal autonome



Principe de fonctionnement des terminaux « grappés » ou concentrés



exécuter la majeure partie des autres fonctions de sécurité (par exemple, le contrôle de validité de l'instrument) sur un contrôleur monétique distant auquel le terminal est connecté en permanence. Ce concentrateur monétique peut être situé chez le commerçant ou chez un prestataire externe. Le concentrateur monétique effectue la liaison avec les serveurs d'acquisition de l'établissement acquéreur du commerçant. Cette approche permet de diminuer les coûts et de faciliter la gestion des changements applicatifs lorsque le commerçant dispose de plusieurs points d'acceptation (par exemple de plusieurs caisses) car ceux-ci peuvent être effectués de manière centralisée, soit par une mise à jour sur le serveur, soit par la mise à jour de tous les terminaux, commandée depuis le serveur. Les terminaux en mode concentré sont principalement utilisés dans le commerce de grande distribution, par les péages d'autoroute, les automates de distribution de carburant. On notera que les solutions qui permettent de transformer un téléphone mobile de type *smartphone* en système d'acceptation de paiements par carte peuvent en général être classées dans cette catégorie.

1|2 Rappel des principaux risques et des mesures pouvant être mises en œuvre pour les maîtriser

On se contentera ici de rappeler, tout en invitant le lecteur à consulter le chapitre sur les techniques de fraude qui figure dans le rapport 2012 de l'Observatoire (chapitre 3, p. 32), que les attaques visant les terminaux de paiement peuvent être de type physique ou de type logique et qu'elles peuvent cibler tant le terminal directement que le lien utilisé pour l'échange des données entre le terminal et le concentrateur monétique ou bien le concentrateur monétique lui-même.

Ces attaques visant directement les terminaux peuvent être mises en œuvre pour :

- capturer des données qui seront ensuite utilisées pour contrefaire des cartes de paiement ou pour effectuer des paiements frauduleux à distance ;

- tromper le commerçant en lui faisant croire que le paiement a été validé ;

• forcer le terminal de paiement à accepter un paiement réalisé avec une carte contrefaite et/ou falsifiée, en rendant inopérantes les fonctions de contrôle qui auraient dû conduire à son refus ;

• modifier le montant de la transaction.

Les mesures mises en œuvre pour protéger les terminaux contre les attaques physiques peuvent reposer sur :

• des moyens de protection contre l'accès physique aux composants internes du terminal ;

• des mesures de lutte contre l'injection de code malveillant ;

• des mesures de protection des réseaux, en particulier dans le cas des terminaux concentrés ;

• des mesures permettant d'empêcher la substitution de terminaux de paiement en point de vente ;

• et des consignes de vigilance qui doivent être appliquées par les porteurs et par les commerçants.

Tous les systèmes de paiement par carte opérant en France exigent l'agrément préalable des terminaux de paiement avant que ceux-ci puissent être utilisés par les commerçants pour accepter les paiements des cartes émises par les participants d'un système. Cet agrément repose sur une évaluation sécuritaire préalable du matériel au regard d'exigences définies par le gestionnaire du système de paiement par carte. L'évaluation vise à s'assurer du respect des exigences et du niveau requis de robustesse des mécanismes de protection implémentés par le fabricant dans son modèle de terminal.

1|3 État des lieux de la mise en œuvre des précédentes recommandations de l'Observatoire (2008 à 2012)

1|3|1 Processus d'agrément des terminaux

Dans le cadre du système CB, le Groupement des Cartes Bancaires « CB » édicte pour le domaine des terminaux de paiement des règles de recevabilité à l'agrément qui comprennent entre autres :

• une conformité au standard EMV Level 2 [2], établie par un laboratoire EMV ;

• une conformité au standard CB « Manuel de paiement électronique CB » qui précise les exigences fonctionnelles qui s'appliquent aux terminaux de paiement pour l'acceptation des paiements au standard CB ;

• une conformité sécuritaire au standard PCI [3] PTS POI (*Payment Card Industry – PIN Transaction Security Point of Interaction*) dont l'objet est la protection au sein du terminal du code PIN et des données de compte du porteur.

Ces règles sont compatibles *de facto* avec les règles d'agrément des systèmes de paiement par carte internationaux.

L'agrément est prorogé à chaque renouvellement des certifications qui le sous-tendent. Dans le cas où l'une de ces certifications, d'ordre sécuritaire ou fonctionnel, échoit, le produit agréé change de statut et n'est plus commercialisable. Des échéances de fin de vie des terminaux déployés peuvent également être appliquées par les gestionnaires de systèmes de paiement par carte.

Ces règles visent à s'assurer que le niveau de protection physique des terminaux de paiement agréés est propre à garantir un haut niveau de sécurité pour les données traitées.

Elles s'appliquent également aux dispositifs permettant de transformer un téléphone portable de type *smartphone* en terminal de paiement. Dans son rapport annuel 2011, l'Observatoire a mené une étude dédiée à cette évolution du mode d'acceptation des paiements par carte, en constatant que les *smartphones* étant, par essence, multiapplicatifs, multitâches et dépourvus d'éléments de sécurité, ils apparaissent *a priori* peu adaptés aux requis habituellement exigés sur les terminaux de paiement traditionnels, dédiés à cette fonction. Notamment,

2 La conformité EMV Level 2 couvre notamment le processus de sélection de l'application de paiement carte, et englobe également EMV Level 1, c'est-à-dire la conformité physique et électrique des composants au standard.

3 Les standards PCI sont développés par l'organisme « PCI SSC » (*Payment Card Industry Security Standard Council*), fondé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc.

la question de leur conformité à l'ensemble des exigences sécuritaires PCI reste à ce jour posée, en l'absence d'un équipement spécifique qui leur est adjoint (on se reportera pour plus de détails au rapport 2011, chapitre 3, p. 31).

La « *prise en compte de l'état de l'art en matière de développement* », recommandée précédemment par l'Observatoire, fait bien l'objet d'un point d'attention dans les processus de certification et d'agrément. Ce contrôle repose actuellement sur des évaluations conduites par un laboratoire choisi par le fabricant du terminal lui-même sur la base de critères définis par les gestionnaires de systèmes de paiement par carte, selon des méthodologies précisées dans les standards. Depuis juin 2013, la nouvelle version du standard PCI PTS POI comprend une analyse plus poussée du code source, même si cette tâche est toujours rendue difficile, principalement par l'absence d'outil efficace permettant d'automatiser cette analyse et par les coûts importants que nécessite donc une analyse humaine.

Les standards de sécurité intègrent des exigences en matière de « *durcissement de la sécurité des systèmes d'exploitation des terminaux de paiement, notamment en désactivant ou en supprimant les composants logiciels et les fonctionnalités inutilisés, et en mettant en place des restrictions d'accès à certaines données* », comme recommandé précédemment par l'Observatoire. Toutefois, les terminaux hébergent à la fois des applications de paiement des gestionnaires de systèmes de paiement par carte et des applications tierces développées pour les commerçants, par exemple, la gestion de programmes de fidélisation, et ces applications ne font pas partie aujourd'hui du périmètre de certification.

La « *réalisation de tests réguliers incluant le système d'exploitation et les applications embarquées des terminaux de paiement, afin d'évaluer de façon continue le niveau de sécurité de l'ensemble et sa capacité de résistance à des attaques* », préconisée précédemment par l'Observatoire, n'est actuellement pas exigée par les gestionnaires de paiement par carte dans leurs processus d'agrément et ce test n'est en pratique réalisé qu'à l'occasion de l'évaluation initiale du produit.

L'Observatoire note toutefois que les règles définies par les gestionnaires de systèmes de paiement par carte exigent la mise en place par le fabricant d'un processus de veille sécuritaire sur l'ensemble des composants du produit, et que ce processus est évalué lors de la certification. Chaque nouvelle version d'un produit doit par ailleurs faire l'objet d'une certification propre. Ces règles permettent donc en pratique de mesurer régulièrement le niveau de sécurité de l'ensemble et sa capacité de résistance à des attaques.

L'Observatoire note également que les gestionnaires de systèmes de paiement par carte ont la possibilité de demander aux fabricants de terminaux de procéder à des contrôles spécifiques sur les modèles agréés et, en cas de résultat négatif, d'engager les actions nécessaires.

1|3|2 Exploitation et maintenance des terminaux

L'Observatoire a pu constater que sa recommandation sur la mise en œuvre par les systèmes de paiement par carte et par les établissements acquéreurs d'une traçabilité rigoureuse du matériel d'acceptation déployé en point de vente, n'avait pas été suffisamment prise en compte. En effet, si les établissements acquéreurs sont bien en mesure d'assurer une bonne traçabilité des terminaux de paiement dont ils sont les propriétaires, par exemple lorsque le terminal est loué au commerçant, il leur est en pratique plus difficile d'assurer la qualité de cette traçabilité lorsque le terminal est la propriété du commerçant ou la propriété d'un prestataire retenu par le commerçant.

Fin 2012, une attaque est survenue sur un modèle particulier de terminal utilisé dans un contexte de monétique intégrée, correspondant au modèle de terminaux concentrés. L'attaque consistait en la substitution d'un terminal, situé sur un point de vente, par un terminal modifié préalablement par ajout d'un dispositif de *skimming*. Celui-ci permet l'enregistrement des données de la piste magnétique et du code PIN, et leur transmission à distance par Bluetooth. Le recensement des points de vente utilisant le modèle de terminal ciblé par cette attaque a nécessité plus de six mois de délais, en raison principalement d'un défaut de traçabilité technique des points d'acceptation. Une mise à jour des protocoles monétiques a été engagée par le Groupement des Cartes Bancaires « CB » pour permettre la collecte de toutes les informations nécessaires au recensement des terminaux déployés, y compris lorsque ceux-ci sont reliés à un concentrateur.

L'expérience tirée de cette attaque a permis de démontrer l'efficacité des dispositifs d'appairage entre les terminaux et le reste du système monétique (notamment la caisse). Cet appairage, qui peut consister en une simple reconnaissance du numéro de série du terminal par la caisse, a la vertu de limiter les possibilités de substitution ou d'insertion de terminaux frauduleusement modifiés. L'appairage pourrait aller jusqu'à la mise en œuvre d'une véritable authentification mutuelle entre les éléments du système, qui nécessiterait alors la mise en œuvre de certificats.

De même, l'attaque a permis de démontrer l'intérêt de la sensibilisation des commerçants et de leur personnel à la nécessité de rester à tout moment vigilants à l'égard de leurs matériels d'acceptation.

Concernant les recommandations sur la mise à jour régulière des systèmes d'exploitation des terminaux et sur la mise en œuvre des correctifs à distance et de manière sécurisée, l'Observatoire a pu constater que les fabricants de concentrateurs fournissaient généralement des solutions permettant la mise à jour des terminaux grappés à partir des concentrateurs auxquels ils sont reliés.

De telles solutions ne sont pas encore disponibles pour les terminaux autonomes, et la mise en œuvre des correctifs nécessite toujours pour ces derniers une intervention locale sur le terminal.

Si les établissements acquéreurs sont bien en mesure de mettre à jour, à distance, les TPE dont ils sont les propriétaires, par exemple lorsque le terminal est loué au commerçant, il apparaît que ces opérations concernent principalement les paramètres de fonctionnement du terminal et plus rarement leurs systèmes d'exploitation.

1|4 Recommandations de l'Observatoire

À la lumière de la tendance haussière des attaques visant les terminaux de paiement, l'Observatoire appelle l'ensemble des acteurs à une vigilance accrue dans ce domaine.

L'Observatoire recommande plus particulièrement que les processus d'agrément des dispositifs d'acceptation par les systèmes de paiement par carte soient renforcés afin de mieux gérer les terminaux défaillants ou en fin de vie.

L'Observatoire souligne que les efforts engagés pour disposer d'une meilleure traçabilité des équipements, avec pour conséquence une évolution attendue des protocoles monétiques mis en œuvre, doivent également se poursuivre et aboutir dans les meilleurs délais car ils permettront une gestion plus rigoureuse des parcs de terminaux déployés, qu'ils soient la propriété de l'acquéreur, du commerçant ou d'un prestataire technique de ce dernier.

Dans ce contexte, l'Observatoire invite les gestionnaires de systèmes de paiement par carte, en collaboration avec les autres acteurs et notamment les commerçants, à étudier la conception et la mise en œuvre de dispositifs techniques permettant aux acquéreurs ou aux émetteurs de ne plus accepter de paiements à l'aide de terminaux non agréés ou dont l'agrément n'est plus valide ou a été retiré.

Enfin, l'Observatoire renouvelle sa recommandation concernant la mise à jour régulière des systèmes d'exploitation des terminaux et invite tous les acteurs concernés à généraliser les solutions permettant la mise à jour des TPE (logiciel et paramètres), à distance et de manière sécurisée.

2| État des lieux des techniques d'authentification renforcée du porteur

L'Observatoire constate depuis plusieurs années, dans son suivi statistique, un écart important [4] entre les taux de fraude observés sur les paiements de proximité et ceux réalisés en vente à distance (VAD). Pour cette raison, la sécurisation des paiements par carte en vente à distance et sur Internet en particulier a fait l'objet de plusieurs recommandations visant à renforcer l'authentification des porteurs.

Ainsi, la progression continue de la fraude VAD a poussé l'Observatoire à recommander dès 2008 un

4 Cf. le chapitre 2 du présent rapport.

renforcement des mécanismes d'authentification du porteur qui étaient jusqu'alors majoritairement fondés sur la saisie du numéro de carte et du cryptogramme visuel. La définition des modalités techniques de l'authentification forte (ou non rejouable) promue a été laissée au libre choix des systèmes de paiement carte ainsi que des émetteurs, en charge de généraliser le dispositif à l'ensemble des porteurs.

Début 2014, la généralisation de l'équipement des porteurs en dispositif d'authentification non rejouable était quasiment atteinte avec environ 93,7 % de porteurs équipés [5].

Parallèlement, la BCE a publié en janvier 2013 un ensemble de recommandations et bonnes pratiques sur la sécurité des paiements par Internet, issues des travaux du forum européen sur la sécurité des paiements de détail (forum *SecuRe Pay*). Ces recommandations, en particulier celles visant à sécuriser l'enrôlement du porteur et à l'équiper d'une solution d'authentification renforcée pour les paiements à distance, confortent celles de l'Observatoire. La mise en œuvre de ces recommandations par tous les acteurs concernés est attendue en Europe le 1er février 2015 au plus tard.

La présente étude vise à dresser un état des lieux des techniques d'authentification renforcée mises en œuvre par les systèmes de paiement par carte et émetteurs français.

2|1 Caractéristiques de l'authentification renforcée du porteur

L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté préalablement (par exemple un identifiant) [6]. S'il est aisé de définir l'authentification statique par l'utilisation d'un simple mot de passe, l'authentification renforcée fait appel à des concepts qu'il est nécessaire de préciser. Dans son rapport sur la sécurité des paiements par Internet, la BCE définit l'authentification renforcée [7] par « *un ensemble de procédures fondées sur l'utilisation d'au moins deux des trois éléments caractérisant la possession, la connaissance ou l'identité propre d'une personne :*

- *élément possédé par la personne (*token *ou jeton d'authentification, carte à puce, téléphone portable, etc.) ;*
- *élément connu par la personne et elle seule (mot de passe, identifiant, etc.) ;*
- *élément constitutif de l'identité de la personne (empreinte biométrique, etc.).*

Ces trois éléments doivent être indépendants dans le sens où la compromission de l'un ne doit pas entraîner la compromission de l'autre. En outre, l'un de ces trois facteurs au moins doit être non rejouable et non reproductible (excepté pour la biométrie). »

Ainsi, l'utilisation en proximité de la carte à puce assortie de la saisie d'un PIN (*Personal Identification Number)* pour valider un paiement correspond bien à la définition de l'authentification renforcée. Les chapitres suivants visent à présenter un inventaire des principales solutions d'authentification renforcée utilisées dans le cadre des paiements à distance, d'abord sur Internet en règle générale, puis plus spécifiquement lors d'un paiement effectué depuis un mobile et enfin par courrier ou au moment d'une commande passée au téléphone auprès d'un opérateur.

2|2 Authentification renforcée du porteur lors d'un paiement Internet traditionnel

L'authentification renforcée du porteur constitue un maillon essentiel du dispositif de lutte contre la fraude aux paiements par carte, lui-même plus large et permettant ainsi de lutter plus efficacement contre les tentatives d'initiations d'opérations de paiement frauduleuses. Ce chapitre vise à dresser un état des lieux des principales techniques d'authentification renforcée utilisées dans le cadre d'un paiement

5 Collecte statistiques « 3D-Secure », novembre 2013 à fin avril 2014.
6 Définition ANSSI (*http://www.securite-informatique.gouv.fr/gp_rubrique33.html*).
7 *Strong customer authentication*.

par Internet traditionnel, correspondant à un usage d'Internet depuis un ordinateur. Chaque émetteur étant libre de ses choix de dispositifs d'authentification, divers types de solutions ont été déployés en fonction des établissements émetteurs ainsi que de la typologie de clientèle.

2|2|1 Le SMS OTP

La sécurisation des transactions par l'envoi d'un SMS contenant un code non rejouable sur le mobile du porteur (SMS OTP [8]) est la solution d'authentification renforcée la plus utilisée par les émetteurs du marché français, en particulier à travers le protocole de sécurisation des paiements « 3D-Secure ». Si, à ce jour, les déploiements sont dans les faits achevés, leur utilisation effective par les émetteurs a pu prendre plus de temps, en raison d'une nécessaire fiabilisation des numéros de mobile enregistrés dans leurs bases de données.

Si ce dispositif permet de répondre au besoin d'authentification renforcée du porteur, il présente néanmoins plusieurs faiblesses en termes de sécurité : le canal de communication utilisé lors de l'envoi du SMS n'est pas sécurisé [9], la présence d'un logiciel malveillant installé sur le téléphone peut compromettre la sécurité du dispositif et enfin la possibilité, sous certaines conditions, de désactiver la carte SIM du porteur légitime et d'activer une carte SIM différente mais pointant sur le même numéro peut faciliter la réalisation d'opérations frauduleuses.

Des mesures existent toutefois afin de pallier ces limites. En premier lieu, il est nécessaire de rappeler que l'utilisation d'un dispositif d'authentification par SMS OTP s'inscrit dans un mécanisme plus global de lutte contre la fraude. En particulier, les outils de gestion de risque et de *scoring* des transactions mis en place par les systèmes de paiement par carte, les émetteurs ou encore les commerçants, comme les contrôles effectués par les émetteurs lors d'une demande d'autorisation, viennent compléter l'authentification renforcée du porteur et participent à la détection de transactions d'origine frauduleuse. Ensuite, s'agissant de la problématique des logiciels malveillants, l'environnement technique des téléphones mobiles continue d'évoluer pour offrir des fonctionnalités améliorant leur sécurité, notamment à travers la sécurisation des systèmes d'exploitation mobiles afin de prévenir l'exécution d'applications malveillantes non autorisées. Il est à ce titre nécessaire que les progrès réalisés dans ce domaine se poursuivent. Enfin, en ce qui concerne la lutte contre la désactivation illégitime d'une carte SIM, un renforcement des procédures existantes a été mis en place par les opérateurs de téléphonie mobile mais les efforts doivent être intensifiés afin de rendre ces mesures plus efficaces.

Fort de ces constats, il semble important que l'Observatoire reste vigilant quant à la sécurité de ce moyen d'authentification renforcée du porteur, dont l'efficacité n'est toutefois pas remise en cause à ce jour.

Par ailleurs, l'usage du SMS OTP s'avère paradoxalement peu adapté aux paiements réalisés depuis un téléphone mobile, supprimant de fait la sécurisation de la transaction par l'usage de deux canaux de communication distincts, mais également par le manque d'ergonomie entre la réception d'un SMS et le processus de paiement sur mobile, qu'il soit réalisé au moyen d'un navigateur ou d'une application mobile [10].

2|2|2 La carte virtuelle dynamique

La carte virtuelle dynamique (CVD) permet à un porteur de ne pas saisir son véritable numéro de carte lors d'un paiement sur Internet. Pour ce faire,

8 *One-time password.*
9 Absence de chiffrement des données transmises par SMS permettant une interception des données en clair.
10 Il convient cependant de souligner l'utilité du canal SMS lorsqu'il s'agit d'informer en temps réel le porteur d'opérations atypiques (transaction à l'étranger, de montant élevé, etc.) et ainsi lui permettre de faire opposition rapidement en cas d'opération frauduleuse.

un environnement dédié, généralement accessible depuis la banque en ligne du porteur, lui permet de générer un ensemble de codes uniques [11] et valables pour une seule transaction qu'il pourra saisir à la place des données présentes sur le support physique de sa carte. L'accès au code dynamique n'étant pas réalisé sur un canal de communication distinct, il est nécessaire que l'accès à l'environnement de génération de l'OTP soit lui-même sécurisé par une authentification renforcée. Par conséquent, la CVD ne peut être considérée comme dispositif d'authentification renforcée que si l'accès au dispositif est bien protégé par une authentification renforcée.

2|2|3 Le lecteur de carte physique pour générer un OTP

Le mini-lecteur autonome de cartes de paiement permet la génération d'un code à usage unique en insérant la carte dans celui-ci et en s'authentifiant par la saisie de son code PIN. Ce dispositif présente l'avantage d'un niveau de sécurité [12] proche de celui des paiements de proximité, ce qui le place parmi les dispositifs d'authentification renforcée les plus déployés parmi les principaux émetteurs de cartes après le SMS OTP. En raison du coût du terminal ainsi que des contraintes liées au déploiement d'une solution matérielle, ce type de solution est privilégié sur certaines typologies de porteurs (professionnels, porteurs ne souhaitant pas utiliser le SMS OTP, etc.).

Un second type de lecteur de carte cette fois-ci connecté [13] à l'ordinateur personnel du porteur est également déployé dans certains pays. Il permet de valider un paiement *via* une application dédiée installée sur le poste de l'utilisateur. Ce type de solution a déjà fait l'objet d'une large tentative de déploiement sur le marché français mais sans succès.

2|2|4 Cartes équipées de fonctions d'affichage (*display card*)

Les avancées technologiques dans la miniaturisation de certains composants ont permis aux fabricants de cartes d'y intégrer une zone d'affichage et un clavier numérique permettant une interaction avec son porteur. Lors d'un paiement à authentifier et comme vu dans le dispositif précédent, le porteur sera invité à saisir un code confidentiel sur sa carte, ce qui lui permettra d'obtenir un code à usage unique qu'il pourra renseigner dans la page de validation du paiement. Ce dispositif, déjà offert par certaines banques à l'étranger, fait actuellement l'objet de pilotes en France. Il présente l'avantage de ne pas avoir à équiper le porteur d'un dispositif matériel supplémentaire et bénéficie d'un niveau de sécurité équivalent à celui d'un lecteur de carte générateur d'OTP (ou d'un jeton d'authentification, voir ci-après).

2|2|5 Le jeton d'authentification (*token*)

11 PAN (*Primary Account Number* ou numéro de la carte de paiement), date de validité de la carte et cryptogramme visuel.
12 En particulier du fait de la certification exigée sur les lecteurs de carte.
13 Généralement au moyen d'une connexion de type USB.

Le jeton d'authentification est un dispositif matériel de la taille d'une clé USB permettant de générer un code à usage unique, le plus souvent synchronisé avec un serveur d'authentification distant et changeant au bout d'un laps de temps donné (par exemple 60 secondes). Ce code est ensuite saisi sur la page d'authentification lors du processus de paiement par carte. Des dispositifs de type « mini-calculette » existent également et permettent d'ajouter un clavier numérique. Celui-ci permet une interaction supplémentaire : un code à usage unique valide ne peut être obtenu qu'après avoir tapé un code confidentiel connu seulement du porteur du dispositif. Alternativement et en fonction du dispositif concerné, lors de l'étape d'authentification liée à un paiement, le serveur distant peut aussi présenter un nombre aléatoire qu'il sera nécessaire de saisir afin d'obtenir un code à usage unique en retour. De façon similaire au lecteur de carte physique, ces dispositifs sont déployés en tant que solution complémentaire par les principaux émetteurs, en ciblant par exemple certaines catégories de leurs porteurs.

2|3 Authentification renforcée du porteur lors d'un paiement mobile

Le développement de l'Internet sans fil [14] et mobile [15] a favorisé l'usage de nouveaux terminaux adaptés à des environnements de mobilité comme les tablettes ou les téléphones mobiles évolués, de type *smartphones*.

Dans ce contexte, les solutions d'authentification renforcée utilisées sur le canal Internet traditionnel soit ne sont plus adaptées, soit sont confrontées à des problématiques d'ergonomie. Le recours au SMS OTP peut créer par ailleurs une faiblesse d'un point de vue sécuritaire dans le cas d'un paiement mobile. En effet, pour un paiement effectué à partir d'un ordinateur personnel relié à Internet, la phase d'authentification repose sur un second canal utilisé, celui du réseau du téléphone mobile, ce qui renforce la sécurité de l'ensemble. Ce n'est plus le cas dès que le paiement et l'étape d'authentification ont lieu sur le même équipement.

De nouvelles solutions apparaissent afin de répondre aux exigences du canal mobile. À ce titre, il convient de mentionner l'essor des portefeuilles électroniques [16] permettant de répondre notamment aux problématiques d'ergonomie propres au canal mobile puisque l'enregistrement des données sensibles de paiement est réalisé une seule fois lors de l'étape d'enrôlement, évitant ainsi au porteur la saisie des coordonnées de sa carte de paiement sur un terminal non sécurisé.

Le niveau de sécurité de ces dispositifs a fait l'objet de recommandations par l'Observatoire [17] et plus récemment par le forum européen *SecuRe Pay* [18]. Ainsi, ces recommandations portent sur le recours, par le gestionnaire du portefeuille électronique, à une authentification renforcée du porteur par l'émetteur de la carte de paiement au moment de l'enrôlement des données de celle-ci au sein du portefeuille électronique. Le gestionnaire du portefeuille électronique doit également mettre en œuvre une analyse de risques conduisant au déclenchement d'une authentification renforcée pour les paiements considérés comme risqués. Les portefeuilles électroniques respectant a *minima* ces deux recommandations sont à même de protéger efficacement les paiements effectués sur mobile.

D'autres solutions innovantes, actuellement en phase pilote, apparaissent pour sécuriser les paiements effectués depuis un téléphone mobile. L'une d'entre elles consiste par exemple à enregistrer les données personnelles et de paiement dans un portefeuille électronique, puis initier les paiements par la lecture au moyen de son *smartphone* d'un QR code [19] affiché sur le terminal de paiement électronique (TPE) habituel du commerçant. L'utilisateur visualise alors le montant à payer sur son *smartphone*, valide celui-ci et déclenche la saisie d'un code secret sur le TPE du commerçant. Cette solution, reposant sur deux facteurs d'identification et deux canaux distincts répond aux critères de l'authentification renforcée.

14 De type Wifi public ou privé.
15 De type GPRS, 3G, 4G, etc.
16 Solutions ayant fait l'objet d'une étude dans le rapport 2011 de l'Observatoire.
17 Cf. rapport 2011, chapitre 3, 2| : « Portefeuille électronique et paiement par carte ».
18 *https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf*
19 *Quick response code* : code base en deux dimensions permettant de stocker des informations en vue d'initier, notamment, des opérations de paiement.

Il existe également des initiatives qui visent à intégrer au sein des *smartphones* de dernière génération des dispositifs d'authentification biométrique, reposant notamment sur la lecture d'empreinte digitale [20]. La diffusion de cette fonctionnalité pourrait à l'avenir jouer un rôle dans la sécurisation des paiements mobiles, dans la mesure où les dispositifs d'authentification retenus s'avéreraient particulièrement robustes d'un point de vue sécuritaire et ne pourraient être aisément contournés par l'exploitation de failles de sécurité du dispositif biométrique ou des composants périphériques qui lui sont attachés. La mise en place de processus d'évaluation et de certification sécuritaires de ces éléments pourrait œuvrer en ce sens.

Enfin, il convient de mentionner l'existence de téléphones mobiles équipés d'éléments de sécurité spécifiques embarqués (appelés « *secure elements* »), permettant ainsi d'isoler les fonctionnalités de paiement du reste des applications mobiles. Ces solutions, bien que ne faisant pas l'objet d'un déploiement important en raison de leur coût de mise en œuvre, sont opérationnelles et utilisées dans des secteurs d'activité requérant un haut niveau de sécurisation des échanges par le canal du téléphone mobile.

2|4 Authentification renforcée sur le canal MO/TO

En raison du développement soutenu du commerce par Internet, le paiement carte par courrier ou téléphone (*Mail Order/ Telephone Order* – MO/TO) est en diminution sensible. Cependant, ces deux canaux demeurent toujours utilisés dans certaines situations (coupons papiers, abonnements, etc.) et peuvent donc constituer une cible pour les fraudeurs, avec le risque de voir une partie de la fraude se déplacer du canal Internet, aujourd'hui mieux sécurisé, vers ces canaux de vente plus traditionnels.

À ce jour, le paiement carte par courrier reste difficile à sécuriser, car il est peu adapté à ce canal. Pour les paiements réalisés par téléphone, l'authentification du porteur par la génération d'un code à usage unique est envisageable et vient renforcer l'analyse produite par des outils de *scoring* des transactions chez le commerçant, largement utilisés pour la vente à distance sur Internet [21]. Pareillement, des mécanismes connus de protection des données sensibles du paiement par carte sont mis en place au niveau des commerçants afin de les protéger contre le risque de vol de ces données.

Par ailleurs, le développement des portefeuilles électroniques pourrait également bénéficier à la sécurisation des paiements par carte réalisés par téléphone. Les données sensibles liées au paiement étant déjà enregistrées dans le portefeuille électronique, le payeur n'a plus qu'à communiquer son identifiant (généralement son numéro de téléphone), puis valider la demande de paiement dans une application mobile ou par *push* SMS [22]. Ainsi, le commerçant ne voit plus circuler les données sensibles de paiement.

3| Conclusion

Le secteur de la vente à distance connaissant un taux de fraude près de vingt fois supérieur à celui des paiements de proximité, les efforts en matière de lutte contre la fraude doivent être poursuivis, notamment en renforçant l'authentification du porteur, conformément aux recommandations formulées par l'Observatoire depuis 2008. Les émetteurs demeurant libres du choix des dispositifs à mettre en place, l'Observatoire constate qu'un ensemble diversifié de solutions, tant en termes de fonctionnalités que de robustesse face aux attaques de sécurité, est proposé sur le marché.

20 On peut aussi mentionner les solutions à l'étude reposant sur une authentification du porteur d'un portefeuille électronique par sa voix.
21 Cf. rapport 2009 de l'OSCP, chapitre 3|2 sur la sécurité des paiements par courrier et téléphone.
22 *Push* SMS : l'utilisateur valide son paiement en répondant au SMS reçu et non par la saisie externe de l'OTP.

Parmi ces dispositifs, l'envoi d'un code non rejouable par SMS sur un téléphone mobile, ou *smartphone*, est aujourd'hui la solution la plus utilisée en France. Si, d'un point de vue sécuritaire, l'efficacité de cette solution n'est pas à ce jour remise en cause, l'Observatoire considère cependant que les progrès en termes de sécurisation du *smartphone* en tant que support d'authentification non rejouable doivent être poursuivis afin de se prémunir contre des attaques découlant de la présence de logiciels malveillants. Il conviendra également de renforcer les procédures visant à empêcher les fraudeurs de désactiver la carte SIM du porteur légitime et d'activer une SIM différente pointant sur le même numéro, ce qui peut conduire à la réalisation d'opérations frauduleuses. Fort de ces constats, l'Observatoire restera vigilant quant à la sécurité de ce dispositif d'authentification renforcée du porteur.

Plusieurs autres solutions existent et permettent un renforcement de l'authentification du porteur lors d'un paiement par carte sur Internet. Les cartes virtuelles dynamiques peuvent par exemple remplir cette fonction, à condition que l'accès au dispositif de génération des codes uniques utilisables en ligne soit bien protégé par une authentification renforcée. L'Observatoire constate également le déploiement effectif de solutions reposant : sur un lecteur de carte physique pouvant générer des codes à usage unique suite à l'insertion d'une carte de paiement, sur des cartes de paiement intégrant directement un écran miniaturisé permettant d'afficher de tels codes, ou encore sur des jetons (*tokens*) d'authentification autonomes présentant une fonction similaire.

L'essor du paiement en ligne effectué depuis un *smartphone* connecté à Internet pose cependant la question des dispositifs les plus adaptés à ce mode de fonctionnement. Si les solutions reposant sur l'envoi d'un SMS apparaissent dans ce contexte peu ergonomiques, l'Observatoire constate que le développement des portefeuilles électroniques constitue une solution possible à ce problème. Le niveau de sécurité de ces dispositifs a fait l'objet de recommandations par l'Observatoire dans son rapport 2011 et plus récemment par le forum européen *SecuRe Pay*, en 2012. Elles portent ainsi sur une authentification renforcée du porteur par l'émetteur de la carte de paiement au moment de l'enrôlement des données de celle-ci au sein du portefeuille électronique et sur le déclenchement d'une authentification renforcée pour les paiements considérés comme risqués. Les portefeuilles électroniques respectant *a minima* ces deux recommandations sont à même de protéger efficacement les paiements effectués sur mobile.

Enfin, l'Observatoire note que les récentes évolutions technologiques visant à intégrer des dispositifs biométriques sur les *smartphones* pourraient être de nature à renforcer la sécurité des opérations de paiement mobile. Il apparaît toutefois nécessaire que les dispositifs d'authentification mis en œuvre sur le *smartphone* soient particulièrement robustes. Dans cette perspective, la mise en place de processus d'évaluation et de certification des composants biométriques utilisés devrait favoriser le déploiement à grande échelle de tels dispositifs pour un usage en paiement.

Protection des données personnelles dans le cadre des traitements de lutte contre la fraude

Si dans le domaine du paiement par carte en proximité, l'utilisation de la carte à puce au standard EMV permet notamment d'assurer l'authentification du porteur de manière renforcée, il n'en est pas de même pour les paiements par carte à distance qui peuvent être initiés avec un nombre limité d'informations (numéro de carte, date d'expiration et cryptogramme visuel [1]), les rendant ainsi particulièrement exposés à la fraude.

Le développement rapide des paiements par carte à distance a ainsi créé de nouveaux besoins en termes de lutte contre la fraude, incitant le développement d'outils visant à identifier les comportements frauduleux et permettre aux commerçants d'authentifier le porteur de manière renforcée au travers de leur prestataire de services de paiement, par exemple par un dispositif tel que « 3D-Secure », chaque fois que cela est possible et pertinent.

Dans ce contexte, les données à caractère personnel sont devenues un enjeu crucial pour les acteurs de la lutte contre la fraude qui les utilisent afin d'évaluer le niveau de risque d'un paiement par carte à distance et procéder si besoin à des vérifications supplémentaires (comme par exemple l'authentification renforcée du porteur) ou s'ils sont habilités à le faire, refuser la transaction en cas de risque jugé trop élevé.

Le recours à des traitements utilisant ces données, fussent-ils pour lutter contre la fraude, est encadré par la loi « Informatique et libertés », dont la bonne application est garantie par la Commission nationale de l'informatique et des libertés (CNIL).

Dans un contexte d'évolution rapide des technologies relatives à la lutte contre la fraude à distance, l'Observatoire a souhaité comprendre les défis de la règlementation applicable en matière de traitement de données à caractère personnel dans le cadre de la lutte contre la fraude.

Après avoir rappelé la définition et le périmètre des données concernées, la présente étude propose de faire un point sur les pratiques en matière de traitement de lutte contre la fraude, les dispositions règlementaires actuelles les encadrant ainsi que sur les perspectives d'évolution. Il convient de noter que bien que cette problématique de la protection des données personnelles dans le cadre des traitements de lutte contre la fraude porte dans la présente étude sur les paiements par carte, elle s'applique de manière générale aux autres moyens de paiement.

1| La protection des données à caractère personnel : une prise en compte nécessaire dans les dispositifs de lutte contre la fraude

Les dispositifs de lutte contre la fraude ont pour principal objectif de s'assurer que l'opération de paiement a bien été initiée et validée par le porteur légitime de la carte.

En France, et plus généralement en Europe, l'utilisation de la carte à puce au standard EMV permet d'assurer une authentification renforcée du porteur en proximité, garantissant un niveau de fraude très faible sur ce canal (0,013 % en 2013).

En l'absence d'un dispositif similaire pour les paiements par carte à distance, la collecte et l'exploitation de données dites à caractère personnel, c'est-à-dire qui permettent d'identifier une personne physique [2], sont devenues un véritable enjeu pour les acteurs de la lutte contre la fraude.

1 Connu aussi sous le terme « CVX2 ».

2 Le législateur a défini la notion de donnée à caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

Ainsi, grâce notamment aux évolutions technologiques, ces derniers ont la possibilité d'élargir le nombre et la nature des données à caractère personnel collectées lors d'une transaction sur Internet afin de vérifier la cohérence entre ces données et augmenter le degré de certitude quant à la personne initiant la transaction de paiement.

1|1 Les acteurs de la lutte contre la fraude

Un paiement par carte fait intervenir de nombreux acteurs jouant chacun un rôle dans les dispositifs de lutte contre la fraude selon la nature des informations dont ils disposent et selon leur positionnement dans la chaîne du paiement.

Les principaux acteurs sont les suivants :

• L'émetteur de la carte de paiement dispose par nature du champ le plus large de données sur l'utilisation de la carte par le porteur. Il est par ailleurs responsable des dispositifs de sécurité relatifs à l'instrument de paiement délivré au porteur, notamment en ce qui concerne l'authentification renforcée pour les paiements par carte sur Internet. Il dispose néanmoins d'une connaissance très limitée sur la nature de l'achat réalisé par son porteur auprès du commerçant.

• L'acquéreur des ordres de paiement est en charge du traitement des opérations de paiement par carte pour le compte de l'accepteur (commerçant). Il dispose par nature d'une connaissance limitée du porteur mais peut construire des outils de lutte contre la fraude sur la base de l'ensemble des transactions traitées en tant qu'acquéreur (par exemple en empêchant l'utilisation auprès d'un commerçant d'une carte ayant déjà fait l'objet d'une fraude auprès d'un autre commerçant dont il a la charge [3]).

• L'accepteur, à savoir le commerçant, dispose essentiellement des informations relatives à l'achat réalisé (nature du bien par exemple, mode de livraison, etc.) et le cas échéant des informations relatives au client lui-même lorsque celui-ci est déjà connu.

• Les systèmes de paiement par carte qui ont la vision la plus transversale de l'ensemble des opérations de paiement réalisées par les porteurs et/ou auprès des commerçants « affiliés » au système de paiement. À ce titre, ils réalisent des traitements de lutte contre la fraude à destination de leurs adhérents (émetteurs et/ou acquéreurs).

• Les prestataires techniques spécialisés, qui peuvent se voir confier des traitements de lutte contre la fraude par chacun des acteurs précédents, apportant ainsi une expertise et une mutualisation de traitements à des acteurs souhaitant déléguer cette fonction.

D'autres acteurs indirectement liés à la chaîne de paiement contribuent également aux dispositifs de lutte contre la fraude.

Les autorités judiciaires et de police ont en charge les enquêtes et les poursuites en cas de fraude avérée et peuvent avoir besoin le cas échéant d'accéder et de conserver les différentes données collectées par chacun des acteurs cités précédemment par voie de réquisitions judiciaires.

Les sociétés de logistique, en particulier les transporteurs de marchandises, peuvent également disposer d'informations utiles à la fois sur les points de distribution centralisés comme sur l'adresse physique de livraison d'un bien acheté sur Internet, permettant le cas échéant aux commerçants en ligne d'améliorer la qualité des informations collectées lors des traitements de lutte contre la fraude.

Enfin, le porteur de la carte est un acteur clé dans la sécurité du dispositif, en veillant notamment à conserver son code personnel confidentiel et en protégeant les données de sa carte. Il peut en outre jouer un rôle important dans la détection des opérations frauduleuses, en particulier lorsque son émetteur a mis en place des systèmes d'alerte (par exemple par l'envoi de SMS) sur les opérations réalisées. Ces dispositifs d'alerte, si mis en place en quasi-temps réel, permettent en effet à l'émetteur de réagir rapidement en cas de fraude et de bloquer ainsi toute nouvelle tentative de fraude sur une carte compromise. L'Observatoire rappelle à ce titre l'obligation pour le porteur de carte de signaler dans les meilleurs délais toute détection d'opération non autorisée à l'émetteur de sa carte et de la mettre en opposition.

3 Il appartient aux acteurs de s'assurer de la correcte information préalable du porteur légitime en cas de blocage d'une opération de paiement.

1|2 L'évolution des technologies permet d'élargir le nombre et la nature des données personnelles collectées et d'améliorer ainsi les traitements de lutte contre la fraude mis en œuvre par les différents acteurs

En l'absence de dispositif d'authentification renforcée généralisé permettant de s'assurer que le porteur légitime réalise un paiement avec sa carte, les dispositifs de lutte contre la fraude ont eu tendance, grâce notamment aux évolutions technologiques, à élargir le nombre et la nature des données, certaines étant à caractère personnel, collectées lors d'une transaction sur Internet afin de vérifier la cohérence entre ces données et d'augmenter le degré de certitude quant à la personne initiant la transaction de paiement.

Ainsi, aux côtés des données traditionnellement collectées relatives à l'identité et aux coordonnées de la personne initiant la transaction (nom, prénom, adresse postale, adresse de livraison, e-mail, numéro de téléphone, etc.), les outils de lutte contre la fraude ont progressivement intégré :

• les habitudes de consommation du porteur de la carte (nombre et détail des commandes, ancienneté de la relation, périodicité et montant des achats, habitudes de consommation, moyens de paiements utilisés, etc.) ;

• sa localisation (par exemple par l'adresse IP de l'ordinateur utilisé) ;

• les outils utilisés pour accéder à Internet (par exemple par la prise d'une empreinte numérique du terminal d'accès à Internet [4] consistant à relever des caractéristiques techniques propres au terminal et à ses composants matériels et logiciels) ;

• des données liées à son comportement (analyse du temps de remplissage de formulaires, type de saisie clavier, etc.).

L'élargissement du périmètre de données traitées permet ainsi de mettre en place des traitements plus subtils, plus ciblés qui permettent de faire des rapprochements d'informations, de construire des algorithmes sophistiqués conduisant à une analyse prédictive des comportements frauduleux au moyen d'outils dit de « *scoring* » des transactions. L'augmentation du nombre de critères retenus dans la détermination du score d'une transaction vise ainsi à obtenir une meilleure fiabilité dans la pertinence du niveau de risque évalué.

Au-delà de l'efficacité de ces traitements se pose la question du risque d'atteinte à la vie privée. Les acteurs de la chaîne du paiement par carte sont ainsi passés d'une logique déclarative où le client communique ses données (données d'identité, coordonnées, etc.) à une logique de collecte automatique de données liées à l'environnement informatique du client, sans que ce dernier en soit systématiquement informé. Les technologies utilisées permettent alors de tracer les actions et habitudes des clients, ce qui peut se traduire le cas échéant par l'enregistrement de comportements délictuels présumés dans des listes dites « noires » ou « grises ».

2| Les traitements de lutte contre la fraude reposant sur l'exploitation de données personnelles font l'objet d'une règlementation spécifique amenée à évoluer

2|1 Un régime d'autorisation assorti de nombreuses garanties entourant la protection des données

L'article 25-I-4° de la loi du 6 janvier 1978 soumet au régime d'autorisation préalable les fichiers comportant des informations destinées à prévenir la fraude ou à ficher les fraudeurs, dès lors qu'ils privent les personnes fichées d'un droit ou du bénéfice d'un contrat [5]. Il en est de même pour tous les traitements qui ont pour résultat d'établir une présomption de fraude à la charge de la personne objet du traitement et qui peuvent conduire au blocage total ou partiel d'une carte de paiement.

4 Technique dite du « *device fingerprinting* ».
5 Par exemple en refusant une commande passée lors d'un achat par Internet.

Pour obtenir cette autorisation dans les cas visés par la loi, l'entité responsable du fichier de données et/ou des traitements de lutte contre la fraude doit soumettre un dossier précisant en particulier un certain nombre de garanties relatives :

1. À la finalité du traitement : celle-ci doit être déterminée et légitime [6], permettant ainsi de vérifier que les données seront exploitées pour la ou les finalités déclarées par le responsable du traitement.

2. À la nature des données collectées : le responsable du traitement précise de manière exhaustive les données à caractère personnel qui seront utilisées dans les systèmes de lutte contre la fraude qui remonteront des alertes sur les transactions à risques, celles-ci devant être adéquates, pertinentes et non excessives. Concernant plus précisément la collecte de données liées à la carte de paiement, la CNIL a mis à jour ses recommandations [7] en 2013 sur leurs conditions de collecte, de conservation et de réutilisation.

3. À la nature des traitements réalisés : chaque type de traitement réalisé doit faire l'objet d'une description précise. Ainsi, l'élaboration d'outils de *scoring* doit être fondée sur des modèles statistiquement établis et fiables et ne doit pas porter atteinte aux droits et aux libertés individuelles. Dans un souci de proportionnalité, les différents niveaux d'analyse opérés par les différents acteurs intervenant dans le cadre de la lutte contre la fraude doivent être complémentaires. Par ailleurs, lorsque des documents justificatifs complémentaires sont demandés aux clients, il appartiendra au responsable de traitement de s'assurer que cette demande est proportionnée à la finalité du traitement. À titre d'exemple, la CNIL préconise de ne conserver que la copie du verso de la carte d'identité et proscrit la collecte de toute photocopie d'une carte de paiement ou de relevés bancaires dans le cadre d'une demande de justificatifs complémentaires.

4. Au droit d'information, de consultation et de suppression : les responsables des traitements doivent donc informer les personnes concernées de la mise en œuvre des traitements et des droits associés conformément aux dispositions de l'article 32-II de la loi du 6 janvier 1978 modifiée, ainsi que les modalités d'exercice de ces droits en précisant les différents organismes auprès desquels la personne peut exercer ses droits (par exemple si recours à un prestataire extérieur).

5. Au délai de conservation des données : le délai de conservation doit être adapté en fonction du type de traitement réalisé et de la finalité poursuivie.

6. À la sécurité physique et logique des données : ceci constitue une obligation majeure pour le responsable du traitement qui doit s'assurer de la confidentialité et de l'intégrité des données collectées. À cette fin, l'ensemble des données doit faire l'objet d'une politique de sécurité adaptée aux enjeux, passant par le recours à des mécanismes de protection physique et logique des serveurs et applications hébergeant les données collectées, mais aussi par la mise en place d'une piste d'audit permettant de détecter et d'analyser tout accès, modification ou suppression de données dans la base du responsable du traitement.

7. Au recueil du consentement : dans certain cas, il convient de faire application des dispositions de l'article 32-II de la loi du 6 janvier 1978 modifiée qui requiert le consentement explicite de la personne selon les modalités prévues dans la délibération portant recommandation n° 2013-378 du 5 décembre 2013. C'est le cas en particulier du stockage d'informations sur l'équipement d'un utilisateur ou de l'accès à des informations préalablement stockées [8].

En dépit de l'usage d'outils de lutte contre la fraude par les acteurs de la chaîne du paiement par carte, notamment les commerçants en ligne, la majorité d'entre eux n'a pas effectué de demande d'autorisation préalable conformément au requis de la CNIL. Dans ce contexte, cette dernière a engagé des travaux en vue de simplifier les formalités déclaratives relatives aux traitements visant plus particulièrement la lutte contre la fraude. Ces travaux seront l'occasion de prendre en compte un certain nombre de points d'attention soulignés par les acteurs de la filière.

6 Par exemple « détection et prévention des fraudes par carte bancaire ».
7 Délibération n° 2013-358 du 14 novembre 2013.
8 Ainsi, les « *cookies* », ces fichiers présents au sein des navigateurs Internet et comportant des informations sur l'usage du site par un visiteur, sont concernés par cette disposition, comme tout autre mécanisme similaire.

2|2 La simplification des formalités déclaratives sera l'occasion de prendre en compte les dernières évolutions relatives aux traitements de lutte contre la fraude

Dans le cadre des échanges menés au sein de l'Observatoire pour la présente étude, plusieurs freins relatifs à la protection des données personnelles ont été identifiés dans le cadre de la lutte contre la fraude :

• dans la mesure où de nombreux accepteurs ont dans les faits recours à des prestataires externalisés pour réaliser les traitements de lutte contre la fraude, la question de leur responsabilité au regard des traitements externalisés mériterait d'être clarifiée ;

• une facilitation de la mutualisation des informations collectées est souhaitée entre certains acteurs, notamment lorsqu'il s'agit de listes noires permettant d'identifier des fraudeurs avérés, afin de lutter plus efficacement contre la fraude.

Cette mutualisation facilitée pourrait être bénéfique pour les commerçants dans certains secteurs, comme cela est déjà le cas dans celui de la téléphonie mobile (GIE Préventel).

Une mutualisation est par ailleurs actuellement envisagée entre les forces de l'ordre dans le cadre d'une procédure de dépôt de plaintes en ligne, afin de faciliter l'instruction des fraudes aux paiements par carte sur Internet ;

• l'exploitation des données d'identification des nouveaux canaux d'accès à Internet (ordinateurs mais aussi *smartphones*, tablettes, etc.) par les responsables de traitements de lutte contre la fraude demeure aujourd'hui strictement encadrée et limitée. Dans la mesure où la personne concernée y donne son consentement, la CNIL a cependant récemment autorisé certains acteurs à mettre en œuvre des traitements reposant sur de telles données, dans le cadre d'un dispositif de lutte contre la fraude ;

• les règles relatives aux durées de conservation des données personnelles à des fins de lutte contre la fraude sont claires, mais certains acteurs ont souligné que ces durées peuvent fortement varier en fonction des situations rencontrées, ce qui peut être source de confusion (cf. encadré) ;

• enfin, dans un contexte où la maîtrise du taux de fraude d'un e-commerçant revêt un enjeu financier et concurrentiel important, il conviendrait d'harmoniser les règles de protection des données personnelles dans le cadre des traitements de lutte contre la fraude au niveau européen. Il est à noter à ce titre que les autorités européennes de protection des données se sont réunies au sein d'un G29, avec pour mission de contribuer à une application uniforme des règles de l'Union européenne en matière de protection des données. Cependant, à ce jour, de nombreuses dispositions font encore l'objet d'une appréciation différente selon le pays dans lequel est réalisé le traitement.

Pour répondre à ces problématiques, la CNIL a engagé des travaux en vue de l'adoption d'une autorisation dite unique en matière de lutte contre la fraude aux moyens de paiement. Cette autorisation unique permettrait ainsi d'encadrer la collecte et le traitement des données afin que la lutte contre la fraude, qui correspond à l'intérêt légitime des professionnels, soit proportionnée au respect des droits des personnes. À ce titre, il pourra être rappelé que le recours à des dispositifs, tel que « 3D-Secure », permettant l'authentification renforcée du porteur au moment du paiement, peut être de nature à limiter le besoin de recourir à une collecte de données personnelles jugée excessive.

En outre, cette autorisation unique faciliterait l'accomplissement des formalités préalables pour les responsables de traitements et devrait par ailleurs s'accompagner d'une clarification relative à la responsabilité des auteurs des traitements, en particulier lorsque ceux-ci font appel à un prestataire externalisé pour les réaliser dans le cadre d'un dispositif de lutte contre la fraude.

Encadré

Règles de la CNIL relatives à la durée de conservation des données personnelles dans le cadre de la lutte contre la fraude

Il convient de distinguer notamment la durée de conservation des données analysées et générées dans le cadre de l'émission d'alertes de celle des données contenues en listes noires (entraînant un score négatif immédiat) ou grises (ne générant pas nécessairement un score négatif immédiat mais indiquant le besoin d'informations complémentaires pour mener à bien une transaction).

Les alertes émises dans le cadre de la lutte contre la fraude n'ont pas, en soi, vocation à être conservées mais peuvent donner lieu à des contrôles auprès des personnes concernées, confirmant ou infirmant la fraude. La durée de conservation est nécessairement courte et liée à ces vérifications. Certains responsables de traitement souhaitent toutefois conserver les données issues des alertes, pour affiner et faire évoluer leur modèle de score. Cette conservation pourrait être faite de manière anonymisée.

Les données inscrites en liste noires/grises sont liées aux fraudes et aux tentatives de fraude confirmées (hors impayés résultant d'un défaut de provision du compte) à la suite notamment d'une enquête. Dans ce cas, la CNIL préconise une durée de conservation n'excédant pas trois ans, durée qui correspond au délai de prescription des délits.

Lorsqu'une procédure judiciaire est engagée, les données relatives à la transaction sont conservées jusqu'au terme de la procédure.

Enfin, les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses.

3| Conclusion

En l'absence d'un dispositif similaire à la carte à puce au standard EMV pour les paiements par carte à distance, la collecte et l'exploitation de données dont certaines à caractère personnel, sont devenues un véritable enjeu pour les acteurs de la lutte contre la fraude.

Grâce aux évolutions technologiques, ces derniers ont la possibilité d'élargir le nombre et la nature des données à caractère personnel collectées lors d'une transaction sur Internet afin de vérifier la cohérence entre ces données et d'augmenter le degré de certitude que la personne initiant la transaction de paiement est bien le détenteur légitime de la carte.

Les acteurs de la lutte contre la fraude sont ainsi passés d'une logique déclarative où le client communique ses données (données d'identité, coordonnées, etc.) à une logique de collecte automatique de données liées à l'environnement informatique du client, sans que ce dernier en soit systématiquement informé.

Si les traitements de lutte contre la fraude utilisant les données personnelles répondent à une finalité légitime de protection contre les opérations non autorisées, et viennent compléter l'ensemble des dispositifs de sécurisation existants, ils restent encadrés par la loi « Informatique et libertés », dont la bonne application est garantie par la CNIL.

Cette dernière a toutefois engagé des travaux en vue de simplifier les formalités déclaratives relatives aux traitements de lutte contre la fraude.

Ces travaux seront ainsi l'occasion de prendre en compte les points d'attention soulignés par les acteurs de la lutte contre la fraude, comme le besoin de clarifier la responsabilité des acteurs ayant recours à des prestataires externalisés, celui de l'éventuelle mutualisation des données de fraude entre les

acteurs afin de gagner en efficacité, la possibilité le cas échéant d'avoir recours à de nouvelles données d'identification issues des nouvelles technologies ou encore le besoin de clarifier les règles relatives à la durée de conservation des données personnelles utilisées à des fins de lutte contre la fraude.

Une autorisation simplifiée permettrait, dans les cas prévus à l'article 25 de la loi Informatiques et libertés, d'encadrer la collecte et le traitement des données afin que la lutte contre la fraude, qui correspond à l'intérêt légitime des professionnels, soit proportionnée au respect des droits des personnes. À ce titre, il pourra être rappelé que le recours à des dispositifs, tels que « 3D-Secure », permettant l'authentification renforcée du porteur au moment du paiement, peut être de nature à limiter le besoin de recourir à une collecte de données personnelles jugée excessive.

Enfin, dans un contexte où la maîtrise du taux de fraude d'un e-commerçant revêt un enjeu financier et concurrentiel important, la protection des données personnelles nécessite d'être abordée sur le plan européen. Ainsi, la Commission européenne a proposé un projet de règlement relatif à la protection des données directement applicable aux pays membres de l'Union européenne afin que l'Europe se dote de règles uniformes en cohérence avec les directives sur les services de paiement. Ce futur règlement européen devrait être adopté courant 2015 et devrait permettre une harmonisation des obligations imposées aux acteurs réalisant des traitements de lutte contre la fraude reposant sur l'exploitation de données à caractère personnel.

Annexes

Conseils de prudence à l'usage des porteurs

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

Soyez responsables

- Votre carte est strictement personnelle : ne la prêtez à personne, même pas à vos proches.
- Vérifiez régulièrement qu'elle est en votre possession.
- Si votre carte comporte un code confidentiel, gardez-le secret. Ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter et surtout ne le rangez jamais avec votre carte.
- Lorsque vous composez votre code confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal ou du distributeur de votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.

Soyez attentifs

Lors des paiements chez un commerçant

- Vérifiez l'utilisation qui est faite de votre carte par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider la transaction.

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

- Protégez votre numéro de carte : ne le stockez pas sur votre ordinateur, ne l'envoyez pas par simple courriel et vérifiez la sécurisation du site du commerçant (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 conditions générales de vente.
- 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.

Lors de vos déplacements à l'étranger

- Renseignez-vous sur les précautions à prendre et contactez l'établissement émetteur de votre carte avant votre départ, 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 votre carte.

A2

Sachez réagir

Vous avez perdu ou on vous a volé votre carte

• Faites immédiatement opposition en appelant le numéro que vous a communiqué l'établissement émetteur de la carte. Pensez à le faire pour toutes vos cartes perdues ou volées.
• 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 anomalies sur votre relevé de compte, alors que votre carte est 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 carte.

Sauf 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 carte 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 proche le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir), il faut déposer une réclamation auprès de l'établissement émetteur de la carte, dès que possible et dans un délai fixé par la loi, de 13 mois à compter de la date de débit de l'opération contestée. Dans ces conditions, votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être immédiatement remboursées sans frais. 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 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).

Protection du titulaire d'une carte 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 titulaire d'une carte de paiement.

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 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 titulaire de la carte.

Opérations nationales ou intracommunautaires

Les opérations de paiement visées sont les opérations effectuées en euros ou en francs CFP sur le territoire de la République française [1]. Sont également concernées les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer, à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un autre État partie à l'accord sur l'EEE (Union européenne + Liechtenstein, Norvège et Islande), en euros ou dans la devise nationale de l'un de ces États.

Concernant les opérations non autorisées, c'est-à-dire en pratique les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, le titulaire de la carte devra contester, auprès de son prestataire 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 titulaire de la carte 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.

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.

Avant information aux fins de blocage de la carte

Avant « opposition » [2], 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 la carte 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 titulaire de la carte ne voit pas sa responsabilité engagée.

La responsabilité du titulaire de la carte 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 la carte si elle était en possession de son titulaire au moment où l'opération non autorisée a été réalisée.

En revanche, le titulaire de la carte 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 sa carte, convenues avec son prestataire de services de paiement.

Enfin, si le prestataire de services de paiement émetteur de la carte ne fournit pas de moyens appropriés permettant la mise en opposition de la carte, le client ne supporte aucune conséquence financière, sauf à avoir agi de manière frauduleuse.

Après information aux fins de blocage de la carte

Après mise en opposition de la carte, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de la carte ou de l'utilisation détournée des données qui lui sont liées.

Là encore, les agissements frauduleux du titulaire de la carte le privent de toute protection et il demeure responsable des pertes liées à l'utilisation de sa carte.

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 le titulaire de la carte a informé son prestataire de services de paiement de la perte, du vol, du détournement ou de la contrefaçon de sa carte, 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.

2 La loi utilise désormais le terme « information aux fins de blocage de l'instrument de paiement ».

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.

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 conventionnellement étendu à 120 jours. En revanche, le remboursement immédiat de l'opération non autorisée est étendu.

3 Y compris Mayotte depuis le 31 mars 2011.
4 Qui n'est pas partie à l'accord sur l'EEE (UE + Liechtenstein, Norvège et Islande).

Missions et organisation de l'Observatoire

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

Cartes concernées

L'ancien article L. 132-1 du *Code monétaire et financier,* dans sa rédaction antérieure au 1er novembre 2009 [1], définissait une carte de paiement comme toute carte émise par un établissement de crédit permettant à son titulaire de retirer ou de transférer des fonds. L'ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, ayant maintenu le périmètre de compétence de l'Observatoire, il a été décidé de continuer de s'appuyer sur cette définition en l'étendant aux prestataires de services de paiement qui sont, aux termes du I de l'article L. 521-1 du *Code monétaire et financier*, les établissements de crédit, les établissements de monnaie électronique et les établissements de paiement.

En conséquence, les compétences de l'Observatoire concernent les cartes émises par les prestataires de services de paiement ou par les institutions assimilées [2] et dont les fonctions sont le retrait ou le transfert de fonds. Elles ne couvrent pas les cartes parfois appelées « cartes purement privatives » qui peuvent être émises par une entreprise sans avoir à obtenir un agrément délivré par l'Autorité de contrôle prudentiel et de résolution. Il s'agit, d'une part, des cartes monoprestataires émises par une seule entreprise et acceptées en paiement d'un bien ou d'un service déterminé par elle-même ou par des accepteurs ayant noué avec elle un accord de franchise commerciale [3] et, d'autre part, des cartes multiprestataires, qui ne sont acceptées, pour l'acquisition de biens ou de services, que dans les locaux de l'émetteur de la carte ou, dans le cadre d'un accord commercial avec ce dernier, dans un réseau limité de personnes ou pour un éventail limité de biens ou de services [4].

Le marché français compte de nombreuses offres en matière de cartes de paiement qui relèvent des compétences de l'Observatoire. Parmi celles-ci, on distingue généralement les cartes dont le schéma d'acceptation des paiements et des retraits repose sur :

- un nombre réduit de prestataires de services de paiement émetteurs et acquéreurs (cartes généralement qualifiées de « privatives ») ;

- un nombre élevé de prestataires de services de paiement émetteurs et acquéreurs (cartes généralement qualifiées d'« interbancaires »).

1 Cet article a été supprimé par l'ordonnance de transposition de la directive européenne sur les services de paiement. En effet, il n'était pas compatible avec la directive qui fixe les règles applicables aux opérations de paiement en fonction de la cinématique du paiement, ceci afin d'assurer une neutralité technologique entre les différents instruments de paiement utilisés.

2 Les institutions assimilées sont, aux termes du II de l'article L. 521-1 du *Code monétaire et financier*, la Banque de France, l'Institut d'émission des départements d'outre-mer, le Trésor public et la Caisse des dépôts et consignations.

3 Ces cartes sont dispensées d'agrément par le 5° du I de l'article L. 511-7, l'article L. 525-6 et le II *in fine* de l'article L. 521-3 du *Code monétaire et financier*.

4 Ces cartes sont dispensées d'agrément par le II de l'article L. 511-7, l'article L. 525-5 et le I de l'article L. 521-3 du *Code monétaire et financier*.

Ces cartes peuvent offrir des fonctions diverses qui conduisent à la typologie fonctionnelle suivante en matière de cartes de paiement :

• les cartes de débit sont des cartes associées à un compte de paiement [5] permettant à son titulaire d'effectuer des retraits ou des paiements qui seront débités selon un délai fixé par le contrat de délivrance de la carte. Ce débit peut être immédiat (retrait ou paiement) ou différé (paiement) ;

• 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 (supérieur à quarante jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

• les cartes nationales permettent d'effectuer des paiements ou des retraits exclusivement auprès d'accepteurs établis sur le territoire français ;

• les cartes internationales permettent d'effectuer des paiements et des retraits dans tous les points d'acceptation, nationaux ou internationaux, de la marque ou d'émetteurs partenaires avec lesquels le système de paiement par carte a signé des accords ;

• les porte-monnaie électroniques sont des cartes sur lesquelles sont stockées des unités de monnaie électronique. Aux termes de l'article L.315-1 du *Code monétaire et financier*, *« la monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L.133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique »*.

La typologie fonctionnelle rappelée ci-dessus inclut également les paiements sans contact.

Attributions

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

• il suit la mise en œuvre des mesures adoptées par les émetteurs et les commerçants pour renforcer la sécurité des cartes de paiement. Il se tient informé des principes adoptés en matière de sécurité ainsi que des principales évolutions ;

• il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de cartes 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 types de cartes de paiement ;

• il assure une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des cartes 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.

5 Les comptes de paiement qui sont, aux termes du I de l'article L. 314-1 du *Code monétaire et financier*, des comptes détenus au nom d'une ou plusieurs personnes, utilisés aux fins de l'exécution d'opérations de paiement, correspondent aux comptes de dépôts à vue ouverts sur les livres des banques et aux comptes ouverts sur les livres des autres prestataires de services de paiement.

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

Composition

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

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel et de résolution ou son représentant ;
- dix représentants des émetteurs de cartes de paiement, notamment de cartes bancaires, de cartes privatives et de porte-monnaie électroniques ;
- cinq représentants du collège consommateurs du Conseil national de la consommation ;
- cinq représentants des commerçants issus notamment du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;
- trois personnalités qualifiées en raison de leurs compétences.

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 Christian Noyer, gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément à l'article R. 142-23 et suivants du *Code monétaire et financier*, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté en 2003 un règlement intérieur qui précise les conditions de son fonctionnement.

A10

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 cartes 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 cartes 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 cartes de paiement. En 2010, l'Observatoire a décidé la création d'un groupe de travail dédié à la problématique du déploiement de la technologie « 3D-Secure ».

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

Liste nominative des membres de l'Observatoire

En application de l'article R. 142-22 du *Code monétaire et financier*, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre de l'Économie, du Redressement productif et du Numérique. Les derniers arrêtés de nomination datent des 6 septembre 2013 et 11 décembre 2013.

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Philippe GOUJON
Député
Michèle ANDRÉ
Sénatrice

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

Emmanuel CARRERE
Philippe RICHARD
Secrétariat général

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  Dominique RIBAN

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

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

- Le directeur général du Trésor ou son représentant :
  Magali CESANA
  Fabrice WENGER

- Le directeur général de la Compétitivité, de l'Industrie et des Services ou son représentant :
  Mireille CAMPANA

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

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Nathalie KHOKHOLKOFF
  Charles MOYNOT
  Régis PIERRE

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 :
  Valérie MALDONADO
  Philippe DEVRED

Sur proposition du ministre de la Défense :

- Le directeur général de la gendarmerie nationale ou son représentant :
  Éric FREYSSINET

A12

Représentants des émetteurs de cartes de paiement

Frédéric COLLARDEAU
Directeur de la filière des paiements
La Banque Postale
Gilbert ARIRA
Administrateur
Groupement des Cartes Bancaires
Jean-François DUMAS
Vice-Président
American Express France
Willy DUBOST
Directeur Systèmes et Moyens de paiement
Fédération bancaire française
Caroline SELLIER
Directeur Risk management et Lutte contre la fraude
Natixis Paiements
François LANGLOIS
Directeur des Relations institutionnelles
BNP Paribas Personal Finance
Frédéric MAZURIER
Directeur administratif et financier
Carrefour Banque
Gérard NEBOUY
Directeur général
Visa Europe France
Régis FOLBAUM
Président directeur général
MasterCard France
Narinda YOU
Directeur
Stratégie et pilotage interbancaire
Crédit Agricole SA

Représentants du collège « consommateurs » du Conseil national de la consommation

Régis CREPY
Confédération nationale
Associations familiales catholiques (CNAFC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)
Patrick MERCIER
Président
Association de défense d'éducation et d'information du consommateur (ADEIC)
Frédéric POLACSEK
Conseil national des associations familiales laïques (CNAFAL)
Maxime CHIPOY
UFC-Que Choisir

Représentants des organisations professionnelles de commerçants

Philippe JOGUET
Directeur Développement durable, RSE, Questions financières
Fédération des entreprises du commerce et de la distribution (FCD)
Marc LOLIVIER
Délégué général
Fédération du e-commerce et de la vente à distance (Fevad)
Jean-Jacques MELI
Chambre de commerce et d'industrie du Val d'Oise
Jean-Marc MOSCONI
Délégué général
Mercatel
Philippe SOLIGNAC
Vice-président
Chambre de commerce et d'industrie de Paris/ACFCI

Personnalités qualifiées en raison de leurs compétences

Eric BRIER
Chief Security Officer
Ingenico
David NACCACHE
Professeur
École normale supérieure
Sophie NERBONNE
Directeur adjoint à la direction des affaires juridiques, internationales et de l'expertise
Commission nationale de l'informatique et des libertés (CNIL)

Dossier statistique

Le dossier statistique qui suit a été réalisé à partir des données fournies à l'Observatoire de la sécurité des cartes de paiement par :

- les 130 membres du Groupement des Cartes Bancaires « CB » par l'intermédiaire de celui ci, MasterCard et Visa Europe France ;
- dix émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club, Franfinance, JCB et UnionPay ;
- les émetteurs du porte-monnaie électronique Moneo.

Total des cartes en circulation en 2013 : 85,5 millions
- dont 68,4 millions de cartes de type « interbancaire » (« CB », MasterCard, Visa et Moneo) ;
- et 17,1 millions de cartes de type « privatif ».

Cartes mises en opposition [1] en 2013 : environ 861 000

Les transactions nationales sont celles qui mettent en jeu un émetteur français et un commerçant accepteur français.

Jusqu'en 2009, les transactions internationales étaient de deux types :
- émetteur français/accepteur étranger et
- émetteur étranger/accepteur français.

À partir de 2010, l'Observatoire distinguant les transactions internationales avec la zone SEPA de celles avec le reste du monde, les transactions internationales sont donc désormais de quatre types :
- émetteur français/accepteur étranger hors SEPA ;
- émetteur étranger hors SEPA/accepteur français ;
- émetteur français/accepteur étranger SEPA ;
- émetteur étranger SEPA/accepteur français.

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

Tableau 1

Le marché des cartes de paiement en France en 2013 – Émission

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	7 688,46	332,48	137,26	8,30	43,25	3,67
Paiements à distance hors Internet	17,66	2,46	9,49	0,72	7,13	0,52
Paiements à distance sur Internet	709,69	53,40	128,66	5,18	31,38	1,98
Retraits	1 496,32	117,51	28,25	3,14	19,97	2,84
Total	**9 912,14**	**505,84**	**303,66**	**17,34**	**101,71**	**9,01**
Cartes de type « privatif »						
Paiements de proximité et sur automate	117,46	12,84	6,72	0,84	6,27	1,04
Paiements à distance hors Internet	1,82	0,15	nd	nd	nd	nd
Paiements à distance sur Internet	9,53	1,29	3,05	0,35	0,99	0,16
Retraits	3,41	0,31	nd	nd	nd	nd
Total	**132,22**	**14,58**	**9,77**	**1,20**	**7,26**	**1,20**
Total général	**10 044,35**	**520,42**	**313,43**	**18,54**	**108,97**	**10,20**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 2

Le marché des cartes de paiement en France en 2013 – Acquisition

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	7 688,46	332,48	170,65	11,79	65,17	7,80
Paiements à distance hors Internet	17,66	2,46	4,49	1,24	2,09	0,99
Paiements à distance sur Internet	709,69	53,40	29,67	3,72	10,51	1,90
Retraits	1 496,32	117,51	21,68	3,61	7,97	1,74
Total	**9 912,14**	**505,84**	**226,49**	**20,37**	**85,73**	**12,43**
Cartes de type « privatif »						
Paiements de proximité et sur automate	117,46	12,84	4,60	1,00	6,74	3,22
Paiements à distance hors Internet	1,82	0,15	nd	nd	nd	nd
Paiements à distance sur Internet	9,53	1,29	0,67	0,11	0,41	0,10
Retraits	3,41	0,31	nd	nd	0,27	0,11
Total	**132,22**	**14,58**	**5,26**	**1,11**	**7,43**	**3,44**
Total général	**10 044,35**	**520,42**	**231,76**	**21,48**	**93,16**	**15,86**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 3

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » en 2013 – 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	562,0	43 986,7	63,0	7 863,6	87,7	16 963,3
Cartes perdues ou volées	546,3	42 988,2	42,9	4 217,8	17,9	3 748,3
Cartes non parvenues	8,2	410,9	0,5	32,0	0,1	13,3
Cartes altérées ou contrefaites	2,9	163,0	7,5	1 484,5	56,4	10 356,3
Numéro de carte usurpé	4,3	411,3	10,4	1 853,3	11,8	2 567,7
Autres	0,3	13,3	1,7	275,9	1,5	277,6
Paiements à distance hors Internet	355,9	28 947,0	117,7	11 268,1	49,6	6 397,0
Cartes perdues ou volées	0,0	0,3	7,6	779,3	3,9	555,5
Cartes non parvenues	0,0	0,0	0,1	5,6	0,1	3,2
Cartes altérées ou contrefaites	0,0	0,1	37,0	2 791,1	9,9	1 706,1
Numéro de carte usurpé	355,9	28 946,6	72,8	7 662,1	33,4	4 034,3
Autres	0,0	0,0	0,3	30,0	2,4	97,9
Paiements à distance sur Internet	972,2	122 969,2	857,2	45 931,6	122,5	15 530,6
Cartes perdues ou volées	0,0	5,4	63,2	3 996,0	9,2	1 443,7
Cartes non parvenues	0,0	0,2	0,3	9,7	0,0	2,7
Cartes altérées ou contrefaites	0,0	3,3	94,2	5 906,9	19,9	2 532,8
Numéro de carte usurpé	972,2	122 958,9	698,3	35 941,8	93,1	11 523,0
Autres	0,0	1,5	1,2	77,2	0,2	28,5
Retraits	130,5	38 237,8	5,3	1 129,3	186,9	29 887,4
Cartes perdues ou volées	129,8	38 031,9	3,6	835,8	5,2	832,0
Cartes non parvenues	0,6	195,5	0,0	5,6	0,1	20,4
Cartes altérées ou contrefaites	0,0	1,5	1,4	242,6	172,1	27 468,5
Numéro de carte usurpé	0,1	8,9	0,1	9,5	1,5	223,4
Autres	0,0	0,0	0,2	35,9	7,9	1 343,1
Total	**2 020,6**	**234 140,8**	**1 043,3**	**66 192,7**	**446,7**	**68 778,3**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 4

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » en 2013 – Acquisition

(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	562,0	43 986,7	193,9	26 974,3	303,9	57 896,4
Cartes perdues ou volées	546,3	42 988,2	66,5	2 568,5	41,7	8 381,1
Cartes non parvenues	8,2	410,9	2,0	592,2	0,6	95,6
Cartes altérées ou contrefaites	2,9	163,0	16,0	1 404,9	101,9	17 801,0
Numéro de carte usurpé	4,3	411,3	107,8	22 066,0	158,0	31 167,8
Autres	0,3	13,3	1,7	342,6	1,6	450,9
Paiements à distance hors Internet	355,9	28 947,0	nd	nd	nd	nd
Cartes perdues ou volées	0,0	0,3	nd	nd	nd	nd
Cartes non parvenues	0,0	0,0	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,0	0,1	nd	nd	nd	nd
Numéro de carte usurpé	355,9	28 946,6	nd	nd	nd	nd
Autres	0,0	0,0	nd	nd	nd	nd
Paiements à distance sur Internet	972,2	122 969,2	nd	nd	nd	nd
Cartes perdues ou volées	0,0	5,4	nd	nd	nd	nd
Cartes non parvenues	0,0	0,2	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,0	3,3	nd	nd	nd	nd
Numéro de carte usurpé	972,2	122 958,9	nd	nd	nd	nd
Autres	0,0	1,5	nd	nd	nd	nd
Retraits	130,5	38 237,8	11,5	907,8	3,3	945,5
Cartes perdues ou volées	129,8	38 031,9	10,9	809,0	1,1	338,6
Cartes non parvenues	0,6	195,5	0,1	16,4	0,0	6,6
Cartes altérées ou contrefaites	0,0	1,5	0,4	60,4	2,0	569,0
Numéro de carte usurpé	0,1	8,9	0,1	18,2	0,1	30,4
Autres	0,0	0,0	0,0	3,8	0,0	0,8
Total	**2 020,6**	**234 140,8**	**205,4**	**27 882,1**	**307,1**	**58 841,9**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 5

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2013 – 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	4,23	1 771,38	0,66	303,12	3,77	777,65
Cartes perdues ou volées	0,92	319,18	0,09	36,98	0,55	182,14
Cartes non parvenues	0,94	286,93	0,12	52,58	0,02	18,07
Cartes altérées ou contrefaites	0,73	183,38	0,41	207,25	3,10	559,52
Numéro de carte usurpé	0,19	62,59	0,04	5,01	0,10	16,97
Autres	1,45	919,30	0,00	1,30	0,01	0,95
Paiements à distance hors Internet	0,26	265,62	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,03	14,20	nd	nd	nd	nd
Autres	0,24	251,42	nd	nd	nd	nd
Paiements à distance sur Internet	5,28	2 008,95	7,04	1 394,45	2,57	639,21
Cartes perdues ou volées	0,50	116,90	0,09	2,01	0,06	6,01
Cartes non parvenues	0,03	14,76	0,07	3,04	0,01	1,27
Cartes altérées ou contrefaites	0,14	18,31	0,15	7,67	0,11	20,66
Numéro de carte usurpé	4,18	1 576,17	6,70	1 360,63	2,35	602,56
Autres	0,42	282,80	0,04	21,10	0,03	8,72
Retraits	1,75	372,31	nd	nd	nd	nd
Cartes perdues ou volées	1,27	211,41	nd	nd	nd	nd
Cartes non parvenues	0,08	27,35	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,30	83,39	nd	nd	nd	nd
Numéro de carte usurpé	0,10	48,15	nd	nd	nd	nd
Autres	0,01	2,01	nd	nd	nd	nd
Total	**11,52**	**4 418,26**	**7,70**	**1 697,56**	**6,34**	**1 416,86**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 6

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2013 – Acquisition

(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	4,23	1 771,38	0,33	200,66	5,66	3 278,05
Cartes perdues ou volées	0,92	319,18	0,03	18,35	0,54	318,32
Cartes non parvenues	0,94	286,93	0,02	9,98	0,03	12,23
Cartes altérées ou contrefaites	0,73	183,38	0,17	87,80	4,63	2 675,63
Numéro de carte usurpé	0,19	62,59	0,06	15,01	0,23	125,01
Autres	1,45	919,30	0,04	69,53	0,22	146,86
Paiements à distance hors Internet	0,26	265,62	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,03	14,20	nd	nd	nd	nd
Autres	0,24	251,42	nd	nd	nd	nd
Paiements à distance sur Internet	5,28	2 008,95	2,82	741,61	2,82	741,61
Cartes perdues ou volées	0,50	116,90	0,16	66,70	0,16	66,70
Cartes non parvenues	0,03	14,76	0,01	9,15	0,01	9,15
Cartes altérées ou contrefaites	0,14	18,31	0,98	280,87	0,98	280,87
Numéro de carte usurpé	4,18	1 576,17	1,65	378,76	1,65	378,76
Autres	0,42	282,80	0,02	6,13	0,02	6,13
Retraits	1,75	372,31	nd	nd	nd	nd
Cartes perdues ou volées	1,27	211,41	nd	nd	nd	nd
Cartes non parvenues	0,08	27,35	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,30	83,39	nd	nd	nd	nd
Numéro de carte usurpé	0,10	48,15	nd	nd	nd	nd
Autres	0,01	2,01	nd	nd	Nd	nd
Total	**11,52**	**4 418,26**	**2,78**	**1 208,95**	**11,58**	**5 302,60**

Source : Observatoire de la sécurité des cartes de paiement

Définition et typologie de la fraude relative aux cartes de paiement

Définition de la fraude

À des fins de recensement statistique, l'Observatoire estime qu'il convient de considérer comme constitutif de fraude toute utilisation illégitime d'une carte de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation :

• ayant pour conséquence un préjudice pour le banquier teneur de compte qu'il s'agisse du banquier du porteur de la carte ou de celui de l'accepteur (commerçant, administration… pour son propre compte ou au sein d'un système de paiement [1]), le porteur, l'accepteur, l'émetteur, 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 ;

• quels que soient :
  – les moyens employés pour récupérer, sans motif légitime, les données ou le support de la carte (vol, détournement du support de la carte, des données physiques ou logiques, des données de personnalisation et/ou récupération du code secret, et/ou du cryptogramme, piratage de la piste magnétique et/ou de la puce…),

  – les modalités d'utilisation de la carte ou des données qui lui sont attachées (paiement ou retrait, en paiement de proximité ou à distance, par utilisation physique de la carte ou du numéro de carte, sur automate…),

  – la zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :
    - émetteur français et carte utilisée en France,
    - émetteur étranger dans l'espace SEPA et carte utilisée en France,
    - émetteur étranger hors de l'espace SEPA et carte utilisée en France,
    - émetteur français et carte utilisée à l'étranger dans l'espace SEPA,
    - émetteur français et carte utilisée à l'étranger hors de l'espace SEPA ;

  – le type de carte de paiement [2], y compris les porte-monnaie électroniques ;

• que le fraudeur soit un tiers, le banquier teneur de compte, le porteur de la carte lui-même (dans le cas par exemple d'une utilisation après déclaration de vol ou de perte, ou d'une dénonciation abusive de transactions), l'accepteur, l'émetteur, un assureur, un tiers de confiance…

1 Dans le cas d'Internet, l'accepteur peut être différent du fournisseur de service, ou d'un tiers de confiance (paiements, dons effectués par des internautes en soutien d'un site, d'une idéologie…).
2 Tel que défini à l'article L. 132-1 du *Code monétaire et financier* dans sa version antérieure au 1er novembre 2009.

Typologie de la fraude

L'Observatoire a par ailleurs défini une typologie de la fraude qui distingue les éléments suivants.

Les origines de fraude :

• carte perdue ou volée : le fraudeur utilise une carte de paiement suite à une perte ou à un vol ;

• carte non parvenue : la carte a été interceptée lors de son envoi à son titulaire légitime par l'émetteur. Ce type d'origine se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut moins facilement constater qu'un fraudeur est en possession d'une carte lui appartenant et où il met en jeu des vulnérabilités spécifiques aux procédures d'envoi des cartes ;

• carte falsifiée ou contrefaite : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation. La contrefaçon d'une carte suppose la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou une personne quant à sa qualité substantielle. Pour les paiements effectués sur automate de paiement, une telle carte, fabriquée par le fraudeur, supporte les données nécessaires à tromper le système. En commerce de proximité, une carte contrefaite est une carte fabriquée par un fraudeur, qui présente certaines sécurités (dont l'aspect visuel) d'une carte authentique, supporte les données d'une carte authentique et est destinée à tromper la vigilance d'un accepteur ;

• numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (voir le paragraphe sur les techniques de fraude ci-dessous) et utilisé en vente à distance ;

• numéro de carte non affecté : utilisation d'un PAN [3] cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance ;

• fractionnement du paiement : action qui consiste à scinder le paiement en vue de passer en dessous des plafonds fixés par l'émetteur.

Les techniques de fraude :

• *skimming* : technique qui consiste en la copie, dans un commerce de proximité ou dans des distributeurs automatiques, des pistes magnétiques d'une carte de paiement à l'aide d'un lecteur à mémoire appelé *skimmer*. Éventuellement, le code confidentiel est également capturé *de visu*, à l'aide d'une caméra ou encore par détournement du clavier numérique. Ces données seront inscrites ultérieurement sur les pistes magnétiques d'une carte contrefaite ;

• hameçonnage ou *phishing* : technique utilisée par les fraudeurs visant à obtenir des données personnelles, principalement par le biais de courriels non sollicités renvoyant les utilisateurs vers des sites frauduleux ayant l'apparence de sites de confiance ;

• ouverture frauduleuse de compte : ouverture d'un compte de référence en fournissant de fausses données personnelles ;

3 Personal Account Number.

• usurpation d'identité : actes frauduleux liés à un paiement par carte et supposant l'utilisation de l'identité d'une autre personne ;

• répudiation abusive : contestation par le porteur, de mauvaise foi, d'un ordre de paiement valide dont il est l'initiateur ;

• piratage d'automates de paiement ou de retrait : technique qui consiste à placer des dispositifs de duplication de cartes sur des automates de paiement ou des distributeurs automatiques de billets ;

• piratage de systèmes automatisés de données, de serveurs ou de réseaux : intrusion frauduleuse sur de tels systèmes ;

• moulinage : technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de cartes pour générer de tels numéros et effectuer des paiements.

Les types de paiement :

• paiement de proximité, réalisé au point de vente ou sur automate ;
• paiement à distance réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen ;
• retrait (retrait DAB ou autre type de retrait).

La répartition du préjudice entre :

• la banque du commerçant, acquéreur de la transaction ;
• la banque du porteur, émettrice de la carte ;
• le commerçant ;
• le porteur ;
• les éventuelles assurances ;
• et les autres types d'acteurs.

La zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :

• l'émetteur et l'acquéreur sont, tous deux, établis en France. On dira également, dans ce cas, que la transaction est nationale. Pour autant, pour les paiements à distance, le fraudeur peut opérer depuis l'étranger ;
• l'émetteur est établi en France et l'acquéreur est établi à l'étranger dans l'espace SEPA ;
• l'émetteur est établi en France et l'acquéreur est établi à l'étranger hors espace SEPA ;
• l'émetteur est établi à l'étranger dans l'espace SEPA et l'acquéreur est établi en France ;
• l'émetteur est établi à l'étranger hors espace SEPA et l'acquéreur est établi en France.

Le secteur d'activité du commerçant pour les paiements à distance :

- alimentation : épiceries, supermarchés, hypermarchés, … ;
- approvisionnement d'un compte, vente de particulier à particulier : sites de vente en ligne entre particuliers, … ;
- assurance ;
- commerce généraliste et semi-généraliste : textile/habillement, grand magasin, généraliste vente sur catalogue, vente privée, … ;
- équipement de la maison, ameublement, bricolage ;
- jeu en ligne ;
- produits techniques et culturels : matériel et logiciel informatiques, matériel photographique, livre, CD/DVD, … ;
- santé, beauté, hygiène ;
- services aux particuliers : hôtellerie, service de location, billetterie de spectacle, organisme caritatif, … ;
- services aux professionnels : matériel de bureau, service de messagerie, … ;
- téléphonie et communication : matériel et service de télécommunication/téléphonie mobile ;
- voyage, transport : ferroviaire, aérien, maritime ;
- divers.

Le *rapport de l'Observatoire de la sécurité des cartes de paiement* est en libre téléchargement sur le site internet de l'Observatoire (*www.observatoire-cartes.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 cartes de paiement se réserve le droit de suspendre le service de la diffusion et de restreindre le nombre de copies attribuées par personne.

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

Directeur de la publication
Denis Beau,
Directeur général des Opérations
Banque de France

Rédacteur en chef
Frédéric Hervo,
Directeur des Systèmes de paiement et Infrastructures de marché
Banque de France

Secrétariat de rédaction
Marcia Toma, Josiane Usseglio-Nanot

Réalisation
Direction de la Communication
de la Banque de France

Opérateurs PAO
Nicolas Besson, Pierre Bordenave, Angélique Brunelle, Alexandrine Dimouchy, Christian Heurtaux, François Lécuyer, Aurélien Lefèvre, Carine Otto, Isabelle Pasquier

Version papier
Observatoire de la sécurité des cartes 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-cartes.fr