2014 | 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 2014
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Monsieur le ministre de l'Économie,
de l'Industrie 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 douzième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2014, comprend 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 poursuite de la baisse du taux de fraude sur les paiements par carte sur internet témoigne des efforts réalisés par les émetteurs et les e-commerçants pour mieux sécuriser ces transactions.

Plus de 90 % des porteurs de carte sont ainsi équipés de dispositifs d'authentification renforcée. Chez les e-commerçants, le taux d'équipement est proche de 60 %, ce qui représente une hausse significative (43 % l'an passé), principalement due à une adoption du mode de sécurisation « 3D-Secure » chez les petits e-commerçants et la possibilité de déclencher une authentification sur la base d'une analyse de risques.

Le taux d'échec sur les transactions authentifiées est resté à un niveau équivalent à celui du taux d'échec des transactions non authentifiées, confirmant ainsi l'absence d'obstacle à l'adoption de ce type de dispositif de sécurisation pour les e-commerçants.

Dans ce contexte, l'Observatoire rappelle à l'ensemble des acteurs concernés que la généralisation des dispositifs d'authentification renforcée est également une priorité, tant de l'Eurosystème, que de l'Autorité bancaire européenne, dont les recommandations relatives à la sécurité des moyens de paiement sur internet entrent en vigueur au 1er août 2015.

2e partie : statistiques de fraude pour l'année 2014

Le taux de fraude sur les paiements et les retraits sur les cartes émises en France est resté stable en 2014 pour la deuxième année consécutive, à 0,069 %. En incluant les transactions des cartes émises dans d'autres pays, le taux de fraude global reste stable également, à 0,080 % pour la troisième année consécutive.

Cette stabilisation du taux de fraude global résulte toutefois de tendances contraires :

- *Pour la première fois depuis 2004, le montant de fraude sur les transactions nationales diminue à 235 millions d'euros (239 millions d'euros en 2013), alors même que le montant de transactions continue de progresser. Le taux de fraude sur les transactions nationales est ainsi en diminution, à 0,043 % (contre 0,046 % en 2013), de même que le taux de fraude sur les paiements de proximité (0,010 %, après 0,013 % en 2013).*

  Pour la troisième année consécutive, le taux de fraude sur les paiements à distance continue de se réduire, à 0,248 % (contre 0,269 % en 2013). Toutefois, dans un contexte de croissance soutenue du e-commerce, les montants de fraude sur les paiements à distance continuent d'augmenter. Les paiements à distance représentent toujours la majeure partie de la fraude en montant (66,5 %) alors qu'ils ne constituent que 11,6 % du montant total des paiements.

À ce titre, certains secteurs d'activité, notamment celui de la téléphonie et des communications, présentent des taux de fraude pour les transactions en ligne nettement supérieurs à l'ensemble des e-commerçants, appelant à une vigilance renforcée des acteurs concernés.

À l'inverse, le taux de fraude sur les retraits continue à progresser (0,034 %, après 0,033 % en 2013), dans un contexte où le piratage de distributeurs de billets et le vol de cartes avec code restent des malversations prisées des réseaux de fraude organisés.

Par ailleurs, les premières données statistiques relatives aux paiements en mode sans contact font ressortir un taux de fraude limité sur les neuf derniers mois de 2014, à 0,015 %, soit un niveau intermédiaire entre celui des paiements de proximité et celui des retraits aux distributeurs automatiques de billets. Cette fraude a presque exclusivement pour origine le vol ou la perte de la carte, confirmant ainsi l'analyse faite par l'Observatoire qu'un risque de fraude liée à la technologie sans contact demeure très limité.

- *La fraude sur les transactions internationales continue d'augmenter, à 266 millions d'euros (contre 231,3 millions en 2013), mais en raison d'une croissance forte de l'activité, le taux de fraude sur les transactions internationales est orienté à la baisse, à 0,456 %, après 0,480 % en 2013. Il reste toujours plus de dix fois supérieur à celui des transactions nationales. De ce fait, les transactions internationales représentent 41 % du montant total de la fraude sur les cartes émises en France, alors qu'elles ne comptent que pour 6 % de la valeur totale des transactions réalisées.*

  En particulier, les taux de fraude sur les paiements à distance de cartes françaises dans ou hors zone SEPA restent à des niveaux élevés (respectivement 0,910 % et 0,960 %), notamment sous l'effet d'une meilleure sécurisation des transactions à distance sur les sites français et donc d'un report des fraudeurs vers des sites situés à l'étranger. L'entrée en vigueur à l'été 2015 des orientations de l'Autorité bancaire européenne prévoyant la généralisation du recours à l'authentification renforcée des payeurs devrait permettre de lutter plus efficacement contre la fraude sur les paiements à distance dans la zone SEPA.

3e partie : travaux de veille technologique sur l'usage de la biométrie comme facteur d'authentification

Certains modes d'authentification reposant sur la biométrie, déjà utilisée quotidiennement par une part croissante du grand public, pourraient venir renforcer la sécurisation d'opérations de paiement par carte, qu'elles soient à distance ou de proximité, ou de retrait. De ce fait, l'Observatoire a souhaité faire un état des lieux de ces techniques d'authentification et de leurs conditions de mise en œuvre.

L'utilisation de techniques biométriques étant strictement encadrée en France par la loi Informatique et Libertés, l'Observatoire rappelle que leur application au sein de solutions de paiement requiert le dépôt d'une demande d'autorisation auprès de la CNIL.

L'Observatoire constate que les expérimentations menées en France visent en priorité à tester l'ergonomie des dispositifs biométriques. Avant tout déploiement à grande échelle, l'Observatoire estime nécessaire qu'une analyse des risques liés à l'usage de l'authentification biométrique soit conduite afin que le niveau de protection des solutions mises en œuvre soit au moins équivalent à celui offert par les techniques déjà en place (code confidentiel et carte à puce pour le paiement de proximité, code non rejouable pour le paiement à distance).

Par ailleurs, soulignant le manque d'éléments d'appréciation du niveau de sécurité des dispositifs biométriques par rapport aux technologies actuellement en œuvre (carte à puce, carte SIM des téléphones portables, etc.), l'Observatoire appelle les acteurs à développer des référentiels de sécurité permettant de qualifier les solutions proposées en prenant en compte l'ensemble de leurs composants et paramètres (matériels de capture de l'empreinte biométrique et de traitement, algorithmes, cas d'usage).

L'Observatoire appelle également les acteurs à être vigilants durant les phases d'expérimentation de solutions fondées sur la biométrie, la compromission d'empreintes biométriques utilisées par celles-ci pouvant mettre en cause le déploiement de solutions futures à plus grande échelle.

Enfin, du fait des limitations inhérentes à la biométrie et du manque de maturité de l'évaluation sécuritaire de ces dispositifs, l'Observatoire recommande de toujours conserver un moyen d'authentification alternatif capable de se substituer au dispositif biométrique.

4e partie : synthèse de la conférence « Les nouveaux moyens de paiement : de nouveaux enjeux de sécurité » du 22 octobre 2014

La Banque de France a organisé le 22 octobre 2014 à Paris, en collaboration avec la Banque centrale européenne, une conférence internationale sur les nouveaux défis en matière de sécurité des moyens de paiement. Cette journée a été l'occasion de développer un dialogue entre institutions européennes, autorités nationales et acteurs de marché autour de ces sujets. Trois grands axes qui conditionneront l'avenir des travaux sur la sécurité des moyens de paiement se sont ainsi dégagés des échanges.

En premier lieu, la coopération à la fois entre les différentes autorités concernées au niveau européen, au travers d'enceintes telles que le forum européen Secure Pay [1]*, mais aussi entre ces autorités et les nombreuses parties prenantes du marché des paiements (banques, entreprises, fournisseurs de solutions, consommateurs…), est apparue comme une réponse efficace au besoin d'un développement cohérent des exigences sécuritaires sur le marché européen.*

1 Le forum européen *SecuRe Pay*, coprésidé par la BCE et l'ABE, réunit les banques centrales et superviseurs bancaires nationaux sur les sujets relatifs à la sécurité des moyens de paiement scripturaux.

Ensuite, la prise en compte en permanence des évolutions du marché, dans un contexte où l'innovation fait évoluer rapidement les usages des consommateurs, doit faire partie intégrante du fonctionnement des autorités européennes. À ce titre, les travaux conduits au niveau du forum SecuRe Pay *et de l'Autorité bancaire européenne concernant la sécurité des paiements sur internet illustrent cette volonté d'investir les segments les plus innovants en matière de développement de services de paiement sûrs et efficaces.*

Enfin, dans un secteur en forte évolution, la recherche d'un équilibre entre innovation et sécurité est également un paramètre à intégrer dans l'action des autorités, qui doivent veiller à ce que les exigences règlementaires ne constituent pas une barrière au développement de nouveaux services. Les réflexions conduites dans le cadre de la révision de la directive sur les services de paiement, concernant en particulier l'encadrement des activités des tiers de paiement et de leurs conditions de sécurité, illustrent cette volonté de permettre l'ouverture du marché des paiements à l'innovation tout en maîtrisant les risques pour l'ensemble des acteurs et les consommateurs.

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

La fraude sur les paiements par carte sur internet 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 que l'Observatoire recommande, 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 des actions menées par l'Observatoire, la Banque de France et les initiatives au niveau européen pour promouvoir le renforcement de la sécurité des paiements sur internet (partie 2).

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

La multiplication des tentatives de fraude et attaques visant à compromettre des données ou des moyens de paiement oblige les acteurs à s'adapter en permanence aux évolutions des scénarios de fraude mis en œuvre et aux mesures déployées pour y répondre. Parmi celles-ci, la généralisation de l'authentification renforcée du porteur reste une priorité de l'Observatoire.

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

Ce suivi statistique, portant sur un périmètre de 58,8 millions de cartes de paiement et 39,6 milliards d'euros de paiements (dont 12,4 milliards sécurisés par le dispositif « 3D-Secure » [1]), permet de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification renforcée.

La neuvième campagne de collecte, qui portait sur la période du 1er novembre 2014 au 30 avril 2015, met en évidence trois principaux enseignements.

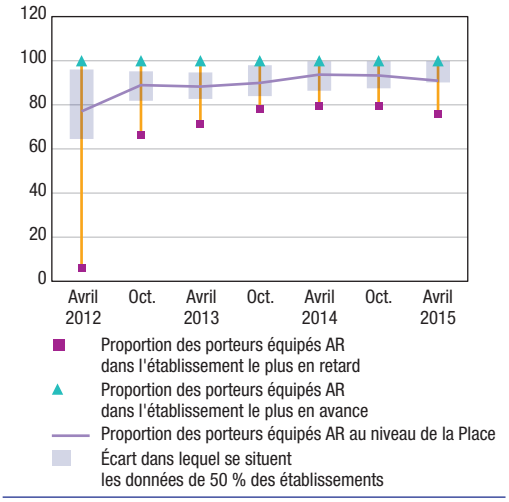
1|1 La quasi-totalité des porteurs est désormais équipée d'au moins un dispositif d'authentification renforcée

Le taux moyen de porteurs équipés d'au moins un dispositif d'authentification renforcée a fortement progressé sur les trois dernières années, passant de 77 % à plus de 90 %. La légère baisse en moyenne observée sur la dernière collecte (90,9 % en avril 2015,

Graphique 1

Distribution des taux d'équipement des porteurs d'un dispositif d'authentification renforcée (AR)

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

1 Protocole interbancaire de sécurisation des paiements par carte en ligne permettant l'authentification du porteur.

contre 93,3 % en octobre 2014) s'explique par la migration de la clientèle d'un grand émetteur de la Place vers un nouveau mode d'authentification forte.

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 OTP [2] reste toujours largement majoritaire.

1|2 Le taux d'échec [3] sur les transactions authentifiées de manière renforcée se rapproche de celui sur les transactions non authentifiées

L'Observatoire a pu constater l'évolution favorable du taux d'échec sur les paiements authentifiés au fil des collectes réalisées, passant de 18 % en 2011 à 14,6 % 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 du système « 3D-Secure » par de grands e-commerçants.

Ainsi, ce taux d'échec est même devenu en 2014 légèrement inférieur au taux d'échec sur les paiements non authentifiés, collecté par l'Observatoire depuis 2013, et qui se situe à 14,9 %. **L'Observatoire note ainsi qu'il se confirme que l'authentification renforcée du porteur, à chaque fois que cela est possible et pertinent, ne constitue pas un obstacle au développement du commerce électronique.**

1|3 Le recours à l'authentification *via* « 3D-Secure » continue à progresser, porté par un meilleur taux d'équipement des e-commerçants

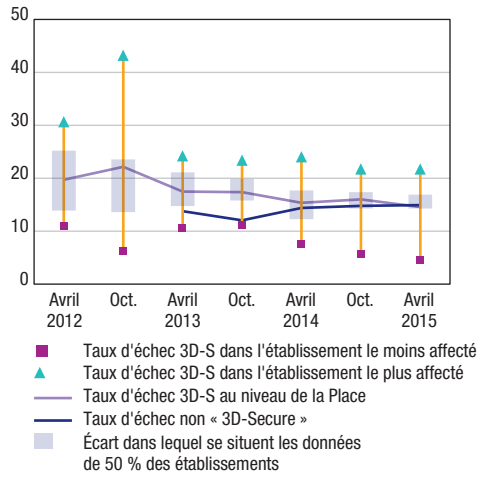
La part des transactions authentifiées en valeur progresse sur un an de 29,7 % à 31,3 % des montants. Cette évolution positive contribue à la diminution du taux de fraude des paiements à distance en 2014.

En outre, la proportion de commerçants équipés en dispositifs d'authentification renforcée progresse significativement, passant en un an de 43 % à 58 %.

Graphique 2

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

(en %)

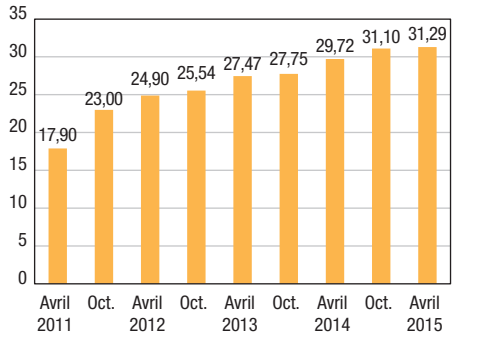


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 3

Part des paiements en ligne sécurisés par « 3D-Secure » (en montant)

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

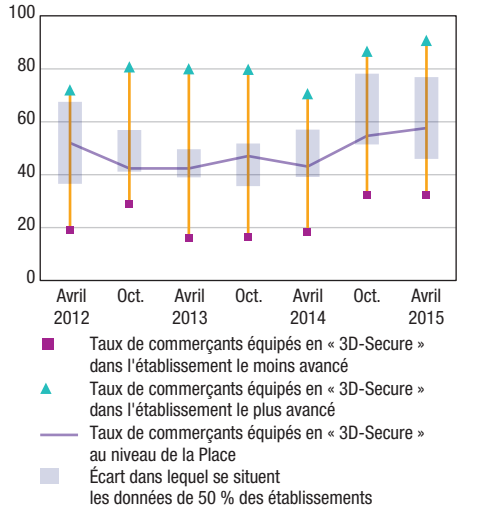
2 SMS « *One-Time Password* » : principe de réception par SMS d'un code unique à chaque transaction pour authentifier le porteur de la carte.

3 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 4

Distribution du taux d'équipement des e-commerçants en dispositif « 3D-Secure »

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

Cette hausse s'explique notamment par une adoption de ce mode de sécurisation des paiements chez les petits e-commerçants et la possibilité de déclencher une authentification « 3D-Secure » sur la base d'une analyse de risques.

2| Les actions menées par les instances nationales et européennes pour promouvoir le renforcement de la sécurité des paiements sur internet

2|1 Les actions menées par la Banque de France et l'Observatoire

La Banque de France a poursuivi son action de sensibilisation des e-commerçants et de leurs prestataires de services de paiement à la lutte contre la fraude, dans le prolongement des actions initiées en 2013 à la demande de l'Observatoire. Par ailleurs, la Banque de France a mis en place auprès des acteurs impliqués dans la chaîne du paiement un processus de remontée des incidents de production liés à l'étape d'authentification des porteurs. Ces informations visent à mieux identifier les points de faiblesse des dispositifs déployés conduisant le cas échéant à détériorer le taux de transformation [4] des paiements authentifiés.

L'Observatoire constate, sur l'exercice 2014, que la majorité des grands e-commerçants rencontrés a déployé des plans d'action visant à réduire le taux de fraude, en particulier au moyen de mécanismes d'authentification renforcée des porteurs. Cette démarche devrait faciliter la mise en œuvre en France des évolutions règlementaires européennes visant à renforcer la sécurité des paiements par internet.

2|2 L'action des autorités européennes

L'Autorité bancaire européenne (ABE) a publié en décembre 2014 une orientation sur la sécurité des paiements sur internet. Celles-ci, reprenant largement les recommandations émises par le forum *SecuRe Pay* en 2013, visent notamment à généraliser l'authentification forte du client en préconisant :

- d'une part, aux émetteurs de cartes de permettre l'authentification forte du titulaire de la carte ;

- d'autre part, aux prestataires de services de paiement d'exiger que leurs commerçants en ligne favorisent des solutions permettant à l'émetteur de procéder à une authentification forte du titulaire de la carte pour les opérations effectuées sur internet. L'ABE précise que l'utilisation de mesures alternatives d'authentification peut être envisagée pour des catégories prédéfinies d'opérations à faible risque, par exemple sur la base d'une analyse du risque inhérent à l'opération.

Les recommandations de l'ABE sur la sécurité des paiements par internet sont applicables à partir du 1er août 2015. Elles ont été incorporées au sein des cadres de surveillance de l'Eurosystème sur les moyens de paiement.

4 Le taux de transformation, ou taux de conversion, vise chez un commerçant en ligne à mesurer le nombre d'achats réalisés par rapport au nombre de visites reçues sur un site.

Le recours systématique à l'authentification renforcée pour les paiements par internet sera en outre pris en compte dans la révision de la directive sur les services de paiement (dite DSP2), dont la publication est prévue au second semestre 2015 et qui nécessitera une transposition en droit national [5].

2|3 Les Assises nationales des paiements ont reconnu le rôle de l'authentification renforcée pour développer des moyens de paiement faciles et sûrs à utiliser

Les Assises nationales des paiements, organisées sous l'égide du ministre des Finances et des Comptes publics, Michel Sapin, et du ministre de l'Économie, de l'Industrie et du Numérique, Emmanuel Macron, se sont tenues le 2 juin 2015. Elles visaient à définir les contours d'une stratégie nationale de modernisation des moyens de paiement avec pour objectifs, d'une part, de répondre aux besoins des utilisateurs en terme de rapidité, de sécurité et d'accessibilité des moyens de paiement, et, d'autre part, de développer l'usage de moyens de paiement innovants et la compétitivité de l'industrie nationale des paiements.

La généralisation des dispositifs d'authentification renforcée des payeurs lors de paiements à distance s'inscrit ainsi dans la perspective du développement de moyens de paiement faciles et sûrs à utiliser, au regard à la fois de la part très importante que représente la fraude sur les paiements à distance dans le total de la fraude constatée pour les paiements par carte, et de la dynamique de développement du commerce en ligne.

Les propositions formulées dans le cadre des travaux préparatoires aux Assises nationales des paiements préconisent notamment d'encourager les initiatives permettant une meilleure diffusion de l'authentification renforcée, en intensifiant les efforts de communication et d'éducation menés auprès des commerçants et des utilisateurs, et le développement de solutions d'authentification renforcée dites de « deuxième génération », dont certaines présentent l'avantage de ne pas nécessiter un équipement spécifique des commerçants en ligne ou par exemple fondées sur l'usage de la biométrie. L'avènement de ces dispositifs nouveaux viserait notamment à répondre aux préoccupations exprimées par les e-commerçants, en particulier au regard du fort développement des paiements par téléphone mobile et au manque d'ergonomie des solutions existantes sur ce type de terminal. À ce titre, les nouvelles solutions qui réussiront à s'imposer dans les prochaines années seront vraisemblablement celles qui allieront facilité d'utilisation et sécurité, tout en reposant sur des modèles économiques viables.

3| Conclusion

L'Observatoire appelle l'ensemble des acteurs du paiement à poursuivre le renforcement de la sécurité des paiements par internet. Au regard de l'augmentation significative de la part des sites d'e-commerce équipés (près de 60 % à avril 2015), l'Observatoire note que la généralisation des dispositifs d'authentification renforcée est bien amorcée mais doit rester une priorité, permettant de se conformer aux recommandations de l'Eurosystème et de l'Autorité bancaire européenne relatives à la sécurité des moyens de paiement sur internet, qui entrent en vigueur au 1er août 2015.

5 Voir précisions sur le dispositif réglementaire de la DSP2 au chapitre 4.

Statistiques de fraude pour 2014

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 2014 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 effectuée (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). Afin d'assurer une cohérence avec les chiffres et taux de fraude européens disponibles auprès de la BCE [1], les données concernant les seules cartes émises en France sont présentées séparément. Elles n'incluent donc pas, par construction, la fraude subie en France par des cartes émises dans d'autres pays et que l'Observatoire est en mesure de recenser. L'Observatoire publie par ailleurs cette année et pour la première fois des données partielles de fraude concernant les cartes de paiement sans contact. Enfin, en complément, une série d'indicateurs détaillés est présentée dans l'annexe 5 de ce rapport.

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 pour l'année 2014 portent ainsi sur :

- *558,7 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 71,0 millions de cartes de type « interbancaire » émises en France (dont 1,98 million de porte-monnaie électroniques et 30,6 millions de cartes sans contact) ;*
- *17,2 milliards d'euros de transactions réalisées (principalement en France) avec 14,6 millions de cartes de type « privatif » émises en France ;*
- *49,0 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».*

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 Cf. *Third report on card fraud*, février 2014, rapport disponible en anglais sur le site de la BCE : *https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html*

1| Vue d'ensemble

En 2014, le montant total de la fraude affectant les cartes de paiement françaises sur les transactions de paiement et de retrait réalisées en France et à l'étranger s'élève à 395,6 millions d'euros, en augmentation de 5,0 % par rapport à 2013, pour un montant total de transactions qui atteint 575,9 milliards d'euros, en augmentation de 4,9 % par rapport à 2013.

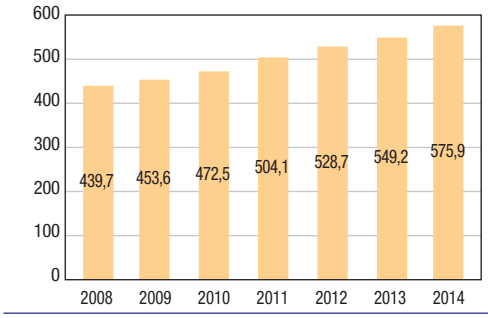
Compte tenu de ces éléments, le **taux de fraude sur les cartes de paiement françaises reste stable à 0,069 %** après trois années consécutives d'augmentation.

Le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2014 s'élève à 905 600 (+ 5,2 % par rapport à 2013).

Graphique 1

Évolution du montant des transactions des cartes françaises

(en milliards d'euros)

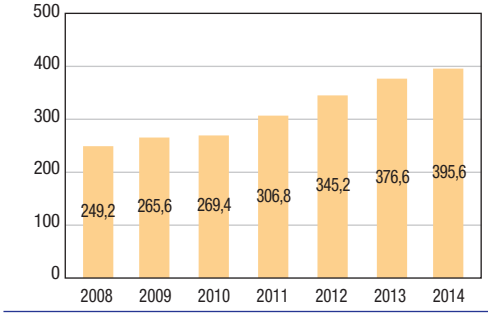


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 2

Évolution du montant de la fraude des cartes françaises

(en millions d'euros)

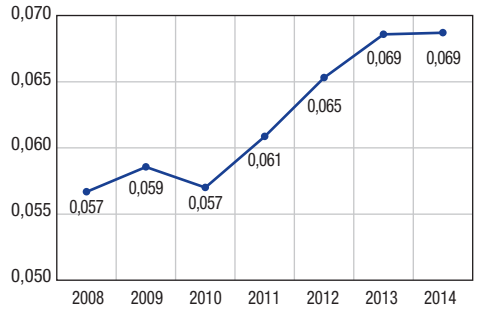


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 3

Évolution du taux de fraude des cartes françaises

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

En incluant également les transactions réalisées en France avec les cartes émises dans d'autres pays, le montant total de la fraude s'élève à 500,6 millions d'euros en 2014, en augmentation de 6,5 % par rapport à 2013, pour un montant total des transactions qui atteint 624,9 milliards d'euros, en croissance également de 6,5 % par rapport à 2013.

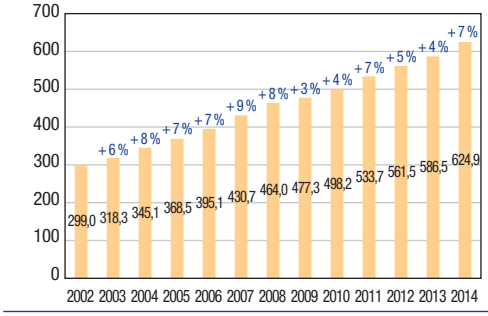
Compte tenu de ces éléments, le taux de fraude global sur les transactions traitées dans les systèmes français, comprenant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises et les paiements et les retraits réalisés en France avec des cartes étrangères, reste stable à 0,080 % pour la deuxième année consécutive après cinq années d'augmentation.

Le montant moyen d'une transaction frauduleuse est en diminution, pour s'établir à 112 euros, contre 116 euros en 2013.

Graphique 4

Évolution du montant des transactions traitées dans les systèmes français

(en milliards d'euros)

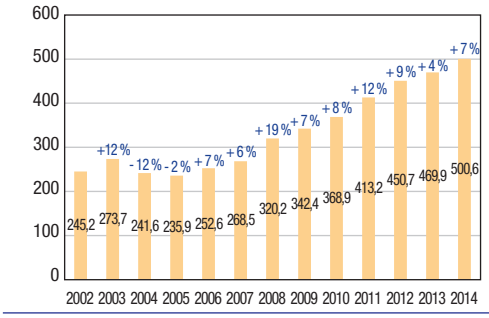


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 5

Évolution du montant de la fraude sur les transactions traitées dans les systèmes français

(en millions d'euros)



Source : Observatoire de la sécurité des cartes de paiement.

Graphique 6

Évolution du taux de fraude sur les transactions traitées dans les systèmes français (cartes françaises et étrangères)

(en %)

Source : Observatoire de la sécurité des cartes de paiement.

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 2014, niveau stable depuis deux années, après cinq années consécutives d'augmentation. Le taux de fraude pour les cartes de type « privatif » s'établit à 0,062 % en 2014 (contre 0,065 % en 2013), en diminution pour la troisième année consécutive après quatre années d'augmentation.

Tableau 1

Répartition de la fraude par type de carte

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

	2010	2011	2012	2013	2014
Cartes de type « interbancaire »	0,074	0,077	0,080	0,080	**0,080**
	(351,5)	(394,9)	(434,4)	(455,8)	**(486,4)**
Cartes de type « privatif »	0,080	0,083	0,076	0,065	**0,062**
	(17,4)	(18,3)	(16,3)	(14,0)	**(14,2)**
Total	0,074	0,077	0,080	0,080	**0,080**
	(368,9)	(413,2)	(450,7)	(469,9)	**(500,6)**

Source : Observatoire de la sécurité des cartes de paiement.

Pour les cartes de type « interbancaire », la valeur moyenne d'une transaction frauduleuse est de 112 euros, contre 122 euros en 2013. Pour les cartes de type « privatif », elle s'élève à 297 euros, contre 352 euros en 2013.

3| Répartition de la fraude par zone géographique

Le **montant de la fraude sur les transactions domestiques est en diminution pour la première fois depuis la création de l'Observatoire**. Il s'élève à 234,6 millions d'euros, pour un taux de fraude de 0,043 %, contre 238,6 millions d'euros et un taux de fraude de 0,046 % en 2013.

À l'inverse, le montant de la fraude sur les transactions internationales est en augmentation à 266,0 millions d'euros (+ 15,0 % par rapport à 2013) pour devenir sensiblement supérieur à celui de la fraude sur les transactions domestiques, alors que ces deux montants étaient restés proches ces trois dernières années. Le taux de fraude sur les transactions internationales, bien qu'en diminution notable en 2014 (0,316 %, contre 0,350 % en 2013), demeure toujours plus de sept fois supérieur au taux de fraude sur les transactions domestiques.

Ainsi les transactions internationales représentent 53,1 % du montant total de la fraude alors qu'elles ne comptent que **pour 13,5 % de la valeur totale des transactions**.

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

- pour les cartes françaises, le taux de fraude sur les transactions effectuées hors zone SEPA (0,636 %) est près de deux fois supérieur à celui des transactions effectuées au sein de la zone SEPA (0,374 %) ;

Tableau 2

Répartition de la fraude par zone géographique

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

	2010	2011	2012	2013	2014
Transactions domestiques	**0,036**	**0,044**	**0,045**	**0,046**	**0,043**
	(163,8)	**(211,5)**	**(226,4)**	**(238,6)**	**(234,6)**
Transactions internationales	**0,423**	**0,367**	**0,380**	**0,350**	**0,316**
	(205,0)	**(201,7)**	**(224,3)**	**(231,3)**	**(266,0)**
– dont carte française et accepteur hors SEPA	0,728	0,638	0,759	0,688	0,636
	(54,9)	(51,0)	(62,5)	(70,2)	(70,0)
– dont carte française et accepteur SEPA	0,331	0,255	0,316	0,366	0,374
	(50,6)	(44,3)	(56,3)	(67,9)	(91,0)
– dont carte étrangère hors SEPA et accepteur français	0,831	0,892	0,639	0,404	0,336
	(64,5)	(81,3)	(78,2)	(64,1)	(65,6)
– dont carte étrangère SEPA et accepteur français	0,195	0,122	0,132	0,135	0,134
	(35,0)	(25,1)	(27,3)	(29,1)	(39,3)
Total	**0,074**	**0,077**	**0,080**	**0,080**	**0,080**
	(368,9)	**(413,2)**	**(450,7)**	**(469,9)**	**(500,6)**

Source : Observatoire de la sécurité des cartes de paiement.

• pour les cartes émises dans d'autres pays que la France, le taux de fraude sur les transactions effectuées en France avec des cartes émises hors de la zone SEPA (0,336 %) est deux fois et demie supérieur à celui des cartes émises au sein de la zone SEPA (0,134 %).

Ces résultats récompensent les efforts réalisés depuis plusieurs années en Europe et, dans une moindre mesure et de façon plus tardive, dans le monde entier, pour migrer l'ensemble des cartes et des terminaux de paiement vers le standard EMV ; ils soulignent également, en France, l'amélioration de la détection des tentatives de fraude par contrefaçon de piste magnétique provenant de pays situés hors zone SEPA.

Dans ce contexte, les mesures incitatives annoncées par Visa, MasterCard, American Express et Discover (Diners Club International) visant à encourager l'adoption du standard EMV sur le plan international méritent d'être soulignées. En effet, la mise en œuvre par de nouveaux pays, d'un transfert de responsabilité de l'émetteur de la carte vers le commerçant en cas de fraude pour les points de vente qui n'auront pas migrés vers EMV, devrait fortement inciter à la fois les émetteurs à adopter rapidement ce standard pour toutes les nouvelles cartes émises et les commerçants à engager la migration de leurs terminaux. Il est ainsi prévu aux États-Unis que près de 500 millions de cartes soient renouvelées au standard EMV au cours de l'année 2015, soit environ la moitié du parc actuel.

4| Répartition de la fraude par type de transaction

La typologie de transaction de paiement par carte adoptée par l'Observatoire distingue trois types d'opérations :

• les paiements de proximité et sur automate, (réalisés au point de vente ou sur les automates de distribution de carburant, de billets de transport, de parking, etc.), y compris les paiements sans contact ;

• les paiements à distance (réalisés sur internet, par courrier ou par téléphone/fax) ;

• et les retraits.

Pour une meilleure lisibilité, les développements qui suivent distinguent les données des transactions domestiques des données des transactions internationales.

En ce qui concerne les transactions domestiques (cf. tableau 3), on observe que :

• le **taux de fraude sur les paiements de proximité et sur automate est en diminution à 0,010 %.** Ces paiements représentent 66 % du montant des transactions nationales pour seulement 16 % du montant de la fraude ;

• le **taux de fraude sur les retraits est en légère augmentation pour s'établir à 0,034 %**. Cette augmentation s'explique principalement par le nombre toujours élevé de piratages de distributeurs automatiques de billets (plus de 1 000 en 2014) et de points de vente (560 en 2014, soit trois fois plus de cas qu'en 2013), qui sont devenus des cibles privilégiées pour les réseaux de fraude organisée, ainsi que par un nombre toujours important de vols de carte avec code confidentiel.

Face à la confirmation de ces tendances observées depuis 2011, 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 également en diminution à 0,248 %** pour la troisième année consécutive.

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

Ainsi, **les paiements à distance, qui ne représentent que 11,6 % de la valeur des transactions domestiques, comptent pour plus de 66,5 % du montant de la fraude**.

Le niveau de la fraude sur les paiements à distance conduit l'Observatoire à renouveler ses recommandations visant au déploiement, par les e-commerçants, notamment ceux d'entre eux qui connaissent les montants de transactions frauduleuses les plus élevés, de dispositifs tels que « 3D-Secure » permettant l'authentification renforcée du porteur de la carte pour les paiements les plus risqués. L'entrée en vigueur à l'été 2015 des orientations de l'Autorité bancaire européenne relatives aux paiements sur internet viendra d'ailleurs appuyer ces recommandations (cf. chapitre 1 du présent rapport).

Tableau 3

Répartition du taux de fraude domestique par type de transaction

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

	2010	2011	2012	2013	2014
Paiements	0,041	0,049	0,049	0,050	0,046
	(137,3)	(177,8)	(190,0)	(199,9)	(193,0)
– dont paiements de proximité et sur automate	0,012	0,015	0,015	0,013	0,010
	(36,2)	(48,1)	(51,2)	(45,8)	(37,8)
– dont paiements à distance	0,262	0,321	0,299	0,269	0,248
	(101,1)	(129,6)	(138,8)	(154,2)	(155,9)
– dont par courrier/téléphone	*0,231*	*0,259*	*0,338*	*1,122*	*0,147*
	(27,3)	*(25,4)*	*(29,4)*	*(29,2)*	*(2,8 a)*
– dont sur internet	*0,276*	*0,341*	*0,290*	*0,229*	*0,251*
	(73,9)	*(104,2)*	*(109,4)*	*(125,0)*	*(153,0 a)*
Retraits	0,024	0,029	0,031	0,033	0,034
	(26,5)	(33,7)	(36,4)	(38,6)	(41,4)
Total	**0,036**	**0,044**	**0,045**	**0,046**	**0,043**
	(163,8)	**(211,5)**	**(226,4)**	**(238,6)**	**(234,6)**

a) La diminution très importante par rapport à 2013, du montant de la fraude sur les paiements à distance effectués par courrier ou par téléphone, et à l'inverse l'augmentation de celle sur les paiements sur internet, s'expliquent pour grande partie par une modification de la méthodologie statistique utilisée par le Groupement des Cartes Bancaires (CB). Cette modification, qui n'affecte pas le montant total de la fraude ni le taux de fraude des paiements à distance tous canaux confondus, impacte la répartition de celle-ci entre le canal internet et le canal courrier/téléphone. Une étude conduite par le Groupement CB a démontré qu'il était préférable d'affecter désormais au canal internet la fraude non qualifiée par les enseignes de commerce à distance, qui était auparavant affectée par défaut au canal courrier/téléphone. Sur le même sujet, on rappellera l'action similaire, conduite en 2013, qui avait également permis d'améliorer la qualité des données d'activité (voir le rapport annuel 2013 de l'Observatoire). L'Observatoire encourage à ce titre toutes les parties prenantes à poursuivre les actions visant à améliorer la qualité des données qui lui sont déclarées.

Source : Observatoire de la sécurité des cartes de paiement.

Encadré 2

Fraude aux paiements par carte sans contact

L'Observatoire a collecté, pour la première fois cette année, les données permettant d'évaluer le taux de fraude sur les paiements sans contact. Ainsi, sur l'ensemble de l'année 2014, 72,2 millions de paiements sans contact ont été enregistrés pour un montant total de 780,9 millions d'euros, soit un montant moyen de 11 euros par opération. Les données de fraude, quant à elles, sont collectées de manière exhaustive depuis le 1er avril 2014. Sur les neuf derniers mois de l'année 2014, 9 600 paiements frauduleux ont été recensés pour un montant total de 108 000 euros. Le taux de fraude sur les transactions sans contact peut être estimé à 0,015 % sur cette période, et s'établirait donc à un niveau intermédiaire entre le taux de fraude des paiements de proximité tous modes confondus (0,010 %), et celui des retraits (0,034 %).

La fraude aux paiements sans contact a pour origine quasi exclusive le vol ou la perte de la carte ; la technologie sans contact elle-même ne semble donc pas avoir présenté de faille exploitable pour les fraudeurs (de type écoute passive des données de carte lors d'une transaction, ou activation à distance de la carte dans des lieux publics, par exemple), confirmant ainsi l'analyse des risques conduite par l'Observatoire et publiée dans son rapport annuel 2012. En outre, la mise en place par les émetteurs de carte de plafonds sur le montant maximum d'une transaction unitaire (généralement fixé à 20 ou 25 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (généralement fixé à 100 euros), permet de limiter le préjudice subi en cas de perte ou de vol d'une carte.

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

Dans un contexte de fort développement du taux d'équipement des porteurs, avec plus de 30 millions de cartes disposant de la fonctionnalité de paiement sans contact en circulation à fin décembre 2014, l'Observatoire appelle les émetteurs à toute la vigilance nécessaire, et rappelle les engagements pris concernant la possibilité de désactiver la fonction sans contact des cartes, soit en mettant des étuis de protection [3] à la disposition des utilisateurs, soit en mettant en œuvre la désactivation à distance de la fonction sans contact [4], soit en permettant le remplacement, à la demande du porteur, d'une carte sans contact par une carte dépourvue de cette fonctionnalité.

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

1 *Voir détails en annexe 2.*
2 *Voir annexe 1 : une opération de paiement par carte en mode sans contact est en effet effectuée sans l'utilisation du dispositif personnalisé de sécurité de la carte (absence de saisie de code), ce qui signifie que même avant opposition suite à la perte ou vol du moyen de paiement, le porteur ne peut pas supporter de pertes liées à un paiement non autorisé.*
3 *Étuis de carte bloquant les ondes de communications de type NFC, permettant d'éviter toute activation non sollicitée de la carte.*
4 *La fonction sans contact est alors désactivée par l'exécution d'un script EMV sur la carte, qui est réalisée au moment de l'insertion dans un distributeur automatique de billets ou un terminal de paiement électronique.*

En ce qui concerne les transactions internationales (cf. tableaux 4), on remarque que la fraude sur les paiements à distance réalisés par les cartes françaises auprès des e-commerçants étrangers a très fortement augmenté en 2014 (104,5 millions d'euros, contre 81,2 millions d'euros en 2013). Ce phénomène 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 le report des fraudeurs vers des sites étrangers moins sécurisés.

On constate ainsi des taux de fraude sur les paiements à distance particulièrement élevés à la fois hors zone SEPA (0,960 %) et en zone SEPA (0,910 %). Le déploiement de dispositifs d'authentification renforcée, sous l'impulsion notamment des recommandations du forum européen *SecuRe Pay* sur la sécurité des moyens de paiement et des orientations de l'Autorité bancaire européenne (cf. chapitre 1) devrait toutefois permettre d'infirmer cette tendance en zone SEPA.

Enfin, on note la poursuite de la 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. On notera en particulier que le taux de fraude sur les retraits effectués en zone SEPA (0,033 %) est près de 25 fois inférieur à celui des retraits effectués hors zone SEPA (0,890 %), où la piste magnétique est encore très utilisée dans certains pays.

Tableau 4a

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

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

Carte française – Accepteur étranger hors SEPA	**2011**	**2012**	**2013**	**2014**
Paiements	0,561	0,687	0,547	0,532
	(30,5)	(37,8)	(40,3)	(41,7)
– dont paiements de proximité et sur automate	0,369	0,456	0,377	0,350
	(16,0)	(19,8)	(17,7)	(19,2)
– dont paiements à distance	1,320	1,551	0,848	0,960
	(14,5)	(18,0)	(22,6)	(22,5)
– dont par courrier/téléphone	*1,011*	*1,150*	*1,234*	*4,955*
	(3,1)	*(4,0)*	*(6,4)*	*(7,5)*
– dont sur internet	*1,440*	*1,720*	*0,755*	*0,682*
	(11,4)	*(14,1)*	*(16,2)*	*(14,9)*
Retraits	0,800	0,904	1,054	0,890
	(20,5)	(24,7)	(29,9)	(28,3)
Total	**0,638**	**0,759**	**0,688**	**0,636**
	(51,0)	**(62,5)**	**(70,2)**	**(70,0)**
Carte française – Accepteur étranger SEPA				
Paiements	0,300	0,372	0,434	0,434
	(43,1)	(55,3)	(66,8)	(89,8)
– dont paiements de proximité et sur automate	0,140	0,131	0,089	0,067
	(12,6)	(11,7)	(8,2)	(7,8)
– dont paiements à distance	0,571	0,735	0,937	0,910
	(30,5)	(43,6)	(58,6)	(82,0)
– dont par courrier/téléphone	*0,643*	*0,532*	*1,566*	*1,317*
	(5,6)	*(6,5)*	*(11,3)*	*(13,9)*
– dont sur internet	*0,557*	*0,788*	*0,856*	*0,856*
	(24,9)	*(37,1)*	*(47,3)*	*(68,1)*
Retraits	0,040	0,036	0,036	0,033
	(1,2)	(1,1)	(1,1)	(1,2)
Total	**0,255**	**0,316**	**0,366**	**0,374**
	(44,3)	**(56,3)**	**(67,9)**	**(91,0)**

Source : Observatoire de la sécurité des cartes de paiement.

Tableau 4b

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

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

Carte étrangère hors SEPA – Accepteur français	2011	2012	2013	2014
Paiements	1,056	0,735	0,451	0,380
	(80,7)	(77,7)	(63,2)	(65,0)
– dont paiements de proximité et sur automate	–	0,353	0,230	0,162
	(–)	(30,3)	(25,3)	(21,9)
– dont paiements à distance	–	2,378	1,268	1,213
	(–)	(47,4)	(37,9)	(43,1)
– dont par courrier/téléphone	–	*0,737*	*0,930*	*1,018*
	(–)	*(8,8)*	*(9,2)*	*(7,7)*
– dont sur internet	–	*4,833*	*1,436*	*1,265*
	(–)	*(38,6)*	*(28,7)*	*(35,4)*
Retraits	0,042	0,033	0,051	0,026
	(0,6)	(0,6)	(0,9)	(0,6)
Total	**0,892**	**0,639**	**0,404**	**0,336**
	(81,3)	**(78,2)**	**(64,1)**	**(65,6)**
Carte étrangère SEPA – Accepteur français				
Paiements	0,155	0,158	0,158	0,156
	(24,3)	(26,6)	(28,2)	(38,5)
– dont paiements de proximité et sur automate	–	0,046	0,039	0,026
	(–)	(5,7)	(4,9)	(5,1)
– dont paiements à distance	–	0,466	0,458	0,476
	(–)	(20,9)	(23,2)	(33,1)
– dont par courrier/téléphone	–	*0,216*	*0,308*	*0,397*
	(–)	*(3,8)*	*(3,8)*	*(4,8)*
– dont sur internet	–	*0,626*	*0,506*	*0,492*
	(–)	*(17,1)*	*(19,4)*	*(28,6)*
Retraits	0,017	0,017	0,025	0,018
	(0,8)	(0,7)	(0,9)	(0,9)
Total	**0,122**	**0,132**	**0,135**	**0,134**
	(25,1)	**(27,3)**	**(29,1)**	**(39,3)**

Source : Observatoire de la sécurité des cartes de paiement.

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 entre l'émetteur et le 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.

Encadré 3

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

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

Tableau

Ventilation de la fraude domestique 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
Services aux particuliers et aux professionnels	31,8	20,4
Voyage, transport	30,8	19,7
Commerce généraliste et semi-généraliste	29,5	18,9
Téléphonie et communication	26,7	17,1
Équipement de la maison, ameublement, bricolage	12,7	8,2
Produits techniques et culturels	8,0	5,1
Divers	6,0	3,8
Jeu en ligne	3,2	2,0
Alimentation	2,6	1,7
Approvisionnement d'un compte, vente de particulier à particulier	2,5	1,6
Santé, Beauté, Hygiène	1,8	1,1
Assurance	0,4	0,3
Total	**155,9**	**100,0**

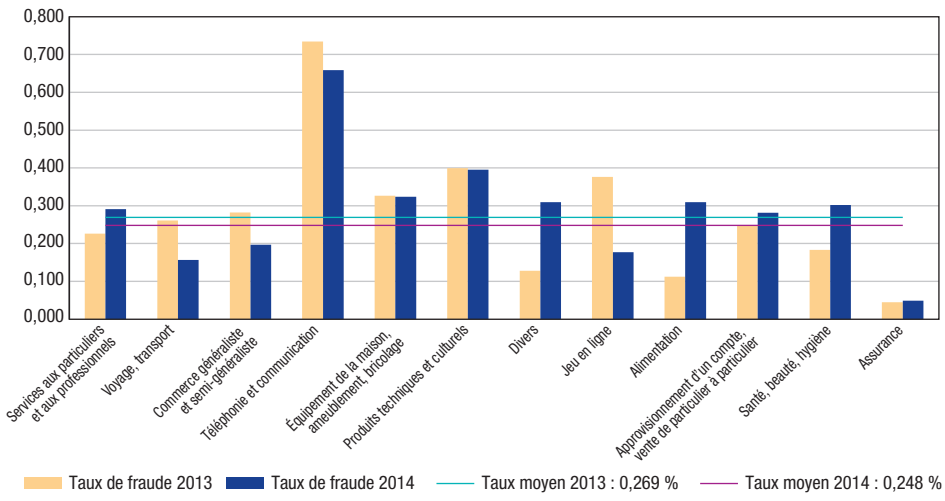
Les secteurs « Services aux particuliers et aux professionnels », « Voyage/transport », « Commerce généraliste et semi-généraliste » et « Téléphonie et communication » représentent 76 % du montant de la fraude en vente à distance, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, tels les « Produits techniques et culturels », qui comptent pour une plus faible part du total de la fraude, subissent toutefois une exposition élevée.

On note que les taux de fraude par secteur sont presque tous proches voire inférieurs au taux de fraude moyen, à l'exception notable du secteur « Téléphonie et communication » qui connaît de manière durable un taux de fraude très supérieur à la moyenne. L'Observatoire appelle tout particulièrement les acteurs de ce secteur à renforcer les mesures visant à lutter contre la fraude.

Graphique

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

(en %)

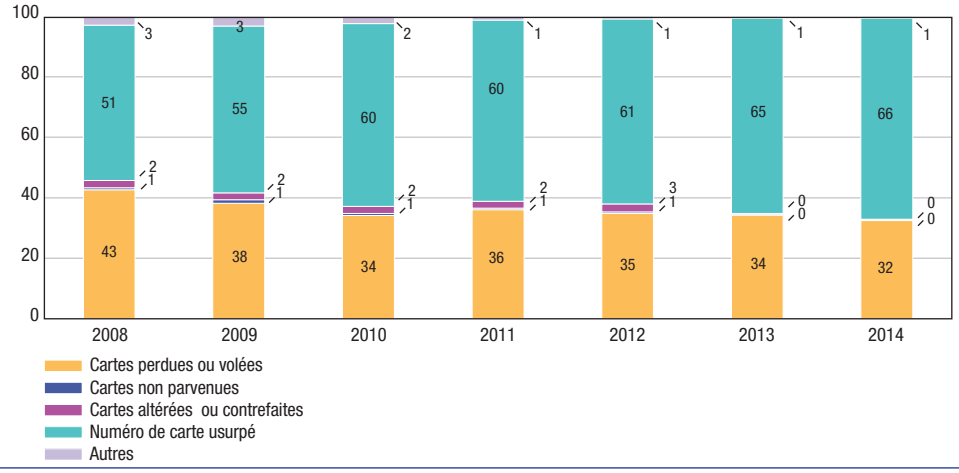


1 *Cf. annexe 6 pour une description des secteurs retenus.*

Graphique 7

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

Le graphique 7 indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements et n'inclut donc pas les retraits).

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux à distance reste la principale origine de la fraude (66,4 % des montants), en augmentation par rapport à 2013 (64,6 %).

La fraude liée aux pertes et vols de cartes représente toujours près du tiers de la fraude sur les transactions domestiques (32,5 %), mais sa part est en diminution continue (34,2 % en 2013) depuis trois années.

La contrefaçon de cartes n'est à l'origine que de 0,1 % des paiements domestiques frauduleux, en diminution sensible depuis plusieurs années (elle s'élevait à 2,6 % en 2011). Cette diminution s'explique principalement par l'adoption de technologies de cartes à puce par un nombre croissant de systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes [2].

Tableau 5

Répartition de la fraude domestique selon son origine et par type de carte en 2014

(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	76,3	32,5	75,6	32,8	0,7	17,3
Carte non parvenue	0,9	0,4	0,5	0,2	0,4	9,6
Carte altérée ou contrefaite	0,2	0,1	0,1	0,1	0,1	1,5
Numéro usurpé	155,9	66,4	154,3	66,9	1,6	40,0
Autres	1,4	0,6	0,1	0,1	1,3	31,6
Total	234,6	100,0	230,6	100,0	4,0	100,0

Source : Observatoire de la sécurité des cartes de paiement.

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

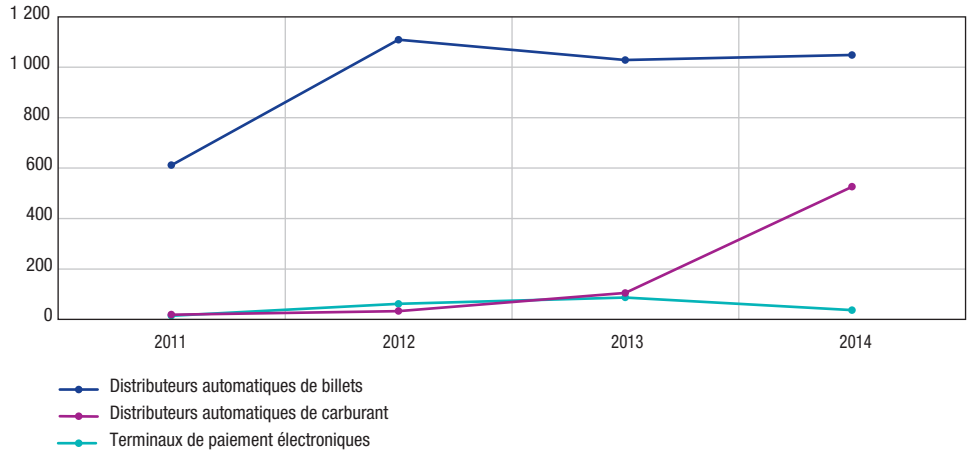
Encadré 4

Indicateurs des services de police et de gendarmerie

Pour l'année 2014, les services de police et de gendarmerie enregistrent à nouveau une baisse importante des interpellations pour fraude à la carte bancaire, faisant état de 45 personnes interpellées, contre 103 en 2013 et 122 en 2012, et près de 200 cas par an entre 2011 et 2009. Cette diminution est à rapprocher de la réponse pénale d'une sévérité croissante apportée à ces infractions, avec dès fin 2011 une chute très nette en France de l'activité liée aux officines de contrefaçon de cartes bancaires étrangères.

Le nombre de piratages de distributeurs automatiques de billets (DAB) reste stable avec 1 048 cas en 2014 (environ 1 000 cas par an depuis 2012, autour de 500 cas par an entre 2011 et 2006, 200 en 2005 et seulement 80 cas en 2004). À ceux-ci s'ajoutent 560 piratages ciblant les points de vente (contre 188 en 2013), dont 525 piratages de distributeurs automatiques de carburant (DAC) et 35 de terminaux de paiement chez les commerçants. Ces chiffres, qui demeurent élevés pour les DAB et qui sont en très nette augmentation pour les DAC, confirment dans les faits l'intérêt constant que portent les réseaux criminels à la collecte des données de carte. Ces données sont ensuite exploitées soit pour contrefaire des cartes à piste magnétique qui seront utilisées pour des paiements et des retraits à l'étranger, principalement dans les pays où la technologie de carte à puce EMV est peu déployée ; soit pour usurper des numéros de carte en paiement à distance, principalement sur les sites de e-commerce qui n'ont pas encore mis en œuvre l'authentification renforcée du porteur de la carte.

Graphique
Nombre d'infractions constatées sur les distributeurs et terminaux



Utilisation des techniques biométriques lors des opérations avec des cartes de paiement

1| Rappel du contexte

La sécurisation des opérations de paiement par carte repose notamment sur celle du canal d'initiation de l'ordre de paiement au moyen de l'authentification du payeur et du bénéficiaire. Si l'authentification du bénéficiaire présente des dispositifs éprouvés et pérennes (terminaux installés chez le commerçant, certificats numériques pour les paiements par internet, etc.), l'authentification du payeur pour les opérations de paiement par carte, principalement à distance mais aussi en proximité, demeure un enjeu fort. Dans ce contexte, le forum européen sur la sécurité des paiements de détail (forum *SecuRe Pay*) a publié en janvier 2013 un ensemble de recommandations et bonnes pratiques sur la sécurité des paiements par internet. Ces recommandations sont en cohérence avec les positions exprimées au sein de l'Observatoire, en particulier sur la mise en œuvre de l'authentification renforcée du porteur dans le contexte des paiements les plus risqués sur internet et, plus généralement, pour toutes les opérations sensibles (par exemple, lors de l'enregistrement d'une carte dans un portefeuille électronique).

Les recommandations du forum *SecuRe Pay* définissent l'authentification renforcée [1] 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.).*

Les éléments retenus 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 facteurs au moins doit être non rejouable et non reproductible (excepté pour la biométrie) ».

Certaines des techniques biométriques, déjà utilisées quotidiennement par une part croissante du grand public, pourraient venir renforcer la sécurisation d'opérations de paiement, qu'elles soient à distance ou de proximité, ou de retrait. La présente étude vise à dresser un état des lieux de l'utilisation des techniques biométriques lors des opérations de paiement ou de retrait par carte.

2| Définition de la biométrie et application à la carte de paiement

2|1 Définition

La Commission nationale de l'informatique et des libertés (CNIL), qui a pour mission principale de protéger les données personnelles dont les données biométriques font partie, définit la biométrie comme « *l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…). Elles se rapprochent ainsi de ce qui pourrait être défini comme un "identificateur unique universel", permettant de fait le traçage des individus* [2] ».

1 *Strong customer authentication.*
2 Cf. *http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/la-biometrie-sur-les-lieux-de-travail/*

Encadré

Point de vue de la CNIL sur l'authentification biométrique

L'utilisation de la biométrie en tant que facteur d'authentification pour accéder à des moyens de paiement, ou effectuer des opérations à distance, n'a jusqu'à présent été autorisée par la CNIL que dans le cadre d'expérimentations. L'objectif des autorisations temporaires accordées à ce titre est de mesurer l'intérêt porté à la solution par les clients, ainsi que la fiabilité de la technologie biométrique utilisée lorsqu'elle est couplée à un moyen de paiement sur internet.

L'expérimentation permet ainsi d'identifier les problèmes rencontrés afin de définir de nouvelles pistes d'amélioration. Les expérimentations ont une durée limitée au temps nécessaire à l'obtention de résultats concluants, et la CNIL exige qu'un bilan détaillé lui soit remis à leur issue. En outre, elles ne sont possibles que sur la base du volontariat, le système biométrique ne pouvant en tout état de cause être imposé aux utilisateurs.

Sur la base des bilans remis par les organismes et en tenant compte du paysage législatif en évolution tant au niveau national (proposition de loi visant à limiter l'usage des techniques biométriques en cours d'examen) qu'au niveau européen (proposition de règlement européen relatif à la protection des données), la CNIL s'attache à dégager des principes directeurs applicables aux dispositifs biométriques.

Bien que la biométrie « grand public » (hors du cadre professionnel) n'ait pas encore fait l'objet de cadre de référence, certaines constantes peuvent être soulignées. Le positionnement de la CNIL marque sa volonté de ne pas voir imposer la biométrie dans tous les usages du quotidien et de garantir aux personnes concernées la maîtrise de leurs données biométriques.

Ainsi, le recours à la biométrie ne saurait être le seul moyen d'accéder à un service mais doit pouvoir être utilisé de manière alternative à un autre moyen. L'utilisateur du service doit donc être en mesure de choisir une technique équivalente en termes de facilité d'usage, présentant les mêmes conditions d'accès que le dispositif biométrique (le choix d'une autre technologie ne doit pas avoir pour effet, par exemple, d'ajouter des contraintes telles qu'un délai, un coût, etc.).

De plus, la maîtrise par les personnes de leurs données biométriques est indéniablement réduite lorsque le gabarit [1] biométrique est stocké dans des serveurs distants et non sur un support placé sous le contrôle exclusif de la personne concernée. La compromission du support individuel emporte des conséquences bien moins importantes que celle d'une base centralisant plusieurs gabarits. Sur la base de ces premiers constats, la CNIL marque une préférence pour le stockage de la biométrie sur support individuel, placé sous le contrôle exclusif de la personne concernée.

Par ailleurs, la CNIL exige une information renforcée des personnes notamment sur le dispositif biométrique, son caractère facultatif (l'existence d'un dispositif alternatif), les modalités de stockage de la donnée ; les personnes doivent avoir la possibilité de revenir à tout moment sur leur choix et d'obtenir la suppression de leur gabarit biométrique le cas échéant.

Enfin, de nombreux acteurs sont susceptibles d'intervenir sur la chaîne de traitement liée à l'authentification biométrique (par exemple, que ce soit en fournissant/gérant le support de stockage des gabarits ou en proposant l'utilisation du facteur d'authentification biométrique). Une attention accrue est donc nécessaire pour clarifier la répartition des responsabilités et prendre en compte les règles de protection des données dès la conception des services concernés.

1 Ensemble des données biométriques servant de référence lors d'une authentification.

En France, les dispositifs de reconnaissance biométrique sont soumis à l'autorisation préalable de la CNIL. Concrètement, la mise en place et l'exploitation d'un tel système nécessitent le dépôt d'une demande d'autorisation ou d'une déclaration de conformité (suivant la finalité du traitement et le type d'empreinte biométrique) à la CNIL. Cette dernière option n'est aujourd'hui toutefois pas ouverte à la biométrie appliquée aux moyens de paiement, les cadres de référence proposés par la CNIL ne couvrant pas cette finalité.

La CNIL distingue plus particulièrement trois types de dispositifs par rapport à la caractéristique physique ou biologique utilisée :

• les dispositifs biométriques « à traces » : les empreintes digitales et palmaires. On les appelle « à traces » car les personnes les laissent à leur insu sur tous les objets qu'elles touchent. Le risque de ces techniques réside dans le fait que ces traces peuvent éventuellement être capturées et reproduites à l'insu des personnes (fabrication d'un faux doigt…) ;

• les dispositifs biométriques « sans traces » : le contour de la main, le réseau veineux des doigts de la main ;

• les dispositifs biométriques dits « intermédiaires » : la voix, l'iris de l'œil, la forme du visage.

Même si ce découpage reste d'actualité, les moyens les plus récents de capture et la prolifération d'informations personnelles – volontaires ou non – sur internet (photos en haute résolution, enregistrements vidéo, etc.) permettent de reconstituer l'empreinte biométrique de ces différents types de dispositifs et tendent par conséquent à en effacer les frontières ; tous les dispositifs tendent ainsi à devenir progressivement « à traces ».

Dans la définition d'un dispositif biométrique, il est nécessaire de distinguer deux modes d'utilisation :

• en identification, l'empreinte biométrique est comparée à l'ensemble des empreintes de référence pour déterminer l'identité du porteur ;

• en authentification, l'identité du porteur légitime est déjà connue et l'empreinte biométrique est comparée uniquement à son empreinte de référence pour s'assurer de son identité.

Dans le domaine des opérations par cartes de paiement, c'est la fourniture de la carte de paiement – ou des données de la carte de paiement – qui permet d'identifier le porteur ; le dispositif biométrique contribue ensuite à l'authentification de ce dernier.

2|2 Application à la carte de paiement

Un nombre croissant de constructeurs de *smartphones* et d'ordinateurs portables ont intégré des dispositifs de reconnaissance biométrique, reposant principalement sur la lecture de l'empreinte digitale (voir le *Rapport annuel* 2013 de l'Observatoire). La commercialisation à grande échelle de ces nouveaux modèles concourt à la familiarisation des techniques biométriques auprès du public et présente une opportunité de déploiement et d'utilisation des technologies biométriques dans le domaine des paiements.

2|2|1 Quels cas d'usage de la biométrie pour les paiements par carte ?

Dans le cadre des **paiements à distance**, l'authentification renforcée du porteur par code à usage unique n'est aujourd'hui acquise que pour un peu plus de 30 % des paiements par carte. Dans le cas de nouveaux modes d'initiation tels les paiements mobiles ou les portefeuilles électroniques, l'authentification du porteur repose couramment sur l'usage d'un mot de passe. Bien que plus complexe qu'un code confidentiel et pouvant être régulièrement renouvelé, il demeure néanmoins toujours rejouable et est généralement saisi sur des claviers standards d'ordinateur ou de téléphone qui ne présentent pas le même niveau de protection que les claviers agréés des automates ou des terminaux de paiement. Les techniques biométriques pourraient fournir une solution complémentaire permettant de renforcer l'authentification du porteur.

Dans le cadre des **paiements de proximité**, l'utilisation d'une carte à puce et du code confidentiel offre un niveau de sécurité élevé. Le taux de fraude mesuré par l'Observatoire sur ce type de transaction ces dernières années est de l'ordre de 0,015 %, soit environ vingt fois moins que celui mesuré en vente à distance.

Cependant, le code confidentiel reste rejouable : un fraudeur qui en prendrait connaissance lors d'une opération de retrait ou de paiement, *via* la compromission de l'automate bancaire, du terminal ou de l'automate de paiement ou, plus simplement, visuellement, pourrait le réutiliser à l'occasion d'une fraude future en cas de vol ou de contrefaçon de la carte. Les claviers des automates bancaires, des terminaux et automates de paiement sont soumis à des règles d'agrément visant à limiter les risques de compromission. L'interception visuelle, par le fraudeur lui-même ou à l'aide d'une caméra miniaturisée, lors de la frappe du code confidentiel, demeure plus difficile à maîtriser et repose principalement sur la vigilance du porteur.

Les techniques biométriques pourraient fournir une solution complémentaire réduisant le risque en cas de compromission du code confidentiel, ou une solution alternative dans certains cas d'usage en réduisant l'utilisation du code confidentiel et son risque de compromission.

2|2|2 Les limitations du recours à la biométrie

La biométrie revêt un aspect pratique certain lorsqu'elle permet de simplifier la procédure d'initiation d'un paiement, d'en raccourcir la durée, voire de pouvoir répondre à la demande des personnes qui rencontrent des difficultés à mémoriser un code confidentiel. Cependant, l'emploi de la biométrie soulève plusieurs problématiques spécifiques :

- le caractère définitif de la compromission d'une empreinte : la compromission d'une empreinte biométrique (par exemple, une empreinte digitale) ne peut généralement plus donner lieu à la génération d'une nouvelle empreinte pour le même élément physique, contrairement à ce qui peut être fait avec un support physique (carte à puce, *token*, etc.) ou un code confidentiel que l'on peut facilement renouveler. Il demeure toutefois possible de changer par exemple de doigt, de main ou d'œil mais avec un nombre d'occurrences qui reste au final toujours limité ;

- les limites à l'universalité du dispositif biométrique : certaines personnes peuvent se trouver dans l'incapacité d'utiliser leurs empreintes biométriques de manière temporaire (usure, salissure, blessure, etc.) voire permanente (caractéristiques physiques incompatibles avec le dispositif biométrique, handicap, etc.) ;

- la difficulté à définir le réglage du niveau de tolérance du dispositif biométrique qui influencera le taux d'erreur : deux taux sont principalement mesurés en biométrie, ceux de faux rejets (*False Rejection Rate*, FRR) et de fausses acceptations (*False Acceptation Rate*, FAR) parce qu'ils traduisent respectivement le niveau d'exigence et celui de permissivité du dispositif envers l'empreinte biométrique prise et comparée à l'empreinte de référence. Ainsi des coupures, brûlures aux doigts, voire la simple transpiration, peuvent conduire à un rejet, de la même manière que du bruit ambiant peut altérer une analyse vocale. Ces taux peuvent varier de manière plus ou moins importante selon la caractéristique physique analysée, la qualité du lecteur biométrique et l'algorithme utilisé. La difficulté vient du fait que si un réglage du niveau de tolérance est possible, ces taux évoluent généralement de manière opposée. Il n'existe aucune donnée publique concernant les taux de faux rejets et ceux de fausses acceptations pour les dispositifs actuellement disponibles, ce qui rend difficile la comparaison avec l'usage du code confidentiel. Ce dernier présente un taux de faux rejets proche de zéro (le bon code n'est jamais rejeté et les claviers des terminaux de paiement et des distributeurs sont conçus pour limiter le risque d'erreur de frappe) et un taux de fausses acceptations de 3 sur 10 000 [3].

Enfin, outre les problématiques techniques évoquées ci-dessus, la réticence potentielle du public à recourir aux dispositifs biométriques pour des raisons d'éthique ou l'absence de confiance dans le dispositif global peuvent constituer d'autres freins au développement de la biométrie. Concernant le premier frein, le recours à un dispositif biométrique est encadré par la CNIL qui contrôle le bien-fondé de la solution proposée. Pour le second frein, la perception de la robustesse des dispositifs biométriques aux yeux du

3 Pour un code PIN à 4 chiffres et 3 tentatives autorisées avant le blocage de la carte.

grand public pourrait être affectée par l'actualité, par exemple en cas de découverte de nouvelles techniques d'attaque ne remettant pas en cause la fiabilité des dispositifs mais faisant l'objet d'une large médiatisation (démonstration en conditions de laboratoire, etc.). Or le succès d'un moyen de paiement réside autant dans la perception de sa sécurité que dans sa sécurité réelle.

2|2|3 Les standards existants

Les expériences en cours s'appuient sur des dispositifs prioritaires ou sur des normes déjà établies qui ont généralement pour origine le domaine du contrôle d'accès. L'ISO (*International Organization for Standardization*) fait notamment référence à la biométrie dans plusieurs de ses publications [4] sur les aspects suivants :

- description détaillée du point caractéristique du doigt, direction et type ;
- conditions de prise de vues pour données d'image de la face ;
- interface de programmation d'applications biométriques ;
- cadre de formats d'échange biométriques communs ;
- méthodologie d'essai de conformité et précisions concernant les défauts ;
- essais et rapports de performance biométriques ;
- essais des mises en œuvre biométriques multimodales.

Cependant, ces normes visent principalement à assurer l'interopérabilité entre les différents composants constituant les dispositifs biométriques (capteurs, algorithmes…).

Les premières évaluations sécuritaires, conduites à partir de 2008, se sont appuyées sur les Critères Communs pour qualifier des dispositifs ou lecteurs biométriques ; toutefois, seuls trois produits ont reçu à ce jour une certification [5], laquelle ne s'avère de surcroît pas suffisante pour les paiements par carte [6]. Plusieurs acteurs du domaine de la biométrie se sont regroupés en association (*Biometrics Alliance Initiative*, BAI) pour définir un processus de tests, de certification et d'habilitation permettant de garantir un niveau de sécurité en adéquation avec les besoins et normes internationales, notamment bancaires, ainsi que les procédures de test qui en découlent. Le projet BEAT (*Biometrics Evaluation And Testing*), soutenu par la Commission européenne, a notamment pour but de mettre en place le cadre d'un standard opérationnel d'évaluation pour les technologies biométriques.

EMV Co, qui regroupe les principaux systèmes de paiement par carte (Visa, MasterCard, American Express, Discover, JCB et Union Pay) étudie l'utilisation des techniques biométriques en tant qu'alternative à la saisie du code confidentiel [7] dans le cadre des travaux menés par le « *Card and Terminal Working Group* ».

En France, le Groupement des Cartes Bancaires a prévu d'intégrer la biométrie dans son référentiel sur l'authentification (disponible courant 2015) et de définir des cas d'usage possible en fonction du niveau de résistance intrinsèque aux attaques mesuré lors d'évaluations sécuritaires.

Enfin, plusieurs parties prenantes du domaine des paiements ont fondé en 2013 une association, *Natural Security Alliance*, pour promouvoir l'utilisation de la biométrie et développer des standards dans le domaine.

4 Notamment dans les normes suivantes : ISO/IEC 19784, 19785, 19794 et 19795.
5 Cf. *http://www.ssi.gouv.fr/administration/glossaire/c/*
6 Le profil de protection mis en œuvre relève du niveau de sécurité EAL 2 (avec résistance basique aux attaques) alors que le niveau EAL 4+ (avec résistance élevée aux attaques) est requis pour les systèmes de paiement par carte.
7 À noter que Visa, MasterCard et Discover sont aussi membres de l'Alliance FIDO (*Fast IDentity Online*), un consortium industriel lancé en février 2013 qui développe des spécifications afin de simplifier et de renforcer l'authentification lors des transactions en ligne et ainsi développer une alternative viable aux mots de passe.

3| État des lieux des dispositifs biométriques utilisés pour des opérations de paiement par carte

3|1 Étapes préliminaires à la mise en œuvre d'un dispositif biométrique

L'utilisation d'un dispositif biométrique pour accéder à un service nécessite de suivre plusieurs étapes qui sont communes à tous les types d'empreinte biométrique.

3|1|1 L'enrôlement des utilisateurs

Chaque utilisateur doit suivre une procédure permettant de capturer une empreinte de référence qui servira par la suite à le reconnaître. Par exemple, dans le cas d'un dispositif fondé sur la reconnaissance de l'empreinte digitale, cette étape consistera en une première prise d'empreinte qui pourra être multiple [8] pour en assurer une meilleure qualité.

Cette étape peut être réalisée dans un environnement sécurisé et contrôlé comme dans une agence bancaire ou dans un environnement banalisé, ou sur un

Encadré

Exemples de fonctionnement d'un dispositif de reconnaissance d'empreinte digitale appliqué au paiement par carte

Enrôlement des utilisateurs et enregistrement des empreintes de référence

	Cas n° 1 – Enregistrement sur un support local détenu par l'usager (exemple : *smartphone*)	Cas n° 2 – Enregistrement sur un serveur distant depuis une agence commerciale
1) Mise en relation	Installation d'une application dédiée ou connexion au service web dédié 	Entrée dans une agence 
2) Identification de l'utilisateur	Saisie des informations relatives au service par le porteur (informations utilisateur, informations carte)	Communication des informations utilisateur/fourniture de pièces justificatives (contrat, carte d'identité…)
3) Prise de l'empreinte de référence		
4) Enregistrement de l'empreinte de référence	Enregistrement local 	Enregistrement sur serveur distant 

8 Plusieurs doigts et plusieurs prises d'empreinte pour chaque doigt.

Authentification de l'utilisateur au moment d'un paiement de proximité
(exemple, cas sans saisie du code confidentiel)

équipement personnel tel que le *smartphone* de l'utilisateur lui-même.

3|1|2 Le stockage des empreintes de référence des utilisateurs

Les empreintes de référence sont stockées pour permettre au dispositif de comparer l'empreinte prise avec la ou les empreinte(s) de référence.

Ce stockage peut être centralisé sur un site qui contiendra les empreintes de référence de tous les utilisateurs du service, ou bien assuré localement sur un support propre à chaque utilisateur comme la puce d'une carte de paiement, d'un téléphone portable ou sur un *token* sécurisé. Le stockage local sécurisé des données de l'empreinte biométrique est généralement privilégié car il limite le risque d'une compromission massive d'empreintes en cas d'intrusion dans le dispositif de stockage centralisé. Cependant, certains types de biométrie, comme la biométrie vocale par exemple, peuvent exiger une puissance de calcul importante que les matériels portatifs actuels (par exemple, *smartphones*) ne sont pas encore en mesure de fournir ; un traitement centralisé s'avère alors nécessaire.

3|1|3 L'accès au service conditionné par le dispositif biométrique

L'accès au service suppose une première étape d'identification, qui est similaire à celle d'un dispositif

de paiement « traditionnel » : introduction de la carte dans un terminal, approche d'une borne NFC, saisie d'un identifiant ou du numéro de la carte… La lecture de l'empreinte biométrique vient ensuite, selon les cas, se substituer à l'authentifiant habituel (saisie du code confidentiel ou d'un mot de passe, recours à une authentification « 3D-Secure »...) ou le compléter. Enfin, l'empreinte du porteur est comparée à l'empreinte de référence, ce qui suppose l'accès par le dispositif de paiement au support de stockage, par connexion locale ou internet selon la nature de ce dernier.

3|2 Apport possible de l'authentification biométrique par rapport aux dispositifs existants

Le dispositif biométrique peut être mis en place pour renforcer un dispositif d'authentification existant soit en tant que dispositif complémentaire, c'est-à-dire en ajoutant un contrôle supplémentaire dans le processus d'authentification du porteur (par exemple, en ajoutant la reconnaissance d'une empreinte digitale à la saisie d'un mot de passe ou d'un code confidentiel), soit en tant que dispositif alternatif, c'est-à-dire en se substituant à un dispositif d'authentification existant (par exemple, saisie d'une empreinte biométrique à la place d'un code confidentiel).

En **utilisation complémentaire**, l'ajout d'un facteur d'authentification biométrique vise à renforcer le niveau de sécurité global d'un dispositif existant en rendant plus difficile l'initiation de paiements frauduleux. Par exemple, la biométrie peut contribuer à renforcer la sécurité d'un paiement sans contact de faible montant, pour lequel la saisie du code confidentiel de la carte n'est pas requise, sans avoir d'impact significatif sur la rapidité du processus d'initiation du paiement. Dans ce mode d'utilisation, le niveau de sécurité offert ne peut être que supérieur à celui du dispositif initial ; toutefois, le risque de compromission des empreintes, inhérent à tout dispositif biométrique, est un risque supplémentaire à prendre en considération. L'authentification biométrique pourra aussi être utilisée en tant que facteur complémentaire à la frappe du code confidentiel pour sécuriser les paiements, par exemple de montants élevés, que l'analyse des risques aura qualifiés comme plus risqués.

En **utilisation alternative**, la substitution d'un facteur d'authentification existant par une reconnaissance biométrique peut également renforcer la sécurité des paiements par carte lorsqu'elle permet de réduire les risques de compromission du dispositif remplacé. Par exemple, l'utilisation de l'authentification biométrique en remplacement de la saisie du code confidentiel de la carte peut dans certains cas d'usage réduire les risques de compromission du code confidentiel (exemple des distributeurs automatiques de carburant). Dans ce mode d'utilisation alternative, le niveau de sécurité de la solution reposera principalement sur celui du dispositif biométrique, et ne tirera pas bénéfice de la protection offerte par les dispositifs remplacés (code confidentiel, « 3D-Secure »...).

3|3 Application au paiement à distance

Les expérimentations de dispositifs biométriques en paiement à distance les plus développées reposent sur la reconnaissance de la voix ou des empreintes digitales. Ces expérimentations s'appuient sur les téléphones des utilisateurs pour ajouter une phase d'authentification du porteur et ainsi améliorer la sécurité des opérations à distance.

Ainsi, TalkToPay notamment en France et VoicePay au Royaume-Uni, font reposer le service d'authentification renforcée sur la possession du téléphone fixe ou mobile enrôlé dans le système et sur la reconnaissance vocale du client. Lors du paiement à distance, l'utilisateur reçoit un appel vocal qui lui permet de s'authentifier. Ce type de solution, qui repose uniquement sur la téléphonie vocale, présente l'avantage de fonctionner avec tout type de téléphone fixe ou mobile.

Les solutions s'appuyant sur la reconnaissance des empreintes digitales visent à tirer bénéfice du lecteur d'empreinte que plusieurs constructeurs de *smartphones* intègrent désormais dans leurs modèles, dans le but premier de sécuriser l'accès au mobile, mais également de permettre une utilisation par des services additionnels. On pourra citer par exemple l'application PayPal disponible sur les modèles Galaxy S5 de Samsung qui permet de payer avec son compte de monnaie électronique en s'authentifiant à l'aide de son empreinte digitale, ou la solution

Apple Pay disponible aux États-Unis sur les derniers modèles iPhone d'Apple et qui permet de donner son consentement lors d'un achat par carte sur internet par la lecture de son empreinte digitale. Dans ces cas de figure, la lecture de l'empreinte se substitue généralement à la saisie d'un mot de passe.

3|4 Application au paiement de proximité

Les paiements de proximité bénéficiant déjà d'un niveau de sécurité élevé, la biométrie est recherchée pour son ergonomie et la rapidité de son exécution. Ainsi, de grandes enseignes pourraient enrôler leurs clients et les faire payer par simple lecture biométrique, déclenchant dans un second temps un paiement par carte ou tout autre moyen de paiement préalablement enregistré. Dans ce cas de figure, la biométrie est utilisée comme alternative aux dispositifs d'authentification traditionnels reposant sur la saisie du code confidentiel, comme facteur de simplification et d'accélération du passage en caisse. Ce cas d'usage nécessite de déployer des terminaux de paiement électronique équipés et de former les commerçants au fonctionnement de ces équipements.

Les expérimentations dans ce domaine ont principalement mis en œuvre la reconnaissance d'empreinte digitale :

- en s'appuyant sur les fonctionnalités intégrées aux *smartphones* de dernière génération dotés de lecteurs d'empreintes digitales : le terminal de paiement interagit dans ce cas avec le *smartphone* dans lequel les références de la carte de paiement ont été préalablement enrôlées, la connexion avec le terminal pouvant être établie *via* un réseau sans fil local (type NFC ou Bluetooth par exemple). Dans ce mode de paiement, la validation se fait au moyen du *smartphone* par la reconnaissance de l'empreinte digitale du payeur, en complément ou non d'autres dispositifs d'authentification tels que la saisie d'un code confidentiel ou d'un mot de passe. C'est ce que propose aujourd'hui, entre autres, la solution Apple Pay. Ce type de solution permet potentiellement par un même procédé de renforcer la sécurité des paiements sans contact de faibles montants (par comparaison à une carte NFC standard, la lecture de l'empreinte ajoute un niveau de sécurité complémentaire), voire de remplacer la saisie du code confidentiel pour les paiements de montants supérieurs, dans les limites fixées par l'émetteur au regard de son analyse des risques ;

- avec une carte intégrant un capteur d'empreinte digitale : MasterCard a annoncé en octobre 2014 le lancement d'une carte sans contact NFC intégrant un lecteur d'empreinte digitale dont l'utilisation peut remplacer la saisie du code confidentiel (carte Zwipe MasterCard). Cette carte de paiement au standard EMV dispose également d'une puce et demande la frappe d'un code confidentiel. Elle n'est cependant pas diffusée en France à ce jour ;

- avec un équipement commerçant équipé d'un capteur d'empreinte digitale ou du réseau veineux de la main : Natural Security Alliance a lancé, en partenariat avec plusieurs enseignes de la grande distribution, une expérimentation en France depuis octobre 2012 mettant en œuvre l'authentification par lecture de ce type d'empreinte en substitution à la saisie du code confidentiel. Le terminal de paiement est équipé d'un module qui capture l'empreinte digitale ou du réseau veineux du doigt du porteur et la compare avec celle enregistrée dans la carte.

D'autres caractéristiques physiques ou biologiques pourraient également faire l'objet d'expérimentations dans un futur proche, comme la reconnaissance faciale. Le fabricant Toshiba a ainsi présenté en janvier 2015 le *Toshiba Touchless Commerce*, un concept de caisse automatique avec une caméra permettant la reconnaissance faciale du client enrôlé au préalable ; cette solution n'a toutefois pas encore donné lieu à un pilote.

3|5 Application au retrait

Le retrait présente l'avantage d'environnements généralement mieux contrôlés, en particulier lorsque les automates sont placés à l'intérieur des agences.

Plusieurs constructeurs proposent déjà des automates de retrait équipés de capteurs biométriques généralement utilisés en remplacement de la saisie du code confidentiel, mais aucune expérimentation n'a été répertoriée à ce jour en France. Deux types de dispositifs biométriques se partagent le marché :

• la reconnaissance du réseau veineux des doigts ou de la main, qui est un mode d'authentification commun sur les automates bancaires au Japon, avec certains déploiements importants également réalisés au Brésil et en Turquie ;

• la reconnaissance de l'iris de l'œil, également expérimentée sur des automates bancaires au sein de plusieurs états aux États-Unis.

Ce cas d'usage nécessite préalablement de déployer des automates bancaires équipés et de former les porteurs et les équipes des agences au fonctionnement de ces équipements.

4| Conclusion

L'utilisation des techniques biométriques lors des opérations avec des cartes de paiement est encadrée en France par la loi Informatique et Libertés. La fourniture de solutions de paiement utilisant des dispositifs biométriques requiert ainsi le dépôt préalable d'une demande d'autorisation auprès de la CNIL, qui fixe les principes directeurs applicables à ce domaine.

L'Observatoire constate que les expérimentations actuellement menées en France visent en priorité à tester l'ergonomie des dispositifs biométriques envisagés et à mesurer le niveau d'adhésion du public aux solutions proposées. Préalablement à tout déploiement à grande échelle, l'Observatoire souligne la nécessité d'une analyse des risques liés aux cas d'usage de l'authentification biométrique afin que les solutions mises en œuvre offrent un niveau de protection des opérations de paiement au moins équivalent à l'état de l'art en la matière (*i.e.* code confidentiel et carte à puce en paiement de proximité, code non rejouable en paiement à distance).

Dans ce contexte, l'Observatoire relève que le niveau de sécurité offert par les dispositifs de biométrie actuels demeure difficile à mesurer faute de standards d'évaluation équivalents à ceux existants pour des technologies éprouvées (carte à puce, carte SIM de téléphone portable, etc.). Par conséquent, l'Observatoire souligne le besoin de disposer rapidement de référentiels permettant de qualifier le niveau de sécurité de ces nouveaux dispositifs en s'appuyant sur une évaluation prenant en compte l'ensemble des composants des solutions (matériels et algorithmes utilisés par les dispositifs biométriques, cas d'usage prévus).

En ce sens, les acteurs devront veiller à ne pas généraliser des dispositifs d'authentification biométrique présentant un niveau de sécurité trop faible et susceptibles d'entraîner la compromission des caractéristiques biométriques d'un grand nombre de porteurs les utilisant. En effet, le déploiement de solutions futures offrant un niveau de sécurité plus adapté mais reposant sur ces mêmes caractéristiques biométriques potentiellement compromises pourrait alors être remis en cause.

Enfin, du fait des limitations inhérentes à la biométrie et du manque de maturité de l'évaluation sécuritaire de ces dispositifs, l'Observatoire recommande de toujours conserver un moyen d'authentification alternatif capable de se substituer au dispositif biométrique dans les cas où celui-ci ne s'avèrerait plus en mesure d'offrir les niveaux de service et de sécurité requis.

Les nouveaux moyens de paiement : de nouveaux enjeux de sécurité

Synthèse de la conférence du 22 octobre 2014 organisée par la Banque de France et la Banque centrale européenne

La Banque de France a organisé le 22 octobre 2014 à Paris, en collaboration avec la Banque centrale européenne (BCE), une conférence internationale sur les nouveaux défis en matière de sécurité des moyens de paiement.

Cette journée a été l'occasion de présenter les évolutions institutionnelles au niveau européen dans le domaine de la sécurité des moyens de paiement, d'échanger sur les mesures pouvant être adoptées pour améliorer la sécurité des paiements par mobile et sur internet, et enfin d'évoquer les conséquences en termes de sécurité du recours à des tiers de paiement.

1| L'émergence de nouveaux enjeux de sécurité

Le gouverneur de la Banque de France, Christian Noyer a rappelé, dans son allocution d'ouverture, que le développement de nouveaux modes de paiement, bien que nécessaire pour répondre aux nouvelles manières de consommer, présentait également des risques en matière de sécurité qu'il convenait de maîtriser.

Le gouverneur a insisté sur les conditions de réussite des nouveaux modes de paiement, au regard notamment de l'expérience acquise dans le cadre de l'Observatoire pour ce qui concerne les paiements par carte :

- une nouvelle solution de paiement sera d'autant plus utilisée qu'elle est perçue par les consommateurs comme étant sûre. Il est ainsi dans l'intérêt des prestataires de services de paiement (PSP) innovants d'investir dans la lutte contre la fraude ;

- la coopération entre tous les acteurs de la chaîne des paiements est nécessaire pour obtenir des résultats durables. Des instances telles que l'Observatoire sont ainsi d'une importance majeure pour déjouer les tentatives de fraude sur le long terme ;

- la meilleure coordination des autorités nationales et européennes compétentes en matière de sécurité des moyens de paiement est indispensable au regard de l'internationalisation des réseaux de fraudeurs. L'apport conséquent du forum européen de la sécurité des moyens de paiement *SecuRe Pay* au cours de ces trois dernières années a démontré les importantes avancées pouvant être réalisées lorsque l'ensemble des autorités travaillent de concert.

Benoît Cœuré, membre du directoire de la BCE, a présenté les évolutions associées à la création du forum *SecuRe Pay* sous l'égide de la BCE. Établi début 2011 en réponse à la hausse de la fraude sur les paiements par carte à distance, le forum réunit les superviseurs (autorités de contrôle prudentiel) et les surveillants (banques centrales) des PSP des pays membres de l'Union européenne. Coprésidé depuis octobre 2014 par la BCE et l'Autorité bancaire européenne (ABE), il a pour vocation d'instaurer un dialogue entre les différentes autorités nationales et européennes en vue de définir des requis sécuritaires communs en matière de moyens de paiement. À ce jour, le forum a publié trois séries de recommandations [1]. Neutres d'un point de vue technologique, ces recommandations et orientations demandent aux PSP de conduire une évaluation exhaustive des risques liés aux paiements sur internet et de renforcer leur sécurité en mettant

1 Les recommandations concernant la sécurité des paiements mobiles et celles relatives aux tiers de paiement alimentent les travaux en cours concernant la révision de la directive sur les services de paiement ; les recommandations pour la sécurité des paiements sur internet ont été reprises par l'Eurosystème pour ses cadres de surveillance et par l'ABE sous la forme d'orientations publiées depuis en décembre 2014 et applicables au 1er août 2015.

Encadré

Programme de la conférence du 22 octobre 2014

Discours d'ouverture
Christian Noyer (gouverneur, Banque de France)

Présentation introductive
Benoît Coeuré (membre du directoire, Banque centrale européenne)

Thème I : La coopération entre autorités européennes dans le domaine de la sécurité des moyens de paiement de détail

Table ronde
Modérateur : Pierre Petit (coprésident, forum SecuRe Pay*)*
Mario Nava (directeur en charge des institutions financières, Commission européenne)
Adam Farkas (directeur exécutif, Autorité bancaire européenne)

Thème II : Les attentes en matière de sécurité sur les moyens de paiement

Table ronde sur les paiements mobiles
Modérateur : Hanna Franiak (conseiller au département des Systèmes de paiement, Banque nationale de Pologne)
Pierre Chassigneux (responsable Risques et Audit, Groupement des Cartes Bancaires)
Rob Marrewijk (manager du programme sécurité des terminaux, Brightsight)
Santiago Minguito Santos (directeur de la Sécurité de l'information, Banco Sabadell)
Edwin Aoki (architecte en chef, PayPal)

Présentation introductive
Adam Farkas (directeur exécutif, Autorité bancaire européenne)

Table ronde sur les paiements en ligne
Modérateur : Dirk Haubrich (responsable de l'unité de Protection des consommateurs, Autorité bancaire européenne)
Dirk Schrade (adjoint au chef du département des Systèmes de paiement et de Règlement, Banque fédérale d'Allemagne)
Ingrid Lauterbach (responsable de la sécurité client au sein du groupe de cyber-sécurité, Deutsche Bank)
Paul Alfing (président, Comité des e-paiements)
Monique Goyens (directeur général, Organisation des consommateurs européens)

Thème III : Acteurs tiers – comment réguler ?

Présentation introductive
Mario Nava (directeur en charge des institutions financières, Commission européenne)

Table ronde sur les tiers de paiement
Modérateur : Denis Beau (directeur général des Opérations, Banque de France)
Pierre Petit (coprésident, forum SecuRe Pay*)*
Irmfried Schwimann (directeur des Services financiers, Commission européenne)
Massimo Doria (responsable de la division des Services et Instruments de paiement, Banque d'Italie)
Jean Clamon (directeur général, BNP Paribas)
Georg Schardt (adjoint au président directeur général, SOFORT AG)

Conclusion de la conférence
Denis Beau (directeur général des Opérations, Banque de France)

notamment en place des dispositifs d'authentification renforcée des utilisateurs. Une attention particulière est également portée sur la protection des données sensibles de paiement et sur la sensibilisation des utilisateurs pour lutter efficacement contre la fraude.

2| La coopération des autorités européennes en matière de sécurité des moyens de paiement

Cette première session a permis de dresser un panorama des compétences des institutions européennes et de leur coopération dans la conduite de leurs missions.

Le mandat de l'Eurosystème et de la BCE en matière de moyens de paiement provient des dispositions des traités constitutifs et des statuts du système européen de banques centrales sur la promotion du bon fonctionnement des systèmes de paiement. La BCE et l'Eurosystème poursuivent deux objectifs en la matière : maintenir la confiance des utilisateurs dans la monnaie et prévenir toute nouvelle fragmentation du marché européen des paiements. Pour ce faire, la BCE et les banques centrales nationales membres de l'Eurosystème interviennent en tant que catalyseurs des initiatives des acteurs de marché contribuant à une plus grande intégration européenne des services de paiement, tout en assurant la surveillance de la sécurité des moyens de paiement d'intérêt commun à l'ensemble des pays de la zone euro. À cette fin, l'Eurosystème a publié des cadres de surveillance coopératifs pour les cartes de paiement (janvier 2008), les prélèvements et les virements (octobre 2008). Des guides d'évaluation correspondant à chacun de ces trois cadres de surveillance sont également disponibles.

La Commission européenne veille à préserver les intérêts des citoyens européens en établissant notamment le cadre juridique nécessaire à l'émergence d'un marché des paiements européens sûr, efficace et compétitif.

Depuis la création des autorités européennes de surveillance, la Commission européenne adopte de manière croissante une approche à deux niveaux lors de la préparation de ses propositions législatives : alors que les grands principes structurants sont inscrits directement au sein des textes législatifs, la définition des modalités techniques de leur mise en œuvre est confiée aux nouvelles autorités européennes de régulation.

Cette approche a notamment été adoptée lors de la révision de la directive sur les services de paiement (DSP2) qui confie à l'ABE, en étroite collaboration avec la BCE, la charge de préciser les modalités de mise en œuvre de certaines dispositions de la directive, dont notamment celles portant sur l'encadrement des risques opérationnels et sécuritaires. C'est notamment le cas du recours à l'authentification renforcée des utilisateurs de moyens de paiement et des transactions.

L'ABE peut, pour se faire, avoir recours à deux types d'instruments réglementaires :

- des normes techniques de réglementation ou d'exécution [2] qui, une fois validées par la Commission européenne, sont d'application directe au sein des différents États membres ;

- des orientations et des recommandations qui doivent être transposées au niveau national par les autorités de supervision des États membres, et dont l'ABE suit la mise en œuvre.

Dans le cadre de la révision de la DSP2, les travaux en vue de l'élaboration de ces différents textes se tiendront au sein du forum *SecuRe Pay*, en conséquence désormais coprésidé par la BCE et l'ABE.

3| Les attentes en matière de sécurité sur les nouveaux moyens de paiement

3|1 La sécurité des paiements par téléphone mobile

La session consacrée aux paiements par téléphone mobile visait à fournir un aperçu des évolutions et des enjeux sécuritaires liés à ce mode de paiement émergent.

2 « *Regulatory Technical Standards* » ou RTS.

La grande diffusion des téléphones mobiles (près de 2 milliards de *smartphones* seraient utilisés dans le monde, soit presque autant que le nombre de cartes de paiement EMV), fait désormais de ceux-ci des instruments de paiement incontournables. La diversité des usages a également été soulignée, les paiements par téléphone mobile pouvant être effectués par des mécanismes très variés : paiements sans contact NFC avec des données de carte de paiement stockées dans la carte SIM (*SIM centric*) ou sur un composant sécurisé dédié (*Secure Element*) ou encore émulées de façon logicielle par le système d'exploitation du téléphone (*Host Card Emulation* [3]), paiements par reconnaissance optique d'un code bidimensionnel (*QR* [4] *Code*), paiements par simple numéro de téléphone, utilisation d'un portefeuille électronique (*wallet*) ou d'une carte de paiement virtuelle…

La diffusion de ces nouveaux modes de paiement et leur diversité appellent à revoir la classification traditionnelle des paiements. En effet, les paiements par téléphone mobile tendent dans certains cas à effacer la frontière entre paiement de proximité et paiement à distance, dans la mesure où, par exemple, certaines transactions par téléphone mobile effectuées en magasin peuvent être validées au moyen d'une connexion internet.

Cette évolution pose de nouveaux défis sécuritaires. Les taux de fraude sur les paiements à distance étant très largement supérieurs à ceux sur les paiements de proximité, le rapprochement de ces deux environnements de paiement ne doit pas mener à un abaissement général des exigences de sécurité et à une dégradation des taux de fraude actuels, notamment en paiement de proximité. L'objectif des acteurs est ainsi aujourd'hui d'apporter, pour les paiements par téléphone mobile, le même niveau de sécurité que celui qui est actuellement connu pour les paiements de proximité par carte à puce de type EMV.

L'identification des menaces constitue le premier défi sécuritaire, en ce qui concerne le paiement par téléphone mobile. Elles peuvent être réparties en trois catégories :

- les menaces sur les systèmes d'exploitation des téléphones, qui peuvent par exemple être infectés par des logiciels malveillants (*malwares*) ;

- les menaces sur les canaux de communication utilisés pour les paiements par téléphone mobile (attaque des transmissions sans fil du type WiFi, NFC ou Bluetooth) ;

- les menaces physiques de piratage des composants des téléphones.

Sur la base de ce constat, au moins quatre axes de réflexion pour renforcer la sécurité des paiements par téléphone mobile sont envisageables.

Tout d'abord associer les fournisseurs de systèmes d'exploitation aux travaux sur la sécurité des paiements par téléphone mobile est une priorité importante, notamment pour promouvoir la sécurisation des systèmes d'exploitation des équipements.

Ensuite, le renforcement des recherches sur la sécurisation des architectures physiques des téléphones mobiles doit être encouragé.

Par ailleurs, avec l'usage grandissant du stockage décentralisé des données sur des serveurs internet distants (gérance informatique dite « en nuage », ou « *cloud computing* »), la question de leur protection doit être repensée dans le but de mieux les sécuriser.

Enfin, un accent doit être mis sur les nouvelles méthodes d'authentification comme la biométrie [5] ou encore sur les techniques de protection des données de paiement en circulation sur les réseaux comme la *tokenisation* [6].

3 Architecture logicielle permettant à un objet connecté (téléphone intelligent, montre…) disposant d'une puce NFC (*Near Field Communication*) d'être reconnu comme une carte de paiement.
4 « *Quick Response* ».
5 Se reporter au sein de ce rapport à l'étude conduite par l'Observatoire dans le cadre de la veille technologique.
6 En monétique, la *tokenisation* est le processus de substitution de données bancaires (numéro de cartes, etc.) par des données à usage unique formant un « jeton » (*token*) sécurisé. Cette solution permet de réduire la transmission de données sensibles sur des canaux de communication.

3|2 La sécurité des paiements par internet

Cette session a permis de présenter le contenu et les modalités de mise en œuvre des orientations de l'ABE sur la sécurité des paiements sur internet. Pour mémoire, les orientations finales sur la sécurité des paiements sur internet ont été publiées par l'ABE le 19 décembre 2014 et entreront en vigueur le 1er août 2015.

Ces orientations reprennent avec quelques aménagements mineurs les recommandations du forum *SecuRe Pay* sur le même sujet publiées le 31 janvier 2013. Tout comme ces dernières, elles abordent différents aspects de la sécurité des paiements sur internet :

- l'environnement général de contrôle et de sécurité (gouvernance, évaluation et atténuation des risques, suivi et déclaration des incidents, traçabilité) ;

- les mesures de contrôle et de sécurité spécifiques pour les paiements sur internet (authentification, suivi des opérations, protection des données sensibles, fixation de limites de paiement et fournitures d'informations aux clients sur les opérations) ;

- la sensibilisation du client et les modalités de communication entre ce dernier et son prestataire de services de paiement (PSP).

Il a été rappelé que l'adoption de ces orientations sur la sécurité des paiements sur internet a en partie été motivée par la très forte hausse du taux de fraude sur les paiements par carte à distance qui a accompagné l'essor du commerce en ligne au cours de ces dernières années. En 2012, les données européennes montrent que ce type de fraude représentait 60 % de la fraude totale au paiement par carte, en progression constante depuis 2008. Le recours à l'authentification forte du payeur lors de la réalisation de paiements sur internet devrait permettre de contrecarrer ce phénomène.

Si les participants à la table ronde se sont accordés sur la nécessité de renforcer la sécurité des paiements sur internet, afin de préserver la confiance des consommateurs dans la sécurité des moyens de paiement mis à leur disposition, certains ont également souligné le besoin de préserver l'ergonomie des différents moyens de paiement et ainsi de s'assurer que les nouveaux dispositifs de sécurité ne soient pas une source de complexité accrue pour les utilisateurs.

3|3 Les défis sécuritaires liés à l'émergence des tiers de paiement

Le projet de refonte de la directive européenne sur les services de paiement (DSP2) prévoit la création de deux nouveaux services de paiement, qui ont pour objet de permettre à un opérateur tiers d'accéder aux comptes de paiement tenus par des prestataires de services de paiement pour : (i) l'initiation de paiements (par exemple, pour payer par virement un commerçant en ligne) ou (ii) l'agrégation d'informations (permettant, par exemple, de présenter le solde des comptes d'une personne dans différents établissements sur une seule page internet).

Ces activités, particulièrement les services d'initiation de paiement, sont actuellement réalisées en dehors de tout cadre juridique par un nombre restreint de sociétés en Europe (quelques acteurs en Allemagne et aux Pays-Bas notamment). Elles représentent, en l'état actuel de la règlementation, un risque en matière de fraude, dans la mesure où elles impliquent la communication par les utilisateurs à un tiers des identifiants et codes d'accès à leurs comptes de banque en ligne.

En termes de sécurité, l'émergence de ces nouveaux acteurs doit être encadrée, pour préserver la sécurité des données bancaires des usagers. À ce titre, la nouvelle directive devrait introduire un statut permettant d'encadrer par la loi ces acteurs. Elle prévoira également un ensemble de dispositions concernant, d'une part, la sécurité des données échangées et stockées, et d'autre part, la sécurité des communications entre les prestataires de services de paiement teneurs de compte, les tiers de paiement et les consommateurs.

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.

A11

Liste nominative des membres de l'Observatoire

En application de l'article R142-22 du *Code monétaire et financier*, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel et de résolution sont nommés pour trois ans par arrêté du ministre chargé de l'Économie, du Redressement productif et du Numérique. Le dernier arrêté de nomination date du 19 décembre 2014.

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

Olivier PRATO
Secrétariat général

Représentants des administrations

Sur proposition du secrétariat général de la défense et de la sécurité nationale :

- Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant :
  José ARAUJO
  Vincent STRUBEL

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

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

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

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

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

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Vincent FILHOL

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
  Sylvain BRUN

Sur proposition du ministre de la Défense :

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

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 DIACONO
Administrateur
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

Éric 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 françaises en circulation en 2014 : 85,6 millions.
- dont 71,0 millions de cartes de type « interbancaire » (« CB », MasterCard, Visa et Moneo) ;
- et 14,6 millions de cartes de type « privatif ».

Cartes mises en opposition [1] en 2014 : environ 905 600.

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

Parmi les transactions internationales, une distinction est faite, à partir de 2010, entre celles qui sont effectuées au sein de la zone SEPA, et celles qui mettent en jeu un acteur – émetteur ou commerçant accepteur – situé dans le reste du monde. Les transactions internationales sont par conséquent de quatre types : émetteur français et accepteur étranger SEPA, émetteur français et accepteur étranger hors SEPA, émetteur étranger SEPA et accepteur français, émetteur étranger hors SEPA et 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 2014 – Émission

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

	Émetteur français, Accepteur français		Émetteur français, Accepteur étranger SEPA		Émetteur français, Accepteur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	8 148,87	344,31	163,38	10,70	46,99	4,38
Paiements à distance hors Internet	14,29	1,85	17,11	1,06	2,04	0,15
Paiements à distance sur Internet	781,70	58,58	155,17	7,50	30,76	1,99
Retraits	1 512,18	121,39	29,85	3,61	20,96	3,18
Total	**10 457,05**	**526,14**	**365,51**	**22,87**	**100,75**	**9,70**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,57	11,73	7,52	0,97	6,24	1,11
Paiements à distance hors Internet	1,13	0,07	–	–	–	–
Paiements à distance sur Internet	17,58	2,40	3,70	0,46	1,28	0,20
Retraits	3,28	0,30	–	–	–	–
Total	**125,56**	**14,49**	**11,22**	**1,43**	**7,51**	**1,31**
Total général	**10 582,61**	**540,63**	**376,73**	**24,30**	**108,27**	**11,01**

Source : Observatoire de la sécurité des cartes de paiement.

Tableau 2

Le marché des cartes de paiement en France en 2014 – Acceptation

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

	Émetteur français, Accepteur français		Émetteur étranger SEPA, Accepteur français		Émetteur étranger hors SEPA, Accepteur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	8 148,87	344,31	217,66	16,51	68,51	9,50
Paiements à distance hors Internet	14,29	1,85	5,61	1,20	1,62	0,76
Paiements à distance sur Internet	781,70	58,58	43,87	5,64	13,20	2,61
Retraits	1 512,18	121,39	26,68	4,86	8,87	2,19
Total	**10 457,05**	**526,14**	**293,82**	**28,20**	**92,20**	**15,06**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,57	11,73	4,31	1,10	7,03	4,03
Paiements à distance hors Internet	1,13	0,07	–	–	–	–
Paiements à distance sur Internet	17,58	2,40	0,88	0,16	0,53	0,19
Retraits	3,28	0,30	–	–	0,44	0,23
Total	**125,56**	**14,49**	**5,19**	**1,26**	**8,00**	**4,45**
Total général	**10 582,61**	**540,63**	**299,02**	**29,46**	**100,20**	**19,51**

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 2014 – Émission

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

	Émetteur français, Accepteur français		Émetteur français, Accepteur étranger SEPA		Émetteur français, Accepteur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	469,7	35 077,6	63,7	7 182,8	106,5	17 879,5
Cartes perdues ou volées	457,5	34 590,8	47,3	4 135,1	17,6	3 840,4
Cartes non parvenues	5,7	309,8	0,3	32,2	0,1	7,3
Cartes altérées ou contrefaites	5,3	99,9	7,1	1 287,8	75,2	11 674,9
Numéro de carte usurpé	0,2	33,1	7,2	1 371,5	11,3	2 008,1
Autres	0,9	44,1	1,7	356,2	2,4	348,7
Paiements à distance hors Internet	18,2	2 579,9	141,3	13 896,5	37,5	7 535,7
Cartes perdues ou volées	0,1	8,3	16,5	1 841,1	6,3	1 285,8
Cartes non parvenues	0,0	0,0	0,1	5,1	0,0	1,1
Cartes altérées ou contrefaites	0,0	1,3	3,1	519,4	2,0	599,5
Numéro de carte usurpé	18,0	2 569,6	121,2	11 498,8	29,0	5 632,4
Autres	0,0	0,7	0,4	32,1	0,2	17,0
Paiements à distance sur Internet	1 355,4	151 716,4	1 276,3	67 142,8	136,4	14 515,6
Cartes perdues ou volées	0,3	21,6	123,9	7 288,6	14,8	1 712,5
Cartes non parvenues	0,0	0,0	0,4	11,6	0,1	4,1
Cartes altérées ou contrefaites	0,1	11,2	34,1	2 077,1	5,2	521,1
Numéro de carte usurpé	1 355,0	151 677,2	1 115,8	57 624,5	115,8	12 230,6
Autres	0,0	6,4	2,1	141,0	0,5	47,4
Retraits	139,5	41 252,8	5,4	1 174,0	179,7	28 315,0
Cartes perdues ou volées	137,9	40 931,6	3,7	853,3	9,7	1 564,6
Cartes non parvenues	0,6	205,8	0,0	5,2	0,0	5,6
Cartes altérées ou contrefaites	0,1	15,3	1,5	273,9	164,4	25 883,5
Numéro de carte usurpé	0,0	4,0	0,0	9,9	1,4	191,2
Autres	0,8	96,0	0,2	31,7	4,2	670,0
Total	**1 982,8**	**230 626,7**	**1 486,7**	**89 396,1**	**460,1**	**68 245,8**

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 2014 – Acceptation

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

	Émetteur français, Accepteur français		Émetteur étranger SEPA, Accepteur français		Émetteur étranger hors SEPA, Accepteur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	469,7	35 077,6	62,9	5 048,0	98,6	18 801,4
Cartes perdues ou volées	457,5	34 590,8	39,6	2 439,4	15,6	3 598,1
Cartes non parvenues	5,7	309,8	1,4	73,1	0,3	78,8
Cartes altérées ou contrefaites	5,3	99,9	10,1	643,7	71,5	12 118,7
Numéro de carte usurpé	0,2	33,1	10,5	1 694,1	10,6	2 808,7
Autres	0,9	44,1	1,3	197,7	0,6	197,2
Paiements à distance hors Internet	18,2	2 579,9	18,0	4 743,7	19,0	7 694,0
Cartes perdues ou volées	0,1	8,3	1,9	157,8	0,9	465,3
Cartes non parvenues	0,0	0,0	0,0	2,4	0,0	9,2
Cartes altérées ou contrefaites	0,0	1,3	1,5	414,4	1,5	698,5
Numéro de carte usurpé	18,0	2 569,6	14,4	4 138,7	16,5	6 472,4
Autres	0,0	0,7	0,2	30,3	0,1	48,6
Paiements à distance sur Internet	1 355,4	151 716,4	125,0	27 548,1	154,0	34 743,3
Cartes perdues ou volées	0,3	21,6	3,9	555,8	7,9	1 962,7
Cartes non parvenues	0,0	0,0	0,2	13,5	0,2	35,3
Cartes altérées ou contrefaites	0,1	11,2	3,0	558,0	12,8	2 470,2
Numéro de carte usurpé	1 355,0	151 677,2	115,9	26 026,6	132,0	28 055,2
Autres	0,0	6,4	2,1	394,2	1,0	219,9
Retraits	139,5	41 252,8	3,8	880,5	2,2	631,4
Cartes perdues ou volées	137,9	40 931,6	3,3	784,3	1,0	305,8
Cartes non parvenues	0,6	205,8	0,0	3,8	0,0	0,4
Cartes altérées ou contrefaites	0,1	15,3	0,2	48,3	1,2	310,9
Numéro de carte usurpé	0,0	4,0	0,2	31,7	0,1	12,5
Autres	0,8	96,0	0,1	12,3	0,0	1,8
Total	**1 982,8**	**230 626,7**	**209,6**	**38 220,3**	**273,8**	**59 870,2**

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 2014 – Émission

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

	Émetteur français, Accepteur français		Émetteur français, Accepteur étranger SEPA		Émetteur français, Accepteur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	3,09	2 040,95	0,93	585,80	5,82	1 323,39
Cartes perdues ou volées	1,18	404,45	0,11	79,53	0,43	94,77
Cartes non parvenues	0,65	356,56	0,15	71,59	0,07	34,41
Cartes altérées ou contrefaites	0,27	51,73	0,36	286,49	4,32	789,18
Numéro de carte usurpé	0,34	173,71	0,32	148,20	1,00	405,03
Autres	0,65	1 054,51	0,0	0,0	0,0	0,0
Paiements à distance hors Internet	0,24	250,74	–	–	–	–
Cartes perdues ou volées	0,00	0,00	–	–	–	–
Cartes non parvenues	0,00	0,00	–	–	–	–
Cartes altérées ou contrefaites	0,00	0,00	–	–	–	–
Numéro de carte usurpé	0,17	171,01	–	–	–	–
Autres	0,07	79,72	–	–	–	–
Paiements à distance sur Internet	5,48	1 498,31	12,92	1 005,94	2,48	429,36
Cartes perdues ou volées	0,31	91,81	0,43	8,87	0,05	1,50
Cartes non parvenues	0,03	3,94	0,01	0,74	0,01	0,39
Cartes altérées ou contrefaites	0,08	8,31	0,13	15,04	0,31	22,60
Numéro de carte usurpé	4,94	1 262,87	12,35	981,29	2,13	404,87
Autres	0,13	131,37	–	–	–	–
Retraits	1,67	226,02	–	–	–	–
Cartes perdues ou volées	1,57	199,59	–	–	–	–
Cartes non parvenues	0,09	24,50	–	–	–	–
Cartes altérées ou contrefaites	0,00	0,00	–	–	–	–
Numéro de carte usurpé	0,00	0,00	–	–	–	–
Autres	0,01	1,93	–	–	–	–
Total	**10,48**	**4 016,01**	**13,85**	**1 591,75**	**8,30**	**1 752,76**

Source : Observatoire de la sécurité des cartes de paiement.

A18

Tableau 6

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2014 – Acceptation

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

	Émetteur français, Accepteur français		Émetteur étranger SEPA, Accepteur français		Émetteur étranger hors SEPA, Accepteur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	3,09	2 040,95	0,20	76,10	4,64	3 059,16
Cartes perdues ou volées	1,18	404,45	0,03	17,10	0,59	368,53
Cartes non parvenues	0,65	356,56	0,00	1,18	0,00	4,25
Cartes altérées ou contrefaites	0,27	51,73	0,06	26,91	3,70	2 435,01
Numéro de carte usurpé	0,34	173,71	0,10	30,92	0,35	250,81
Autres	0,65	1 054,51	0,00	0,00	0,00	0,55
Paiements à distance hors Internet	0,24	250,74	0,01	9,19	0,01	6,50
Cartes perdues ou volées	0,00	0,00	0,00	0,00	0,00	0,00
Cartes non parvenues	0,00	0,00	0,00	0,00	0,00	0,00
Cartes altérées ou contrefaites	0,00	0,00	0,00	0,00	0,00	0,00
Numéro de carte usurpé	0,17	171,01	0,00	0,00	0,00	0,00
Autres	0,07	79,72	0,01	9,19	0,01	6,50
Paiements à distance sur Internet	5,48	1 498,31	2,43	1 030,54	7,93	2 692,55
Cartes perdues ou volées	0,31	91,81	0,01	2,87	0,14	34,12
Cartes non parvenues	0,03	3,94	0,00	2,99	0,10	5,09
Cartes altérées ou contrefaites	0,08	8,31	0,18	77,20	0,73	215,56
Numéro de carte usurpé	4,94	1 262,87	2,22	936,93	6,97	2 437,79
Autres	0,13	131,37	0,01	10,56	0,00	0,00
Retraits	1,67	226,02	–	–	0,00	0,90
Cartes perdues ou volées	1,57	199,59	–	–	0,00	0,00
Cartes non parvenues	0,09	24,50	–	–	0,00	0,00
Cartes altérées ou contrefaites	0,00	0,00	–	–	0,00	0,84
Numéro de carte usurpé	0,00	0,00	–	–	0,00	0,00
Autres	0,01	1,93	–	–	0,00	0,06
Total	**10,48**	**4 016,01**	**2,63**	**1 115,82**	**12,59**	**5 759,12**

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.

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 ;

• 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 ;

3 Personal Account Number.

• 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 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 et aux professionnels : hôtellerie, service de location, billetterie de spectacle, organisme caritatif, matériel de bureau, service de messagerie,… ;
• téléphonie et communication : matériel et service de télécommunication/téléphonie mobile ;
• voyage, transport : ferroviaire, aérien, maritime ;
• divers.

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

Réalisation
Direction de la Communication
de la Banque de France

Opérateurs PAO
Nicolas Besson, 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