2015 | 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 2015
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

François Villeroy de Galhau,
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

CHAPITRE 4 : LES CARTES DE PAIEMENT EN EUROPE : ÉVOLUTIONS RÉCENTES ET DÉFIS POUR L'AVENIR 45

ANNEXES

Le treizième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement (OSCP), relatif à l'exercice 2015, comprend quatre parties dont les principales conclusions sont reprises ci-après.

Les statistiques pour l'année 2015 (présentées en deuxième partie du rapport) confirment la poursuite du repli de la fraude domestique sur les paiements par carte, amorcé l'année précédente, y compris sur les paiements à distance qui restent toutefois significativement plus exposés à la fraude. En revanche, la fraude transfrontière, qu'il s'agisse de paiements de proximité ou à distance, est en hausse.

Pour la première fois depuis la création de l'Observatoire en 2002, la fraude domestique a baissé en valeur (225 millions d'euros, contre 235 millions d'euros en 2014) et en taux, tant dans son ensemble (0,040 %, contre 0,043 % en 2014), que pour chacun des grands modes d'utilisation : paiement de proximité, retraits aux distributeurs automatiques et paiements à distance.

- *Le taux de fraude sur les paiements de proximité domestiques atteint ainsi un plus bas historique à 0,009 %, soit moins de 1 euro pour 10 000 euros de transactions, tandis que le taux de fraude sur les retraits aux distributeurs se replie légèrement, à 0,033 % soit 1 euro de fraude pour 3 000 euros de transactions. L'Observatoire a recueilli en 2015 les premières données statistiques complètes relatives aux paiements en mode sans contact ; le taux de fraude sur ce type de transactions s'établit à un niveau faible et intermédiaire entre celui des paiements de proximité et celui des retraits aux distributeurs automatiques de billets, à 0,019 %. Cette fraude a pour origine exclusive le vol ou la perte de la carte, ce qui confirme l'absence de vulnérabilité technologique spécifique à ce canal.*

- *Le taux de fraude sur les paiements à distance domestiques est également en baisse significative pour la quatrième année consécutive, mais reste toutefois plus de vingt fois supérieur à celui des paiements à un terminal, à 0,228 %, soit 1 euro de fraude pour 440 euros de paiements. De ce fait, 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 au niveau domestique.*

Dans le même temps, la fraude transfrontière continue de se développer de façon significative, pour approcher les 300 millions d'euros en 2015, soit une progression de 30 millions d'euros sur un an (avec un taux de fraude de 0,372 %). Ainsi, les transactions transfrontières supportent 57 % de la fraude, alors qu'elles ne représentent que 12,6 % du total des paiements en montant. Cette fraude est toutefois hétérogène :

- *pour les paiements avec des cartes françaises effectués à l'étranger, le taux de fraude est globalement moins élevé quand ils sont effectués au sein de l'espace SEPA [1] (taux de fraude de 0,459 %) qu'en dehors de l'espace SEPA (0,692 %). Cette différence reflète les efforts entrepris en Europe au cours des dernières années pour renforcer la sécurité des paiements par carte (généralisation du standard EMV [2], recours à l'authentification forte), alors que d'autres zones géographiques (notamment l'Asie et les États-Unis) sont encore en phase de migration vers le standard EMV. La progression de cette migration devrait conduire à terme à une meilleure maîtrise de la fraude aux points de vente et aux automates pour les porteurs de cartes françaises ;*

1 L'espace SEPA comprend les vingt-huit États membres de l'Union européenne, les quatre États membres de l'Association européenne de libre échange (Islande, Liechtenstein, Norvège et Suisse), la principauté de Monaco et la république de Saint-Marin.

2 EMV (Europay MasterCard Visa) : standard géré par le consortium international EMV Co (réunissant les principaux systèmes de paiement par carte) et définissant un ensemble de spécifications techniques fonctionnelles pour les cartes de paiement à puce.

- *pour les porteurs de cartes étrangères effectuant des paiements auprès de commerçants établis en France, le taux de fraude sur les transactions avec des cartes émises dans la zone SEPA (0,153 %) est plus de deux fois inférieur à celui des cartes émises dans une autre région du globe (0,353 %), ce qui souligne à la fois l'effet positif de la définition d'exigences communes au sein de l'Union européenne, ainsi que le report des transactions frauduleuses vers d'autres zones géographiques que la zone SEPA ;*

- *dans tous les cas, le canal de vente à distance reste le plus vulnérable, avec des taux de fraude supérieurs à 1 %, sauf pour les paiements auprès d'e-commerçants établis en France par des porteurs de cartes de l'espace SEPA (0,529 %), qui bénéficient du bon niveau d'équipement des e-commerçants français en dispositif d'authentification forte.*

La poursuite des actions conduites par les commerçants et les émetteurs de cartes pour renforcer la sécurité des paiements à distance, que l'Observatoire a fortement encouragée et accompagnée (elles sont présentées en première partie du rapport), a joué un rôle clé dans cette réduction de la fraude domestique.

*En effet, la poursuite de la baisse du taux de fraude sur les paiements par carte sur internet est le résultat des efforts réalisés par les émetteurs et les e-commerçants pour **diffuser l'utilisation de dispositifs d'authentification forte** :*

- *la quasi-totalité des porteurs effectuant des paiements en ligne sont désormais enrôlés dans un dispositif d'authentification forte ;*

- *du côté des e-commerçants, le taux d'équipement en dispositif d'authentification forte continue de progresser, à 66 % contre 58 % un an auparavant. Cette adoption a pu être favorisée par un taux d'échec sur les transactions authentifiées particulièrement maîtrisé et inférieur à celui sur les transactions non authentifiées, confirmant ainsi que les consommateurs se sont habitués à l'authentification forte, notamment via le système « 3D-Secure ».*

*Le recours accru à l'authentification forte a créé le besoin d'apporter aux e-commerçants une meilleure visibilité sur l'état de fonctionnement des systèmes d'authentification. Pour y répondre, un **dispositif de contact**, mis en place et administré par le secrétariat de l'Observatoire depuis le 1er juillet 2016, permet désormais aux différentes parties prenantes (commerçants, banques, systèmes de paiement par carte ou prestataires techniques) d'assurer une meilleure circulation de l'information en cas d'incidents sur les systèmes d'authentification.*

*Par ailleurs, des actions ciblées ont été conduites par l'Observatoire auprès du **secteur de la téléphonie mobile**, en lien avec l'Autorité de régulation des communications électroniques et des postes (ARCEP), du fait de ses spécificités au regard de la sécurité des paiements à distance :*

- *d'une part, les acteurs de ce secteur subissent une fraude supérieure à celle enregistrée sur les autres secteurs d'activité pour les paiements par cartes à distance ; les investigations conduites ont permis de souligner en particulier la vulnérabilité du canal de vente par téléphone, pour lequel le recours à une authentification par « 3D-Secure » est peu ergonomique. L'Observatoire invite en conséquence les acteurs de ce secteur à renforcer les contrôles effectués sur les canaux de vente par téléphone (meilleure identification des clients), afin de réduire l'exposition à la fraude ;*

- *d'autre part, les opérateurs jouent un rôle central dans le dispositif d'authentification forte le plus répandu en France, en assurant la transmission par le canal SMS des codes de validation à usage unique de leurs clients lors d'achats sécurisés en ligne. Or les fraudeurs développent des techniques d'usurpation d'identité en vue d'intercepter les codes de validation des transactions, utilisés ensuite pour des paiements en ligne frauduleux à partir de numéros de cartes détournés. La lutte contre ce type de fraude passe par une meilleure protection des modalités de réémission des cartes SIM, en vue d'éviter que celles-ci ne puissent être remises à une tierce partie malveillante ; de ce fait, l'Observatoire appelle les opérateurs de téléphonie mobile à la vigilance dans les opérations d'émission de cartes SIM, en améliorant notamment le processus d'identification du demandeur.*

Par ailleurs, l'Observatoire a mené en 2015-2016 des travaux de veille technologique sur deux sujets (présentés en troisième partie du rapport) : les technologies de paiement sans contact par téléphone mobile d'une part, et les nouvelles solutions d'authentification forte d'autre part, qui sont tous deux porteurs d'enjeux importants en matière de maîtrise de la sécurité des paiements par carte.

*Concernant les **technologies de paiement sans contact**, l'Observatoire s'est intéressé en particulier à l'émergence de nouvelles solutions de paiement reposant sur la substitution de la carte par un téléphone mobile doté de la technologie sans contact de type NFC (*near field communication*). De telles solutions, actuellement déployées dans certains pays et en cours d'expérimentation en France, partagent la même technologie que les cartes sans contact, et présentent donc la spécificité de pouvoir être compatibles avec les terminaux de paiement acceptant ces dernières.*

Dans ce contexte, l'Observatoire note l'intérêt de disposer d'expérimentations pilotes associant émetteurs de cartes et systèmes de paiement par carte, et permettant de tester les modalités de sécurisation des différents modèles envisagés sur l'ensemble de leur cycle de vie. Ces expérimentations doivent s'attacher à évaluer le niveau de sécurité global offert par les solutions, dans un cadre contractuel protecteur à l'égard des utilisateurs pilotes en cas de fraude ou de problème technique.

Avant tout déploiement à grande échelle, l'Observatoire invite les acteurs du marché à conduire une analyse des risques liés à l'usage de telles solutions et à définir pour ce faire des référentiels d'évaluation adaptés, en vue de garantir un niveau de sécurité équivalent à celui des paiements par carte en mode NFC.

*Concernant les **solutions de sécurisation des paiements**, l'Observatoire note que les évolutions des cadres règlementaires en Europe, dont principalement la Directive européenne révisée sur les services de paiement (dite DSP2) et publiée en janvier 2016, visent à systématiser le recours à l'authentification forte du porteur de la carte pour les transactions à distance. Dans le même temps, la solution majoritairement déployée en France, reposant sur l'utilisation du protocole « 3D-Secure » pour l'authentification du porteur par l'émetteur de la carte* via *l'envoi par SMS d'un code à usage unique, présente certaines limites en matière d'utilisation (notamment pour les paiements par téléphone ou courrier) et d'ergonomie (cas des achats depuis le mobile).*

Cette situation amène les acteurs à rechercher des solutions de sécurisation innovantes. Ces solutions associent de nouveaux systèmes d'authentification tels que l'évolution du protocole « 3D-Secure » pour une meilleure adaptation aux achats par mobile ou encore le déploiement de cartes à cryptogramme visuel dynamique, et des mesures complémentaires, telles que le développement de dispositifs d'évaluation du niveau de risque d'une transaction (techniques de scoring *des transactions), ou de techniques de substitution du numéro de carte par un numéro désensibilisé (« tokenisation »).*

L'Observatoire souligne la nécessité de disposer d'une évaluation (i) du niveau de sécurité offert par ces solutions, (ii) de leur conformité au regard des exigences règlementaires, notamment de la DSP2, ainsi que (iii) des contraintes qu'elles génèrent pour leurs utilisateurs (ergonomie et universalité des solutions pour les consommateurs, facilité d'implémentation et de gestion pour les commerçants).

Enfin, une conférence ouverte par le gouverneur et intitulée « Les cartes de paiement en Europe : évolutions récentes et défis pour l'avenir » a été organisée par la Banque de France en janvier 2016. Une synthèse en est donnée en quatrième partie de ce rapport.

La conférence internationale des 18 et 19 janvier 2016 a porté sur les perspectives de développement de l'usage des cartes, compte tenu des évolutions récentes en matière de législation, d'innovation technologique et de développement de la fraude. Ces deux journées ont été l'occasion de développer un dialogue entre institutions européennes, autorités publiques et acteurs de marché autour de ce thème, et ont permis de mettre en exergue trois grands enjeux :

- *la poursuite du développement et de la mise en œuvre des innovations. Les différents intervenants ont souligné à cet égard le besoin de continuer le déploiement des paiements sans contact et des paiements mobiles, en soulignant l'impact positif de ces innovations sur les volumes de vente des commerçants. Le développement de l'innovation implique parallèlement de garantir une égalité de traitement entre les acteurs établis et les nouveaux entrants afin de réguler selon le profil de risque du service et non selon la nature ou le statut du fournisseur de ce service ;*

- *le renforcement d'un double mouvement de compétition et de coopération (la « coopétition ») entre les parties prenantes au niveau européen pour construire des services harmonisés et éviter la fragmentation du marché. À ce titre, les efforts de standardisation et d'interopérabilité entre les structures dans le domaine des cartes de paiement sont appelés à se poursuivre, au travers notamment de l'approfondissement du projet SEPA pour les cartes (SEPA* for cards*) ;*

- *enfin, la sécurité des paiements constitue une condition essentielle au développement du paiement par carte, dans un contexte où l'apparition de nouveaux usages, qu'il s'agisse du « sans contact » ou du paiement par* smartphone*, tend à augmenter la complexité technique des opérations et le nombre d'acteurs impliqués. À ce titre, le maintien d'une vigilance forte à l'égard de la fraude et la recherche permanente de solutions de sécurisation en réponse aux nouveaux risques impliquent une pleine coopération de l'ensemble des acteurs, au travers de structures de place non concurrentielles, telles que l'Observatoire.*

Travaux de l'Observatoire en vue de renforcer la sécurité des paiements à distance

L'essor des paiements à distance ces dernières années a sensiblement fait évoluer les usages autour de la carte et a eu également des incidences sur les pratiques en matière de fraude. Dans ce contexte, la méthodologie retenue en 2002 par l'Observatoire pour sa collecte des chiffres de fraude a fait l'objet d'une révision en 2015, dont les principales conclusions sont présentées dans le présent chapitre.

Ce chapitre comporte également un état des lieux de la mise en œuvre des recommandations de l'Observatoire auprès des émetteurs de cartes afin de renforcer la sécurité du paiement à distance. Les recommandations, établies en 2008, portent essentiellement sur la généralisation des dispositifs d'authentification renforcée mis à disposition des porteurs et le déploiement de leur usage par les commerçants en ligne. Elles font l'objet d'un suivi statistique depuis 2011, restitué dans le présent rapport.

Par ailleurs, ce suivi statistique a fait ressortir le besoin d'échanges entre les différentes parties prenantes (émetteurs de cartes, *schemes* cartes [1], commerçants en ligne et leurs prestataires techniques), en cas d'incidents techniques concernant les systèmes d'authentification utilisés par ces différents acteurs. L'Observatoire a en conséquence établi en 2016 un dispositif d'échanges d'information à cette fin.

Enfin, les statistiques de fraude annuelles de l'Observatoire montrent ces deux dernières années que le secteur de la téléphonie est particulièrement concerné. Parallèlement, le dispositif d'authentification renforcée le plus utilisé à ce jour est l'envoi de codes à usage unique par SMS, toutefois vulnérable à certaines attaques. L'Observatoire a en conséquence engagé, en collaboration avec l'Autorité de régulation des communications électroniques et des postes (ARCEP), des actions auprès des principaux opérateurs de téléphonie mobile afin de mieux sécuriser ces deux domaines.

1 Systèmes de paiement par carte.

1| La confirmation de l'approche statistique retenue par l'Observatoire pour l'évaluation des montants de fraude

L'Observatoire a réalisé la revue de l'approche méthodologique retenue pour la mesure du montant de la fraude aux cartes de paiement qui est publié chaque année dans son rapport d'activité.

Deux approches différentes sont possibles pour mesurer la fraude :

- une approche en « fraude brute », qui consiste à recenser l'ensemble des transactions de paiement autorisées ayant ensuite fait l'objet d'un rejet *a posteriori* pour motif de fraude ;

- une approche en « fraude nette », qui consiste à déduire de ce montant de fraude brute les fonds qui ont pu être recouvrés par le commerçant ou par les établissements bancaires.

L'approche en fraude nette se justifie par la mise en œuvre d'un ensemble de mesures afin de réduire le préjudice lié à un paiement frauduleux :

- dans certains cas, le commerçant peut avoir la capacité d'interrompre la livraison des produits ou d'arrêter la fourniture du service après avoir reçu l'information d'un impayé pour motif frauduleux (vol, perte, usurpation de numéro de carte, etc.) ;

- dans d'autres cas, cet impayé relève plutôt d'un litige commercial ou d'une répudiation abusive de la part d'un client qui rencontre des difficultés de paiement (par exemple, dans le cas d'un paiement fractionné) et le commerçant peut trouver un accord amiable avec le client pour le rééchelonnement du paiement ou la restitution des produits ;

• enfin une action en justice, conduite par le commerçant ou par la banque du porteur, peut également permettre l'obtention de réparation pour dommages et intérêts et/ou la restitution des biens et des espèces saisies par les forces de l'ordre.

Néanmoins, depuis 2002, l'Observatoire a privilégié une approche en fraude brute pour les raisons suivantes :

• pertinence : le calcul selon la méthode de la fraude brute exclut bien les tentatives de fraude qui ont été déjouées avant le paiement (par exemple, grâce à la mise en œuvre de l'authentification renforcée du payeur ou par la demande de présentation de la carte et de son code confidentiel au moment du retrait physique d'une commande effectuée à distance). De surcroît, tous les cas de fraude ainsi comptabilisés correspondent bien à des cas réels de fraude ayant impacté au moins un des acteurs légitimes du paiement, le porteur de la carte et/ou le commerçant, l'émetteur de la carte (la « banque du porteur ») ou encore l'acquéreur du paiement (la « banque du commerçant ») ;

• faisabilité : la fraude brute est une donnée plus simple à mesurer avec un haut niveau de fiabilité, dans la mesure où sa collecte peut s'appuyer sur les messages traités dans les systèmes d'information de paiement et de retrait par carte.

En outre, l'approche en fraude brute facilite la comparaison internationale de la fraude aux cartes de paiement puisqu'elle a également été retenue, pour les mêmes raisons, par l'Eurosystème pour son rapport annuel sur la fraude aux cartes de paiement en Europe [2].

Cette approche présente toutefois l'inconvénient d'afficher des données de fraude qui s'avèrent d'une part légèrement supérieures au montant des fonds réellement détournés par les fraudeurs, et peuvent, d'autre part, entraîner des différences de perception du niveau de fraude réel entre d'un côté, les porteurs et les acteurs bancaires, qui supportent la fraude brute et, de l'autre côté, les commerçants dont le modèle économique est plus naturellement fondé sur la fraude nette.

L'étude conduite par l'Observatoire auprès des acteurs bancaires et des commerçants a permis de mesurer l'ampleur de cette différence entre la fraude brute et la fraude nette, qui est en moyenne inférieure à 5 %.

L'écart entre fraude brute et fraude nette est plus important pour les commerçants que pour les banques, les premiers disposant généralement de marges de manœuvre plus imposantes pour réduire le préjudice en cas d'impayé. Des écarts relativement significatifs ont également pu être observés entre commerçants, principalement liés aux différents modèles d'organisation retenus dans le processus de traitement des commandes.

Ainsi à titre d'exemple, les écarts les plus importants entre la fraude brute et la fraude nette concernent les places de marché [3] qui traitent majoritairement des commandes comportant des produits livrés par plusieurs commerçants différents. Le paiement peut alors être remis à l'encaissement plus tôt dans le processus de traitement de la commande que lors d'une commande mono-commerçant. Les tentatives de fraude déjouées avant la remise des produits, mais après la remise à l'encaissement du paiement, peuvent dans ce cas apparaître dans les statistiques de fraude brute de la place de marché sans avoir pour autant généré un préjudice pour cette dernière.

Les résultats de cette étude permettent, au final, de confirmer la pertinence de l'approche brute retenue par l'Observatoire pour mesurer la fraude aux cartes de paiement, l'écart restant faible entre fraude brute et fraude nette, au sens du montant des fonds effectivement détournés par les fraudeurs.

2 Quatrième rapport de l'Eurosystème sur la fraude aux cartes de paiement en Europe (en anglais : « *Fourth report on card fraud* ») : *https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf*

3 Sites en ligne regroupant plusieurs e-commerçants et gérant le plus souvent les opérations de paiement des biens et service vendus par ces derniers.

2| L'état d'avancement de la sécurisation des paiements par carte sur internet

La sécurisation des paiements par carte sur internet est, depuis plusieurs années, la mission première de 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. L'Observatoire a en effet incité depuis 2008 les émetteurs de cartes à équiper leurs porteurs de dispositifs d'authentification renforcée, au travers notamment de leur enrôlement dans le système « 3D-Secure ».

Afin de suivre la mise en œuvre de ses recommandations, l'Observatoire a mis en place une collecte semestrielle initiée en 2011 auprès des principaux acteurs bancaires afin de mesurer la progression des paiements authentifiés. La dernière collecte, relative à la période allant du 1er novembre 2015 au 30 avril 2016, porte sur un volume de 63 millions de cartes de paiement pour un montant global de paiements de 44,8 milliards d'euros.

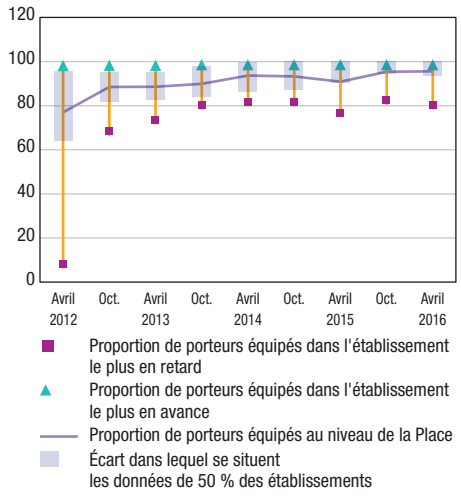
Ce processus d'enrôlement et d'équipement est aujourd'hui achevé, avec un taux moyen d'équipement des porteurs de cartes en solution d'authentification renforcée de 96 %. Les quelques établissements demeurant avec des taux plus faibles d'équipement (autour de 80 %) ne posent pas de difficulté dans la mesure où les porteurs non équipés concernent des populations identifiées comme n'effectuant pas d'achats sur internet.

L'équipement des porteurs s'est déroulé concomitamment à la migration des commerçants vers une acceptation des paiements authentifiés. À ce jour, 66 % des commerçants en ligne disposent d'un contrat permettant l'acceptation de paiements avec déclenchement d'une authentification renforcée. Si le parc de commerçants équipés était constitué initialement de petits commerçants, la représentativité des commerçants équipés a fortement évolué depuis 2014 avec une migration très importante des grands e-commerçants vers un équipement en acceptation « 3D-Secure » en mode sélectif. L'Observatoire se félicite de cette évolution et reconnait le rôle important qu'ont joué certains grands marchands internet dans l'adoption à grande échelle du dispositif « 3D-Secure ».

Graphique 1

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

(en %)

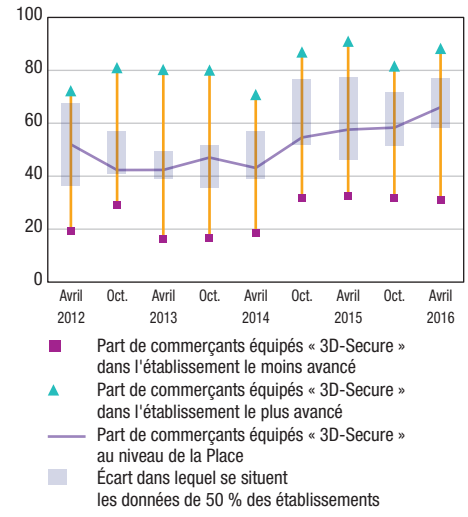


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 2

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

(en %)

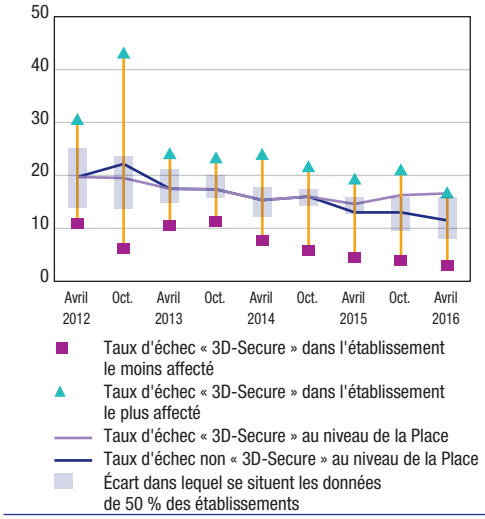


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 3

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

(en %)

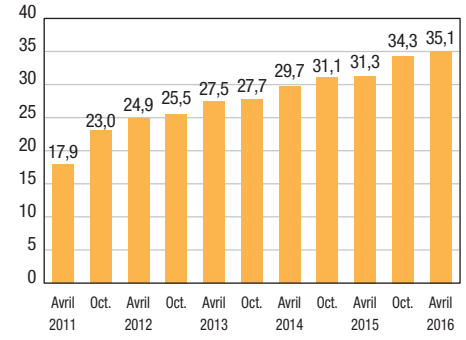


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 4

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

Dans le même temps, les actions conduites par les acteurs de la chaîne des paiements ont permis de ramener le taux d'échec global [4] des transactions authentifiées à 11 % contre environ 20 % lors des premières collectes en 2011. Depuis la fin 2014, ce taux d'échec est même devenu inférieur au taux d'échec sur les paiements non authentifiés [5]. Plusieurs facteurs peuvent expliquer cette tendance, notamment une meilleure appropriation de ces dispositifs par les particuliers, ainsi que la plus grande efficacité des contrôles réalisés sur les sites équipés de l'authentification forte, laquelle pousse les fraudeurs à privilégier par défaut des sites non équipés. En effet, la mise en place de méthodes de *scoring* des transactions permettant le déclenchement d'une authentification forte en fonction du risque associé à la transaction entraîne une fiabilité supérieure de l'opération de paiement ainsi sécurisée.

Compte tenu de ces différentes évolutions favorables au développement du recours à l'authentification forte, la part des paiements en ligne ayant donné lieu à une authentification de ce type a continué de progresser, pour atteindre un peu plus de 35 % des montants de paiement par carte.

3| Le renforcement de l'information des commerçants en cas d'incident affectant les systèmes d'authentification des transactions

Les dispositifs d'authentification forte les plus répandus en France s'appuient sur le protocole « 3D-Secure », qui assure une mise en relation des domaines émetteur et acquéreur au moment de la transaction. Cette mise en relation suppose le recours à un plus grand nombre d'intermédiaires et de prestataires techniques dans la chaîne de paiement par rapport à un paiement sans authentification.

Dans la mesure où le recours à l'authentification forte augmente, il est légitime que le commerçant ait la meilleure visibilité possible sur l'état de fonctionnement du système d'authentification. Une visibilité insuffisante, liée notamment à une relation contractuelle bilatérale avec son prestataire d'acquisition des paiements, qui n'englobe pas les prestataires techniques, peut constituer un frein à l'adoption de ces dispositifs par les e-commerçants, qui y voient un risque de perte sur leur chiffre d'affaires en cas de défaillance technique.

Afin d'apporter une plus grande réactivité et de répondre aux préoccupations des e-commerçants,

4 Le taux d'échec inclut cependant l'intégralité des motifs pouvant amener une opération à ne pas être aboutie et pas seulement les motifs uniquement liées à « 3D-Secure » : tentatives de fraudes, saisie erronée, *timeout*, etc.

5 Paiements non « 3D-Secure » n'ayant pas abouti quel que soit le motif.

l'Observatoire a proposé de constituer et de maintenir un dispositif de contact spécifique à la gestion des incidents liés aux processus d'authentification comprenant les principaux *schemes* carte de paiement, émetteurs, prestataires techniques, grands e-commerçants et opérateurs de téléphonie mobile. Ce dispositif, opérationnel à compter du 1er juillet 2016, est constitué d'une liste de contacts maintenue par le secrétariat de l'Observatoire. Il n'a pas vocation à se substituer aux obligations contractuelles de chacune des parties ou encore aux dispositifs existants mis en place par certains acteurs, mais vise à permettre une meilleure circulation de l'information en cas d'incidents sur les systèmes d'authentification (identification et prise en charge plus rapides), dans l'intérêt de tous.

4| Les actions entreprises avec les opérateurs de téléphonie mobile et l'ARCEP en matière de prévention de la fraude aux paiements

4|1 Contexte des travaux

Les travaux conduits par l'Observatoire sur la sécurisation des paiements à distance ont mis en exergue deux problématiques liées au secteur de la téléphonie :

• d'une part, les opérateurs du secteur présentent depuis plusieurs années des taux de fraude sur les paiements réalisés à distance, sur leurs sites de vente en ligne ou par téléphone, très supérieurs à la moyenne des e-commerçants français ; si cet état de fait peut s'expliquer en partie par l'attractivité de ces produits et services vendus pour les fraudeurs (tels que l'achat de forfaits, de téléphones ou de matériel de communication, ou encore le rechargement de comptes téléphoniques prépayés), l'adoption des mesures de sécurisation des paiements sur internet semble s'être avérée moins efficace que dans les autres secteurs marchands ;

• d'autre part, les opérateurs de téléphonie mobile jouent un rôle central dans une des principales modalités de mise en œuvre du dispositif d'authentification forte déployé en France, en assurant la transmission des codes à usage unique pour la validation des paiements sur internet des porteurs de cartes *via* leurs lignes de téléphonie mobile. À ce titre, les émetteurs de cartes ont noté l'apparition de cas de détournement de lignes téléphoniques par les fraudeurs, au moyen de techniques dites de SIM-*swap*. Les fraudeurs usurpent l'identité du titulaire légitime d'une ligne auprès de son opérateur de téléphonie mobile, en vue de se faire remettre une nouvelle carte SIM lui permettant de recevoir les SMS d'authentification des paiements. Contrairement aux cas de fraude les plus couramment observés, ce type de fraude ne vise ni le porteur de la carte, ni le commerçant, ni un prestataire de services de paiement, mais l'opérateur de téléphonie mobile, soit un acteur qui n'est pas partie prenante directe aux opérations de paiement.

Dans ce contexte, l'Observatoire s'est rapproché du régulateur du secteur de la téléphonie, l'Autorité de régulation des communications électroniques et des postes (ARCEP), pour (i) sensibiliser les opérateurs à ces deux problématiques, (ii) évaluer l'état réel de la situation et (iii) identifier des pistes d'amélioration. L'Observatoire a ainsi conduit, en relation avec l'ARCEP, une consultation auprès des quatre principaux opérateurs de téléphonie mobile sur les mesures de protection mises en œuvre, tant au niveau des paiements par carte encaissés hors point de vente que pour la réémission de cartes SIM vers leur clientèle.

4|2 Spécificités des opérateurs de téléphonie en termes de fraude

Malgré une nette amélioration observée en 2015, le secteur de la téléphonie mobile présente toujours un taux de fraude sensiblement supérieur à la moyenne de l'ensemble des autres e-commerçants.

De façon générale, la consultation conduite par l'Observatoire auprès des opérateurs a permis de constater que ces derniers ont déployé des dispositifs de protection des paiements sur internet similaires à ceux des autres e-commerçants français, et fondés sur le recours au protocole « 3D-Secure » en mode dit « débrayable », c'est-à-dire activé en fonction du niveau de risque estimé de chaque transaction.

Cette approche est conforme aux recommandations émises par l'Observatoire.

Toutefois, le secteur de la téléphonie se caractérise également par un recours important aux services de vente par téléphone et non par internet, par exemple pour le rechargement de comptes mobiles prépayés *via* un Serveur Vocal Interactif (SVI), pour lesquels la mise en œuvre du protocole « 3D-Secure » est globalement peu adaptée [6]. Or, au regard des informations partielles collectées par l'Observatoire, ce canal de vente supporterait la majeure partie de la fraude enregistrée en vente à distance par les opérateurs de téléphonie.

L'Observatoire appelle ces acteurs à poursuivre la mise en œuvre de solutions de lutte contre la fraude notamment en renforçant les contrôles effectués lors des achats par téléphone ou SVI (meilleures identifications de l'usager), afin de réduire l'exposition des porteurs légitimes de carte à la fraude.

4|3 Protection de la réémission des cartes SIM

La réémission de cartes SIM est une opération courante pour les opérateurs, qui représente un volume d'activité cumulé de plus de 2,5 millions d'opérations de ce type par trimestre.

Quatre canaux principaux sont utilisés dans le cadre des opérations de changement de carte SIM des clients d'opérateurs téléphoniques :

1. le SAV téléphonique de l'opérateur,
2. le canal agence physique,
3. le canal RIO (Relevé d'Identité Opérateur) [7],
4. le site web avec accès client.

Les données partielles collectées par l'Observatoire auprès des opérateurs de téléphonie ont permis de souligner l'existence de litiges portant sur des cas de réémission de cartes de SIM, dans des proportions n'excédant pas *a priori* 0,05 % des opérations de cette nature ; elles soulignent également que les canaux de réémission par SAV téléphonique et en agence physique seraient ceux qui généreraient le plus de litiges clientèle, tant en proportion qu'en nombre.

Les actions conduites en 2015 ont permis à l'Observatoire de sensibiliser les opérateurs de téléphonie à l'importance de la sécurisation des réémissions de cartes SIM au regard du rôle central joué par les lignes de téléphonie mobile dans les opérations d'identification à distance. Dans cette perspective, l'Observatoire appelle les opérateurs à renforcer la fiabilité des dispositifs permettant la réémission de cartes SIM en améliorant le processus d'identification des usagers, et assurera, en collaboration avec l'ARCEP, un suivi des solutions mises en œuvre par les opérateurs.

6 Cf. chapitre 3 – Solutions d'authentification.

7 Le RIO est un code à 12 chiffres nécessaire pour conserver la portabilité de son numéro. Il est obtenu en composant le 3179 à partir de la ligne mobile dont le client souhaite conserver le numéro. Suite à cet appel, le client reçoit un SMS avec son RIO et la date de fin d'engagement de son contrat. Le RIO est alors communiqué au nouvel opérateur qui s'occupera de transférer le numéro de mobile et de résilier le contrat auprès de l'ancien opérateur.

Statistiques de fraude pour 2015

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 méthodologie commune, dont les définitions et typologies sont décrites en annexe 6 du présent rapport, établie dès la première année de fonctionnement de l'Observatoire et dont la pertinence a été confirmée par une étude qualitative récemment conduite par le groupe de travail statistiques de fraude (cf. chapitre précédent).

Une synthèse des statistiques pour 2015 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 collectés dans le cadre du Système européen de banques centrales [1], les données concernant les seules cartes émises en France sont présentées séparément. Elles n'incluent donc pas la fraude subie en France par des cartes émises dans d'autres pays et que l'Observatoire recense par ailleurs. L'Observatoire publie également cette année des données complètes de fraude concernant les cartes de paiement sans contact, après la publication de données partielles dans son précédent rapport annuel. Enfin, en complément, une série d'indicateurs détaillés sont présentées dans l'annexe 5.

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 2015 portent ainsi sur :

- *576,4 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 71,7 millions de cartes de type « interbancaire » émises en France (dont 38,7 millions de cartes sans contact) ;*
- *15,7 milliards d'euros de transactions réalisées (principalement en France) avec 12,5 millions de cartes de type « privatif » émises en France ;*
- *43,9 milliards d'euros de transactions réalisées en France avec des cartes de paiement étrangères de types « interbancaire » et « privatif ».*

Les données recueillies proviennent :

- *des 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 ;*
- *de 9 émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance, Cofidis, Diners Club, Franfinance, JCB et UnionPay International.*

1 Cf. *Fourth report on card fraud*, juillet 2015, 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 2015, 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 416,1 millions d'euros, en augmentation de 5,2 % par rapport à 2014, pour un montant total de transactions qui atteint 592,2 milliards d'euros, en augmentation de 2,8 % par rapport à 2014.

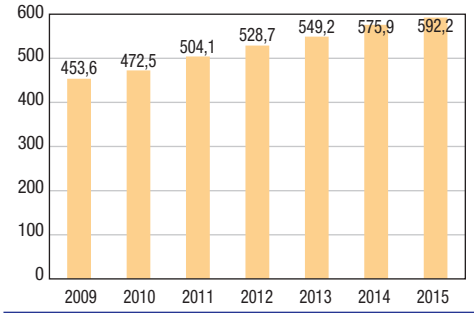
Compte tenu de ces éléments, **le taux de fraude sur les cartes de paiement françaises augmente légèrement à 0,070 %, contre 0,069 % en 2014.**

Le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2015 s'élève à 868 400, en baisse de 4,1 % par rapport à 2014.

Graphique 1

Évolution du montant des transactions des cartes françaises

(en milliards d'euros)

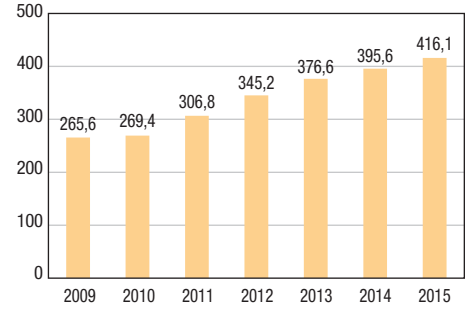


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 2

Évolution du montant de la fraude des cartes françaises

(en millions d'euros)

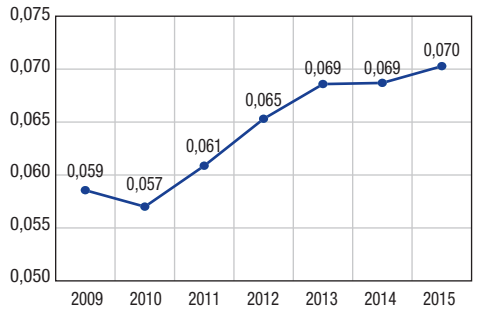


Source : Observatoire de la sécurité des cartes de paiement.

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 des cartes émises dans d'autres pays, le montant total de la fraude s'élève à 522,7 millions d'euros en 2015, en augmentation de 4,4 % par rapport à 2014, pour un montant total des transactions qui atteint 636,1 milliards d'euros, en augmentation de 1,8 %.

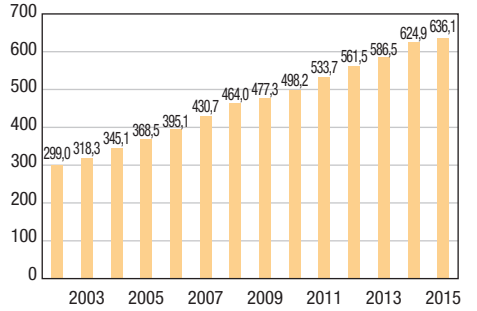
Compte tenu de ces éléments, **le taux de fraude global sur les transactions traitées dans les systèmes français**, comprenant les paiements et les retraits réalisés en France et à l'étranger avec des cartes françaises et les paiements et les retraits réalisés en France avec des cartes étrangères, **augmente légèrement à 0,082 %**.

Le montant moyen d'une transaction frauduleuse est resté stable, à 113 euros, contre 112 euros en 2014.

Graphique 4

Évolution du montant des transactions traitées dans les systèmes français

(en milliards d'euros)

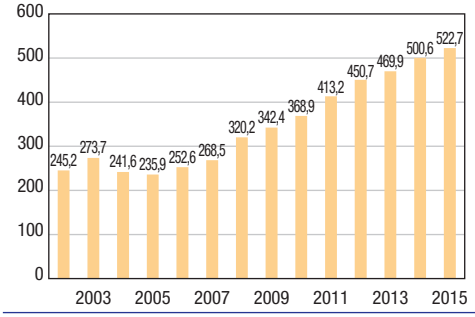


Source : Observatoire de la sécurité des cartes de paiement.

Graphique 5

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

(en millions d'euros)

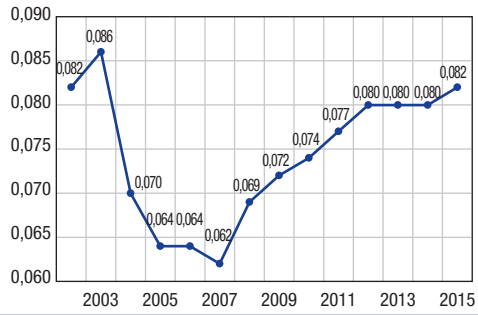


Source : Observatoire de la sécurité des cartes de paiement.

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 0,083 % en 2015, après avoir été stable à 0,080 % durant les trois années précédentes. Le taux de fraude pour les cartes de type « privatif » s'établit à 0,068 % en 2015 (contre 0,062 % en 2014), en augmentation après trois années consécutives de baisse.

Pour les cartes de type « interbancaire », la valeur moyenne des transactions frauduleuses est stable à 111 euros, contre 110 euros en 2014. Pour les cartes de type « privatif », la valeur moyenne des transactions frauduleuses diminue significativement à 250 euros, contre 298 euros en 2014.

Tableau 1

Répartition de la fraude par type de carte

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

	2011	2012	2013	2014	2015
Cartes de type « interbancaire »	0,077	0,080	0,080	0,080	**0,083**
	(394,9)	(434,4)	(455,8)	(486,4)	**(507,2)**
Cartes de type « privatif »	0,083	0,076	0,065	0,062	**0,068**
	(18,3)	(16,3)	(14,0)	(14,2)	**(15,5)**
Total	**0,077**	**0,080**	**0,080**	**0,080**	**0,082**
	(413,2)	**(450,7)**	**(469,9)**	**(500,6)**	**(522,7)**

Source : Observatoire de la sécurité des cartes de paiement.

3| Répartition de la fraude par zone géographique

En 2014, pour la première fois depuis la création de l'Observatoire, la fraude sur les transactions domestiques avait diminué. Cette tendance est confirmée en 2015 puisque **le montant de la fraude sur les transactions domestiques baisse de près de 10 millions d'euros** pour s'établir à 224,8 millions d'euros. Le taux de fraude est également en baisse à 0,040 % contre 0,043 % en 2014.

À l'inverse, **le montant de la fraude sur les transactions internationales [2] continue de progresser fortement** pour s'établir à 297,9 millions d'euros (+ 31,2 millions d'euros par rapport à 2014) et devient à nouveau [3] très sensiblement supérieur à celui de la fraude sur les transactions domestiques. En conséquence, le taux de fraude sur les transactions internationales est près de dix fois supérieur à celui sur les transactions domestiques.

Ainsi **les transactions internationales représentent 57,0 % du montant total de la fraude** alors qu'elles ne comptent que **pour 12,6 % de la valeur totale des transactions.**

On continue à observer, parmi ces transactions internationales, une meilleure maîtrise de la fraude sur les transactions réalisées avec la zone SEPA [4]

2 Concernant donc les cartes de paiement françaises utilisées à l'étranger ainsi que les cartes de paiement étrangères utilisées en France.
3 Le montant de la fraude domestique avait augmenté plus rapidement entre 2011 et 2013 pour s'établir à un niveau proche de celui des transactions internationales, avant de baisser à partir de 2014.
4 La zone SEPA comprend les 28 pays de l'Union européenne ainsi que Monaco, la Suisse, le Liechtenstein, la Norvège, l'Islande et Saint-Marin.

Tableau 2

Répartition de la fraude par zone géographique

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

	2011	2012	2013	2014	2015
Transactions domestiques	**0,044**	**0,045**	**0,046**	**0,043**	**0,040**
	(211,5)	**(226,4)**	**(238,6)**	**(234,6)**	**(224,8)**
Transactions internationales	**0,367**	**0,380**	**0,350**	**0,316**	**0,372**
	(201,7)	**(224,3)**	**(231,3)**	**(266,0)**	**(297,9)**
– dont carte française et accepteur hors SEPA	0,638	0,759	0,688	0,636	0,692
	(51,0)	(62,5)	(70,2)	(70,0)	(74,5)
– dont carte française et accepteur SEPA	0,255	0,316	0,366	0,374	0,459
	(44,3)	(56,3)	(67,9)	(91,0)	(116,8)
– dont carte étrangère hors SEPA et accepteur français	0,892	0,639	0,404	0,336	0,353
	(81,3)	(78,2)	(64,1)	(65,6)	(69,7)
– dont carte étrangère SEPA et accepteur français	0,122	0,132	0,135	0,134	0,153
	(25,1)	(27,3)	(29,1)	(39,3)	(36,9)
Total	**0,077**	**0,080**	**0,080**	**0,080**	**0,082**
	(413,2)	**(450,7)**	**(469,9)**	**(500,6)**	**(522,7)**

Source : Observatoire de la sécurité des cartes de paiement.

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 (0,692 %) reste très supérieur à celui des transactions effectuées au sein de la zone SEPA (0,459 %), même si l'écart tend à diminuer ;

• pour les cartes étrangères, le taux de fraude sur les transactions effectuées en France avec des cartes émises hors de la zone SEPA (0,353 %) est plus de deux fois supérieur à celui des cartes émises au sein de la zone SEPA (0,153 %).

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.

Dans ce contexte, les mesures incitatives décidées par Visa, MasterCard, American Express et Discover (Diners Club International) pour encourager l'adoption du standard EMV sur le plan international méritent d'être soulignées. En effet, la mise en œuvre depuis octobre 2015 [5] d'un transfert de responsabilité, en cas de fraude, de l'émetteur de la carte vers le commerçant si celui-ci n'a pas migré vers EMV, constitue une forte incitation pour que les émetteurs adoptent ce standard pour toutes les nouvelles cartes émises et pour que les commerçants fassent évoluer leurs terminaux. Aux États-Unis, près de 500 millions de cartes ont ainsi été renouvelées au standard EMV au cours de l'année 2015, soit environ la moitié du parc.

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.

5 Ces mesures de transfert de responsabilité sont déjà en vigueur en Europe depuis une dizaine d'années.

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 baisse à 0,009 %, soit un plus bas historique depuis la création de l'Observatoire.** Ces paiements représentent 66,4 %, soit près des deux tiers du montant des transactions nationales, pour seulement 15,4 % du montant de la fraude ;

• **le taux de fraude sur les retraits est en légère baisse pour s'établir à 0,033 %.** Cette baisse s'explique principalement par la baisse du nombre de piratages de distributeurs automatiques de billets, d'automates de paiement et de terminaux de points de vente (1 215 cas en 2015 contre 1 628 en 2014, soit une baisse de 25 %). Ces appareils restant cependant des cibles toujours privilégiées pour les réseaux de fraude organisée, l'Observatoire maintient ses conseils de prudence aux porteurs et rappelle les bonnes pratiques à suivre lors d'une opération de paiement chez un commerçant ou lors d'un retrait (cf. annexe 1).

• **le taux de fraude sur les paiements à distance, qui s'élève à 0,228 %, est également en baisse sensible** pour la quatrième année consécutive.

Toutefois, ce taux demeure plus de vingt fois supérieur au taux de fraude sur les paiements de proximité. Ainsi, **les paiements à distance, qui ne représentent que 11,9 % de la valeur des transactions domestiques, comptent pour plus de 66,9 % 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 est d'ailleurs venue appuyer ces recommandations.

Tableau 3

Répartition du taux de fraude domestique par type de transaction

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

	2011	2012	2013	2014	2015
Paiements	0,049	0,049	0,050	0,046	0,043
	(177,8)	(190,0)	(199,9)	(193,2)	(185,0)
– dont paiements de proximité et sur automate	0,015	0,015	0,013	0,010	0,009
	(48,1)	(51,2)	(45,8)	(37,1)	(34,6)
– dont paiements à distance	0,321	0,299	0,269	0,248	0,228
	(129,6)	(138,8)	(154,2)	(156,0)	(150,4)
– dont par courrier/téléphone	*0,259*	*0,338*	*1,122*	*0,147*	*0,208*
	(25,4)	*(29,4)*	*(29,2)*	*(2,8)* [a]	*(5,1)*
– dont sur internet	*0,341*	*0,290*	*0,229*	*0,251*	*0,229*
	(104,2)	*(109,4)*	*(125,0)*	*(153,2)* [a]	*(145,3)*
Retraits	0,029	0,031	0,033	0,034	0,033
	(33,7)	(36,4)	(38,6)	(41,5)	(39,9)
Total	**0,044**	**0,045**	**0,046**	**0,043**	**0,040**
	(211,5)	**(226,4)**	**(238,6)**	**(234,6)**	**(224,8)**

a) La diminution très importante entre 2013 et 2014, du montant de la fraude sur les paiements à distance effectués par courrier ou par téléphone, et à l'inverse l'augmentation de celle sur les paiements sur internet, s'expliquent pour grande partie par une modification de la méthodologie statistique utilisée par le Groupement des Cartes Bancaires (CB). Un ajustement plus léger a également été effectué en 2015. Cf. le rapport annuel 2014 pour plus de détails.

Source : Observatoire de la sécurité des cartes de paiement.

Encadré 2

Fraude aux paiements par carte sans contact

L'Observatoire a collecté, pour la deuxième année consécutive, les données permettant de mesurer le taux de fraude sur les paiements sans contact. Ainsi, sur l'ensemble de l'année 2015, 248,6 millions de paiements sans contact ont été enregistrés pour un montant total de 2 632,3 millions d'euros, soit un montant moyen de 10,6 euros par opération. Par ailleurs, un peu plus de 44 000 paiements frauduleux ont été recensés sur la même période pour un montant total de 0,5 million d'euros. Par conséquent ***le taux de fraude sur les transactions sans contact s'élève à 0,019 %*** *sur cette période. Il se maintient, comme en 2014, à un niveau intermédiaire entre le taux de fraude des paiements de proximité tous modes confondus (0,009 %) et celui des retraits (0,033 %), soit un niveau très inférieur à celui des paiements à distance (0,228 %).*

Comme en 2014, la fraude aux paiements sans contact a pour origine quasi exclusive le vol ou la perte de la carte. La fixation par les émetteurs de carte de plafonds sur le montant maximum d'une transaction unitaire (généralement fixé à 20 ou 25 euros) et sur le cumul des transactions consécutives pouvant être effectuées sans la saisie du code confidentiel (généralement fixé à 100 euros) permet en effet de limiter le préjudice subi en cas de perte ou de vol d'une carte.

L'Observatoire rappelle à cet effet 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 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 continu de fort développement du taux d'équipement des porteurs, avec désormais près de 40 millions de cartes disposant de la fonctionnalité de paiement sans contact en circulation à fin décembre 2015, l'Observatoire appelle les émetteurs à maintenir 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 paiement scripturaux, assure un suivi de la mise en œuvre de ces mesures.

1 Cf. détails en annexe 2.
2 Cf. 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. tableau 4), on remarque que la fraude sur les paiements à distance réalisés par les cartes françaises auprès des commerçants étrangers a très fortement augmenté en 2015 (138,2 millions d'euros, contre 104,5 millions d'euros en 2014 et 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 donc par le report des fraudeurs vers des sites étrangers moins sécurisés.

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	2012	2013	2014	2015
Paiements	0,687	0,547	0,532	0,735
	(37,8)	(40,3)	(41,7)	(56,3)
– dont paiements de proximité et sur automate	0,456	0,377	0,350	0,509
	(19,8)	(17,7)	(19,2)	(25,8)
– dont paiements à distance	1,551	0,848	0,960	1,174
	(18,0)	(22,6)	(22,5)	(30,5)
– dont par courrier/téléphone	*1,150*	*1,234*	*4,955*	*2,345*
	(4,0)	*(6,4)*	*(7,5)*	*(9,5)*
– dont sur internet	*1,720*	*0,755*	*0,682*	*0,959*
	(14,1)	*(16,2)*	*(14,9)*	*(21,1)*
Retraits	0,904	1,054	0,890	0,586
	(24,7)	(29,9)	(28,3)	(18,1)
Total	**0,759**	**0,688**	**0,636**	**0,692**
	(62,5)	**(70,2)**	**(70,0)**	**(74,5)**
Carte française – Accepteur étranger SEPA				
Paiements	0,372	0,434	0,434	0,526
	(55,3)	(66,8)	(89,8)	(115,7)
– dont paiements de proximité et sur automate	0,131	0,089	0,067	0,071
	(11,7)	(8,2)	(7,8)	(8,0)
– dont paiements à distance	0,735	0,937	0,910	1,004
	(43,6)	(58,6)	(82,0)	(107,7)
– dont par courrier/téléphone	*0,532*	*1,566*	*1,317*	*1,399*
	(6,5)	*(11,3)*	*(13,9)*	*(18,7)*
– dont sur internet	*0,788*	*0,856*	*0,856*	*0,948*
	(37,1)	*(47,3)*	*(68,1)*	*(89,0)*
Retraits	0,036	0,036	0,033	0,033
	(1,1)	(1,1)	(1,2)	(1,1)
Total	**0,316**	**0,366**	**0,374**	**0,459**
	(56,3)	**(67,9)**	**(91,0)**	**(116,8)**

Source : Observatoire de la sécurité des cartes de paiement.

La perspective de l'entrée en vigueur de la deuxième directive sur les services de paiement, qui impose, pour les opérations de paiement électronique à distance, l'authentification forte du porteur comprenant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés (cf. chapitre 3), devrait toutefois permettre d'infirmer cette tendance en Europe.

Par ailleurs, on note la stabilité à des niveaux modérés de la fraude pour les opérations de proximité (paiements et retraits) effectuées au sein de l'espace SEPA, où l'utilisation des standards EMV est généralisée. En particulier pour les cartes françaises, le taux de fraude sur les retraits effectués en zone SEPA (0,033 %) est plus de quinze fois inférieur à celui des retraits effectués hors zone SEPA (0,586 %), pour lesquels la lecture de la piste magnétique est encore couramment utilisée par les automates bancaires de certains pays. Cet écart tend toutefois à diminuer, grâce notamment à l'amélioration des outils de détection des tentatives de fraude par contrefaçon de piste magnétique.

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	2012	2013	2014	2015
Paiements	0,735	0,451	0,380	0,391
	(77,7)	(63,2)	(65,0)	(68,0)
– dont paiements de proximité et sur automate	0,353	0,230	0,162	0,168
	(30,3)	(25,3)	(21,9)	(22,7)
– dont paiements à distance	2,378	1,268	1,213	1,190
	(47,4)	(37,9)	(43,1)	(45,3)
– dont par courrier/téléphone	0,737	*0,930*	*1,018*	*1,173*
	(8,8)	*(9,2)*	*(7,7)*	*(10,8)*
– dont sur internet	4,833	*1,436*	*1,265*	*1,195*
	(38,6)	*(28,7)*	*(35,4)*	*(34,5)*
Retraits	0,033	0,051	0,026	0,069
	(0,6)	(0,9)	(0,6)	(1,6)
Total	**0,639**	**0,404**	**0,336**	**0,353**
	(78,2)	**(64,1)**	**(65,6)**	**(69,7)**
Carte étrangère SEPA – Accepteur français				
Paiements	0,158	0,158	0,156	0,175
	(26,6)	(28,2)	(38,5)	(36,0)
– dont paiements de proximité et sur automate	0,046	0,039	0,026	0,033
	(5,7)	(4,9)	(5,1)	(4,8)
– dont paiements à distance	0,466	0,458	0,476	0,529
	(20,9)	(23,2)	(33,1)	(31,3)
– dont par courrier/téléphone	0,216	*0,308*	*0,397*	*0,736*
	(3,8)	*(3,8)*	*(4,8)*	*(7,7)*
– dont sur internet	0,626	*0,506*	*0,492*	*0,484*
	(17,1)	*(19,4)*	*(28,6)*	*(23,6)*
Retraits	0,017	0,025	0,018	0,025
	(0,7)	(0,9)	(0,9)	(0,9)
Total	**0,132**	**0,135**	**0,134**	**0,153**
	(27,3)	**(29,1)**	**(39,3)**	**(36,9)**

Source : Observatoire de la sécurité des cartes de paiement.

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, parts en %)

Secteur	Montant de fraude	Part du secteur dans la fraude
Services aux particuliers et aux professionnels	36,8	24,5
Commerce généraliste et semi-généraliste	31,8	21,2
Voyage, transport	26,4	17,6
Téléphonie et communication	23,4	15,6
Équipement de la maison, ameublement, bricolage	10,6	7,1
Produits techniques et culturels	8,2	5,5
Divers	5,2	3,5
Approvisionnement d'un compte, vente de particulier à particulier	2,5	1,7
Jeu en ligne	2,3	1,5
Santé, Beauté, Hygiène	1,6	1,1
Alimentation	0,9	0,6
Assurance	0,4	0,3
Total	**150,0**	**100,0**

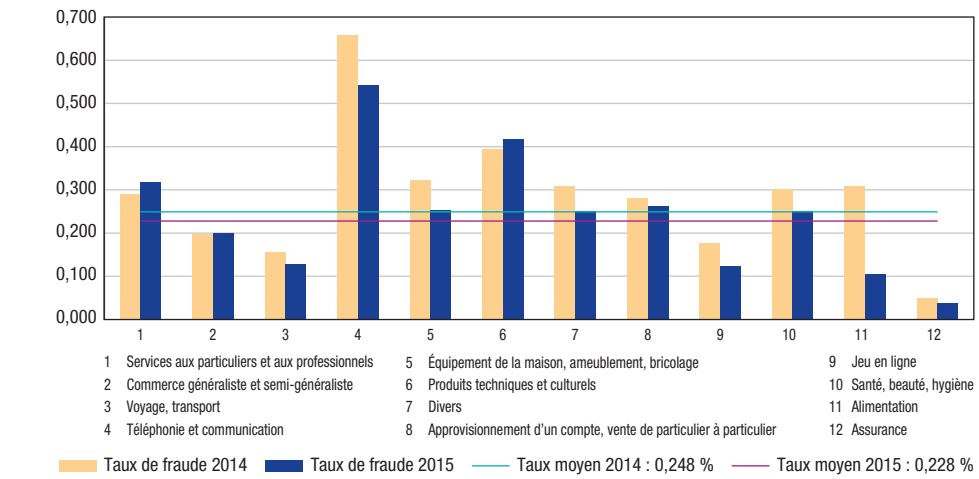
Les secteurs « Services aux particuliers et aux professionnels », « Commerce généraliste et semi-généraliste », « Voyage/transport » et « Téléphonie et communication » demeurent les plus exposés, et concentrent 78,9 % du montant de la fraude en vente à distance.

Malgré une légère baisse en 2015, le secteur « Téléphonie et communication » se maintient à un taux de fraude très supérieur à la moyenne (cf. graphique infra*). L'Observatoire appelle tout particulièrement les acteurs de ce secteur à renforcer les mesures visant à lutter contre la fraude (cf. chapitre 1).*

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.*

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 [6] ou de programmation ; une carte entièrement fausse est réalisée à partir de données recueillies par le fraudeur ;

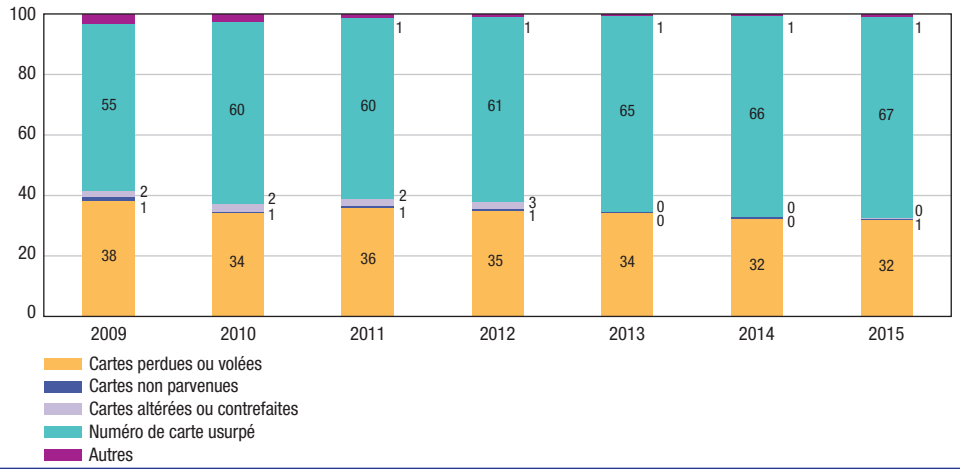
• numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé ensuite en vente à distance.

Le graphique 7 et le tableau 5 indiquent 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).

Graphique 7

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement.

Tableau 5

Répartition de la fraude domestique selon son origine et par type de carte en 2015

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

	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	71,5	31,8	70,8	32,1	0,6	14,8
Carte non parvenue	1,2	0,5	0,7	0,3	0,5	11,6
Carte altérée ou contrefaite	0,2	0,1	0,1	0,1	0,1	2,6
Numéro usurpé	150,2	66,8	148,7	67,4	1,5	34,3
Autres	1,8	0,8	0,2	0,1	1,6	36,7
Total	224,8	100,0	220,5	100,0	4,4	100,0

Source : Observatoire de la sécurité des cartes de paiement.

6 Technique permettant l'impression graphique en relief des numéros d'une carte de paiement.

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux à distance reste la principale origine de la fraude (66,8 % en montant), en légère augmentation par rapport à 2014 (66,4 %).

La fraude liée aux pertes et vols de cartes représente toujours près du tiers de la fraude sur les transactions domestiques (31,8 %). Cette part est toutefois en régression continue depuis quatre années (36,1 % en 2011).

La contrefaçon de cartes n'est à l'origine que de 0,1 % des paiements domestiques frauduleux. Ce niveau très bas s'explique principalement par l'adoption de technologies de cartes à puce par le plus grand nombre de systèmes de cartes privatives et par le renforcement de la sécurité des cartes à puce EMV existantes [7].

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

Encadré 4

Indicateurs des services de police et de gendarmerie

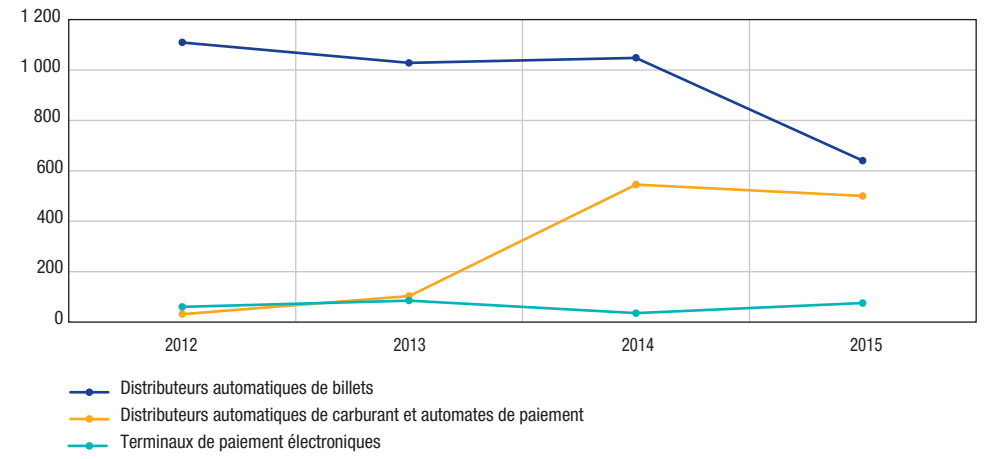
Pour l'année 2015, les services de police et de gendarmerie ont enregistré 47 000 faits relatifs à la fraude à la carte de paiement, en augmentation de 10 % par rapport à 2014. Sur la totalité des infractions recensées, 5 % ont donné lieu à l'interpellation de leurs auteurs présumés, permettant la résolution de 6 % des enquêtes initiées.

Le nombre de piratages de distributeurs automatiques de billets (DAB) est en baisse très sensible avec 640 cas en 2015 (contre environ 1 000 cas par an entre 2012 et 2014, autour de 500 cas par an entre 2011 et 2006, 200 en 2005 et seulement 80 cas en 2004). À ceux-ci s'ajoutent 575 piratages ciblant les points de vente (contre 540 en 2014), dont 440 piratages de distributeurs automatiques de carburant (DAC), 60 d'automates de paiement (tels les bornes de parking) et 75 de terminaux de paiement chez les commerçants. Malgré une baisse encourageante, ces chiffres demeurent élevés et confirment dans les faits l'intérêt constant que portent les réseaux criminels à la collecte des données de carte. Ces données sont ensuite exploitées :

- *soit pour contrefaire des cartes à piste magnétique qui seront utilisées pour des paiements et des retraits à l'étranger, principalement dans les pays où la technologie de carte à puce EMV est encore 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



Travaux de veille technologique

1| La sécurisation du paiement au point de vente en mode sans contact

1|1 Les différentes solutions de paiement de proximité en mode sans contact

Les travaux de veille technologique conduits par l'Observatoire à propos du développement de techniques de paiement de proximité par carte en mode sans contact ont été initiés dès 2004, en anticipation de leur mise en œuvre. L'Observatoire a ainsi régulièrement publié plusieurs analyses relatives à l'évolution des mécanismes d'initiation des paiements de proximité par carte en mode sans contact et à leurs conditions de sécurisation.

Le standard de communication NFC (*Near Field Communication*, « Communication en champ proche ») est aujourd'hui le système le plus déployé, tant en France qu'au niveau international, du fait de son intégration aux standards EMV [1]. On parle ainsi généralement de cartes compatibles NFC EMV.

Pour rappel, la technologie NFC permet à deux équipements distants de quelques centimètres d'échanger des informations [2]. Moyennant certaines contraintes, il est possible de faire communiquer un terminal bénéficiant d'une alimentation électrique avec un équipement qui en est dépourvu, comme c'est le cas pour un paiement de proximité avec une carte de paiement NFC EMV.

Lors d'une transaction sans contact, le terminal commence par entrer en relation avec la carte de paiement qui transmet une liste de données permettant au terminal de déterminer si la transaction peut être réalisée en mode sans contact, si elle nécessite une demande d'autorisation à l'émetteur, si elle doit être refusée, ou si la carte doit être insérée dans le lecteur de carte à puce pour saisie du code confidentiel.

De plus en plus de modèles de *smartphones*, voire d'objets connectés tels que les montres ou bracelets, permettent d'échanger des données selon le même standard NFC. Ce contexte technologique a mené les acteurs de différents marchés (fabricants de terminaux, opérateurs, réseaux de cartes, banques) à envisager le développement de solutions de paiement qui substitueraient un objet doté de cette technologie à la carte de paiement sans contact. Ces solutions présentent l'avantage de pouvoir être acceptées sur les mêmes terminaux de paiement sans contact.

En effet, l'acceptation des paiements sans contact NFC nécessite de disposer d'un terminal équipé des composants propres à la technologie NFC, tels qu'une antenne adéquate. Il est à noter que tous les fabricants de terminaux de paiement proposent désormais des modèles compatibles avec cette technologie, et que près de 29 % des commerces français en sont maintenant équipés, avec une perspective de déploiement couvrant l'ensemble du parc à horizon 2020.

1|2 État des lieux du déploiement du paiement de proximité par carte sans contact en France [3]

1|2|1 Émission

La Banque de France collecte auprès des principaux établissements bancaires de la Place les données de suivi du déploiement des cartes interbancaires de paiement sans contact NFC EMV. À noter qu'il n'existe pas à ce jour de collecte statistique globale relative au paiement de proximité sans contact toutes technologies (intégrant les technologies de type BLE ou QR *code* par exemple – cf. encadré 1) et toutes solutions confondues (carte, virements, monnaie électronique, etc.).

1 Le standard international EMV est maintenu par EMVCo. dont les membres sont American Express, Discover, JCB, MasterCard, UnionPay et Visa.
2 Cf. *Rapport annuel 2012*, chapitre 3, partie 1|2, Évolutions récentes (2009-2013).
3 À l'exception des données de fraude, les chiffres et histogrammes présentés dans cette section du rapport correspondent à l'activité enregistrée par le GIE Cartes Bancaires, qui comptabilise 90 % des cartes sans contact émises et la totalité des terminaux de paiement en France.

Encadré 1

Les autres technologies utilisées pour le paiement de proximité sans contact

Bien que le standard NFC EMV soit utilisé pour une très large majorité des paiements sans contact au point de vente en France, d'autres technologies sont expérimentées :

- *lecture et affichage d'image (QR* code, *codes-barres, etc.) : ce système de mise en relation entre le commerçant et le client consiste à initier une opération de paiement par la photographie ou le* scan *d'un code image. D'une manière générale, cette technologie nécessite de disposer de terminaux supportant la lecture ou l'affichage de codes images tels que des codes-barres à une ou deux dimensions ;*

- *le* Bluetooth Low Energy *(BLE) : cette technologie de communication autorise une distance de quelques dizaines de centimètres, mais nécessite que les équipements soient autoalimentés en énergie. L'utilisation de cette technologie requiert que le terminal du commerçant soit équipé d'une balise BLE ;*

- *la génération d'impulsions électromagnétiques : cette technologie permet d'échanger des informations avec un lecteur de piste magnétique sans passer de carte à piste dans le lecteur. Associée à certains* smartphones, *elle est compatible avec tous les terminaux de paiement électronique équipés de lecteur de piste accessible* [1] *dès lors que l'application respecte le format de données utilisé pour les cartes de paiement. Du fait des règles d'acceptation imposant l'usage de la puce EMV en France, cette technologie ne peut pas être utilisée par des porteurs de cartes françaises en France, mais elle pourrait éventuellement être utilisée par des porteurs de cartes étrangères sur des terminaux de commerçants français ou des porteurs de cartes françaises à l'étranger.*

Il est à noter que les solutions mettant en œuvre ces technologies n'entraînent pas toutes un paiement par carte : elles peuvent également être utilisées pour initier un ordre de virement ou de prélèvement, ou un paiement en monnaie électronique. Par ailleurs, la majorité de ces technologies n'ont pas fait l'objet d'une diffusion massive dans le domaine du paiement, ce qui fait que les différentes solutions expérimentées utilisent des formats ou des cinématiques de paiement divers.

1 Certains automates dans lesquels la carte est entièrement introduite pourraient ne pas être compatibles.

Concernant le paiement de proximité par carte sans contact, près de 40 millions de cartes de paiement sont équipées de la fonctionnalité en juin 2015. Le nombre de porteurs équipés est en régulière augmentation.

Le nombre de cartes de paiement sans contact actives (au moins un paiement réalisé dans le mois) suit également une évolution favorable et se situe autour de 11,5 millions de porteurs à fin 2015.

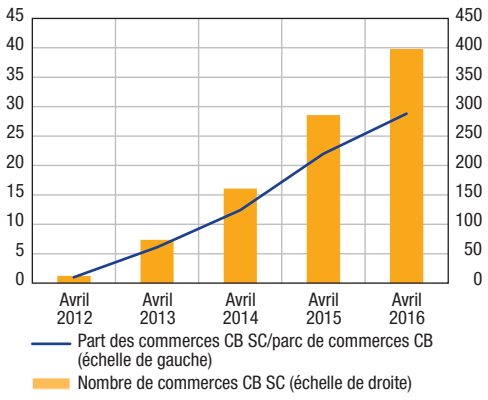
1|2|2 Acquisition

Le nombre de terminaux d'acceptation sans contact se situe aux alentours de 560 000 (réalisation d'au moins une transaction sans contact depuis l'installation du terminal), soit près de 29 % des commerçants de proximité. Environ 56 % de ces

Graphique 1

Évolution du parc d'acceptation

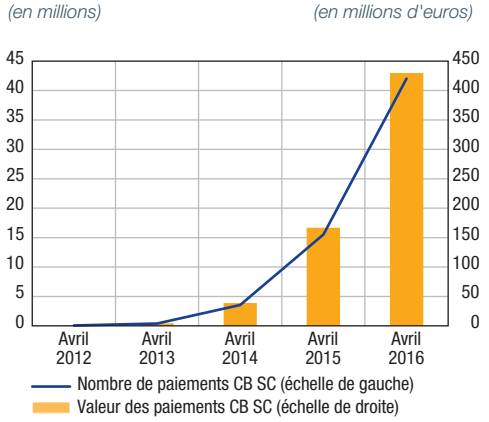
(en %) *(en milliers)*



Source : GIE Cartes Bancaires.

Graphique 2

Évolution du nombre de transactions



Source : GIE Cartes Bancaires.

contrats sont considérés comme actifs (au moins une transaction sans contact réalisée sur le mois).

1|2|3 Paiements

En juillet 2015, le nombre de paiements de proximité sans contact mensuel franchissait la barre des 20 millions, pour un montant d'environ 215 millions d'euros.

Le groupement d'intérêt économique Cartes Bancaires relève qu'en moyenne près de 1,4 million de transactions sans contact sont réalisées chaque jour, ce qui représente plus de 30 % des transactions CB éligibles (c'est-à-dire, pour des montants inférieurs au plafond de paiement sans contact de 20 euros).

1|2|4 Fraude

Dans le cadre de l'OSCP, la Banque de France recense depuis 2015 la fraude concernant les paiements de proximité sans contact. Les principaux groupes bancaires français ont indiqué ne pas subir de fraude significative sur ces paiements. Leur taux de fraude ressort en effet à 0,019 %, soit un niveau proche de celui des paiements de proximité (transactions « puce avec saisie du code confidentiel ») et inférieur à celui des retraits, avec des cas de fraude uniquement liés à la perte ou au vol de la carte. Il est à noter que, du fait du faible volume de transactions sans contact, ce taux de fraude ne représente qu'un montant de l'ordre de 42 000 euros mensuel pour l'ensemble de la Place.

Ce constat atteste qu'aucune faille technologique inhérente à la technologie NFC n'a pu, à ce jour, être exploitée par les fraudeurs, ce qui confirme l'analyse sécuritaire réalisée par l'Observatoire.

1|3 Enjeux sur la sécurité des paiements de proximité sans contact

1|3|1 Rappel des recommandations de l'Observatoire applicables aux paiements de proximité en mode sans contact

L'Observatoire a déjà publié plusieurs analyses de sécurité dans ses rapports annuels 2007, 2009 et 2012 (paiements NFC EMV par carte ou par mobile). Les principales recommandations émises par l'Observatoire visent à :

• proposer des solutions simples permettant d'activer, de désactiver ou d'empêcher l'utilisation de l'application bancaire sans contact sur une carte (étuis protecteurs, scripts EMV [4], émission de cartes non compatibles NFC à la demande [5], etc.) ;

• mettre en place des mesures de sécurité complémentaires, notamment dans le but de désensibiliser ou protéger les identifiants de carte utilisés :

- utiliser un numéro de la carte (PAN [6]) dédié au paiement de proximité sans contact : cette recommandation fait l'objet de travaux de la

4 Un script EMV est une suite d'instructions envoyées par l'émetteur de la carte dans la réponse à la demande d'autorisation. Dans le cas présent, ces instructions ont pour but de désactiver l'interface sans contact de l'application bancaire. De cette manière, la carte répond toujours à une sollicitation NFC par des informations techniques mais le dialogue cesse avant la transmission de toute donnée personnelle ou bancaire. Si besoin, un script de la banque émettrice peut réactiver l'interface sans contact de l'application bancaire.

5 Il peut s'agir selon les cas soit de cartes non équipées d'une antenne NFC, soit de cartes intégrant une antenne NFC mais dont l'application sans contact est inactivable, rendant impossible tout échange de données bancaires en mode NFC.

6 *Personnal Account Number*.

Encadré 2

Une mesure de sécurisation : la « tokenisation »

La « tokenisation » consiste à remplacer le numéro de carte (ou PAN) par un numéro de substitution, appelé jeton ou token *de paiement, dans la chaîne de paiement. Ce* token *est dédié à une utilisation spécifique et peut être à usage unique (PAN émis pour une transaction dédié) ou récurrent (par exemple, PAN dédié aux paiements de proximité sans contact par carte). Cette mesure permet de stocker et de communiquer un « numéro de carte » qui ne pourra pas être détourné pour une autre transaction ou pour un autre mode de paiement. L'établissement émetteur ou son prestataire alimente le dispositif en délivrant les* tokens *et en assurant la correspondance avec le PAN de la carte.*

part des acteurs, dans le cadre plus global du développement des techniques de « tokenisation » (cf. encadré 2).

- chiffrer les communications entre la carte sans contact et le terminal de paiement : le standard NFC EMV actuel ne prévoit pas cette possibilité ; cette fonctionnalité sera disponible dans le cadre de la future mise à jour du standard EMV, dit EMV NextGen. Il est toutefois à noter que l'implémentation de ce nouveau standard supposera une mise à niveau à la fois des cartes et des terminaux, et entraînera donc une migration sur plusieurs années.

Par ailleurs, la Commission nationale Informatique et Libertés (CNIL) a publié fin 2012 une recommandation imposant aux émetteurs de cartes sans contact d'empêcher l'accès au nom du porteur et à son historique de transactions par l'interface sans contact. Les évolutions des caractéristiques techniques des cartes survenues depuis 2012 ont permis de répondre à cette recommandation :

• depuis septembre 2012, les cartes émises ne transmettent plus l'identité du porteur. En prenant en compte la durée de vie maximale d'une carte, depuis septembre 2015, plus aucune carte de paiement française en circulation ne transmet l'identité du porteur *via* l'interface sans contact ;

• depuis la mi-2013, les nouveaux modèles de cartes agréés ne permettent plus d'accéder à l'historique des transactions. Les cycles de renouvellement entraîneront une mise en conformité de l'ensemble du parc d'ici la fin de l'année 2016.

1|3|2 Enjeux de sécurisation des dispositifs de paiement par carte en mode NFC avec un téléphone mobile

La généralisation de l'implémentation de puces NFC au sein d'objets connectés – en particulier les *smartphones* – et du développement d'applications de paiement par carte s'appuyant sur cette technologie, a fait émerger une nouvelle catégorie de dispositifs de paiement de proximité sans contact qui viennent se substituer à la carte. Il faut noter que ces dispositifs ne sont pas nativement liés à un porteur lors de leur émission. Dans la plupart des cas, une opération ultérieure dite d'enrôlement permettra de mettre en service ce mode de paiement. En matière de sécurité, ce processus d'enrôlement doit être suffisamment sécurisé pour ne pas permettre à un fraudeur d'enregistrer des données de cartes usurpées.

En outre, une solution de paiement par téléphone portable de ce type doit être en mesure de gérer toutes les étapes du cycle de vie du dispositif, telles que, par exemple :

- la revente du téléphone,
- la panne/le remplacement du téléphone,
- la perte ou le vol du téléphone,
- la perte ou le vol de la carte de paiement,
- l'expiration de la carte de paiement, etc.

Enfin, la solution de paiement doit être suffisamment robuste pour être mise en œuvre avec un équipement qui, par opposition à la carte, n'est généralement pas la propriété de l'émetteur de la carte de paiement, tout en garantissant un niveau de sécurité équivalent à la carte de paiement « Puce et code confidentiel » pour le porteur.

Pour répondre à ces différentes exigences de sécurité, deux modèles distincts d'architecture font l'objet de développements et d'expérimentations de la part des acteurs de marché :

• **une sécurité fondée sur un élément physique sécurisé (SE pour *Secure Element*).**

L'application de paiement mobile et les données sensibles bancaires sont stockées dans un composant physique sécurisé, qui peut être selon les cas une puce non amovible intégrée au téléphone par le fabricant (dit *Embedded SE*) ou la carte SIM de l'opérateur (dit S*IM based*).

Dans ce modèle, l'accès à l'élément sécurisé est restreint : toute application y accédant doit avoir été acceptée par le « propriétaire » de l'élément, ce qui suppose selon les cas soit un partenariat entre l'émetteur de la carte de paiement et le fabricant du mobile (puce intégrée au téléphone), soit un accord entre l'émetteur et l'opérateur de téléphonie mobile (carte SIM). Afin d'éviter tout risque d'attaque logicielle, la puce intégrée par le fabricant ou la carte SIM communique directement avec le contrôleur NFC du téléphone mobile sur un canal sécurisé dédié aux opérations de paiement.

- **une sécurité fondée sur des solutions logicielles présentes sur le téléphone et dans le *cloud* informatique (HCE pour *Host Card Emulation*).**

Par opposition au modèle précédent, l'application de paiement mobile s'appuie principalement sur des composants logiciels répartis entre l'application de paiement et des serveurs distants. La solution de paiement mobile doit tenir compte des vulnérabilités intrinsèques de l'environnement, notamment du système d'exploitation des *smartphones*. La sécurité de la solution dans sa globalité repose à la fois sur les mécanismes de sécurité mis en œuvre au niveau de l'application de paiement mais aussi sur les applications et serveurs en charge de l'authentification du mobile et du chargement régulier des éléments sensibles utilisés par l'application de paiement. D'autres mécanismes de sécurité sont également mis en œuvre au niveau transactionnel.

1|4 Mesures de sécurité recommandées par l'Observatoire

1|4|1 Mesures de protection relatives aux cartes

L'Observatoire a demandé aux banques d'offrir la possibilité aux porteurs de désactiver ou empêcher le paiement NFC EMV, que ce soit par la distribution d'étuis de protection ou la désactivation des applications NFC EMV intégrées aux cartes par script EMV (la carte voit son application de paiement NFC désactivée lors de la demande d'autorisation suivante pour un paiement ou un retrait). Les groupes bancaires français ont mis en place l'une ou l'autre de ces deux solutions, parfois les deux.

Encadré 3

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

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

*À l'instar des cartes de paiement à puce EMV, les **solutions fondées sur un composant sécurisé physique** doivent faire l'objet d'une évaluation du composant qui garantit un niveau de sécurité élevé (certification EAL4+ délivrée par l'ANSSI [1] ou équivalent).*

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

1 Cf. note de bas de page n° 14.

L'Observatoire rappelle par ailleurs qu'une carte de paiement reste toujours la propriété de la banque émettrice. À ce titre, toute atteinte à l'intégrité de celle-ci est à proscrire (par exemple, destruction volontaire d'un composant de la carte, telle l'antenne NFC).

1|4|2 Recommandations pour le déploiement de solutions non cartes

L'Observatoire note que la généralisation de la technologie NFC au sein des *smartphones* ou d'autres objets connectés et le développement d'applications dédiées au paiement s'appuyant sur cette technologie permettent le développement de nouvelles solutions de paiement de proximité en mode sans contact de type NFC EMV utilisant des supports numériques se substituant physiquement à la carte.

L'Observatoire encourage les acteurs à innover dans ce domaine, tout en rappelant que le déploiement d'une solution de paiement de proximité sans contact non carte doit être conditionné à l'assurance d'un niveau de sécurité équivalent à celui des paiements par carte en mode NFC. Pour ce faire, l'Observatoire souligne le besoin de disposer de référentiels de sécurité adaptés à ces nouveaux dispositifs de paiement de proximité, et permettant d'évaluer et de certifier les solutions proposées. Ces référentiels devront s'attacher à la fois à apporter une vision du niveau global de sécurité offert par ces dispositifs indépendamment de leur architecture, et à couvrir la totalité du cycle de vie du système, de sa mise en service par enrôlement des données de carte de l'utilisateur à son extinction.

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

Par ailleurs, l'Observatoire rappelle son attachement au développement de solutions de « tokenisation », qui sont à même d'apporter un niveau de sécurisation supplémentaire en réservant l'utilisation du numéro de carte à l'utilisation en mode contact.

2| Le développement de nouvelles solutions d'authentification des paiements à distance

2|1 Introduction

La sécurisation des paiements par carte en vente à distance, notamment sur internet, a fait l'objet dès 2008 de plusieurs recommandations de l'Observatoire visant à mettre en œuvre une authentification renforcée du payeur. Les méthodes d'authentification étant laissées au libre choix des émetteurs, plusieurs d'entre elles ont été déployées et proposées aux porteurs de carte. L'Observatoire avait à ce titre dressé un état des lieux de ces méthodes dans son rapport annuel de 2013.

Parallèlement, le forum européen sur la sécurité des paiements de détail (forum *SecuRe Pay* [7]) a défini un ensemble de recommandations et de bonnes pratiques sur la sécurité des paiements par internet qui a été publié en janvier 2013 par la Banque centrale européenne. Celles-ci sont entrées en vigueur le 1er février 2015, et ont été retranscrites par l'Autorité bancaire européenne (ABE) dans ses orientations sur la sécurité des paiements sur internet publiées en décembre 2014. Ces recommandations, en particulier celles visant à sécuriser l'enrôlement du porteur et à l'équiper d'une solution d'authentification forte [8] pour les paiements à distance, rejoignent les recommandations émises jusqu'alors par l'Observatoire.

Enfin, le 13 janvier 2016, la Commission européenne a publié la deuxième directive sur les services de paiement (dite DSP2) qui définit la notion d'authentification forte du porteur en s'appuyant sur la définition du forum *SecuRe Pay*, et en généralise l'utilisation pour l'initiation des

7 Ce forum, co-présidé par la Banque centrale européenne et l'Autorité bancaire européenne, réunit banquiers centraux et superviseurs bancaires autour des sujets relatifs à la sécurité des moyens de paiement de détail.

8 *Strong customer authentication*.

paiements à distance. La DSP2 prévoit par ailleurs qu'avant la date limite de sa transposition en droit national (en décembre 2017) des normes techniques de régulation (RTS) élaborées par l'ABE en collaboration avec les banques centrales viennent préciser les modalités et conditions de mise en œuvre de l'authentification forte des porteurs. Ces RTS, en cours d'élaboration au sein du forum *SecuRe Pay*, seront soumises à consultation publique avant la fin de l'année 2016.

Dans ce contexte, les émetteurs ont réalisé d'importants efforts pour sécuriser les paiements sur internet, largement majoritaires parmi les paiements à distance [9], et qui ont conduit à la quasi-généralisation de l'équipement des porteurs en dispositif d'authentification non rejouable (environ 96 % de porteurs équipés), ainsi qu'à l'équipement progressif des commerçants (66 % à fin 2015). Ces évolutions ont contribué à faire diminuer de façon continue le taux de fraude sur les paiements à distance ces dernières années, de 0,321 % en 2011 à 0,228 % en 2015. Malgré cette évolution positive, l'Observatoire constate toujours un écart important [10] entre les taux de fraude observés sur les paiements de proximité et ceux réalisés en vente à distance, notamment sur internet [11]. Cette préoccupation a par ailleurs été prise en compte dans la stratégie nationale des paiements [12] présentée par le ministre Michel Sapin en octobre 2015, laquelle préconise de généraliser l'authentification renforcée lors des paiements électroniques [13].

La présente étude vise à dresser un état des lieux des techniques d'authentification forte des porteurs mises en œuvre ou envisagées par les systèmes de paiement par carte et émetteurs français dans le cadre des paiements à distance, ainsi que les mesures complémentaires qui participent à la sécurité des paiements par carte.

2|2 Caractéristiques de l'authentification forte du porteur

L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement, elle est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté préalablement [14] (par exemple un identifiant ou un numéro de carte). S'il est aisé de définir l'authentification statique par l'utilisation d'un simple mot de passe, l'authentification forte fait appel à des concepts qu'il est nécessaire de préciser.

Dans la DSP2, l'authentification forte du client est définie comme *« une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification »*.

Par ailleurs, l'article 97 de la DSP2 précise que *« pour les opérations de paiement électronique à distance, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés »*. De cette manière, la DSP2 va plus loin que les recommandations du forum *SecuRe Pay*, qui imposait seulement qu'au moins l'un des éléments d'authentification soit non rejouable (sauf dans le cas de recours à la biométrie), en ajoutant une exigence supplémentaire de lien entre les éléments d'authentification et les données de la transaction pour les paiements à distance.

9 Cf. annexe 5 « Dossier statistique ».
10 Cf. chapitre 2.
11 Cf. annexe 5 « Dossier statistique ».
12 *http://www.economie.gouv.fr/files/files/PDF/Strategienationale_sur_moyens_de_paiement_102015.pdf*
13 Cf. 1re action du « 2e axe : Renforcer la sécurité des moyens de paiement ».
14 Définition ANSSI (*http://www.ssi.gouv.fr/entreprise/glossaire/a/*).

Ainsi, l'utilisation en paiement de proximité de la carte à puce assortie de la saisie d'un code confidentiel, ou code PIN (*Personal Identification Number*), pour valider un paiement correspond bien à la définition de l'authentification forte : elle s'appuie en effet sur la connaissance du code confidentiel et la possession d'une carte, et répond même à l'article 97 dans la mesure où la puce de la carte génère un certificat propre à la transaction.

Les chapitres suivants visent à présenter les solutions d'authentification forte mises en place ces dernières années dans le cadre des paiements à distance, ainsi que les solutions actuellement en devenir.

2|3 Les premières solutions de paiement mises en œuvre pour la « vente à distance sécurisée » [15]

2|3|1 Le protocole « 3D-Secure »

Suite au constat des limites de la sécurisation apportée par le cryptogramme visuel présent au dos des cartes de paiement dans la lutte contre la fraude sur les paiements à distance, les réseaux internationaux ont déployé un protocole dédié à la sécurisation des paiements sur internet initiés à partir d'un navigateur, appelé « 3D-Secure ». Ce protocole déployé au début des années deux mille sépare la chaîne de paiement par carte en trois domaines :

- le domaine acquéreur, qui comprend le commerçant et sa banque ;
- le domaine émetteur, qui comprend le client (porteur d'une carte de paiement) et sa banque ;
- le domaine interbancaire, qui fait le lien entre la banque du commerçant et la banque du porteur.

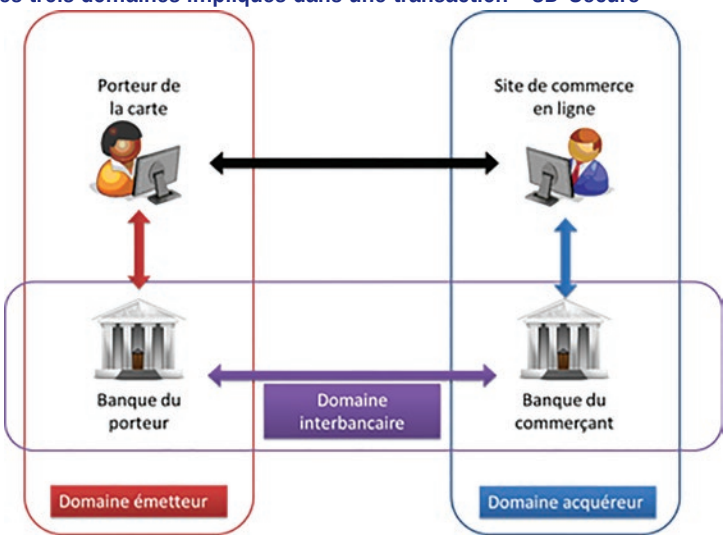
Selon ce découpage :

- dans le domaine acquéreur, le commerçant est reconnu par sa banque qui certifie sa légitimité ;
- l'authentification du porteur relève du domaine émetteur ;
- le protocole permet la création d'une passerelle entre le porteur et sa banque lors du paiement pour que cette dernière puisse l'authentifier.

Le protocole « 3D-Secure » a été développé pour être indépendant de la technique d'authentification implémentée et permettre à chaque émetteur de carte de choisir celle(s) qui lui convien(nen)t le mieux.

Schéma

Présentation des trois domaines impliqués dans une transaction « 3D-Secure »



15 Cf. Chapitre 3 du *Rapport annuel 2013*.

En outre, la définition de ces domaines a permis de délimiter précisément les responsabilités des différentes parties en fonction de l'activation ou non de « 3D-Secure » : dès lors qu'un commerçant aura activé la demande d'authentification par « 3D-Secure » pour une opération, le paiement sera garanti par la banque du porteur, qui supportera le coût de la fraude le cas échéant. Ce transfert de responsabilité est conforme avec les règles en la matière énoncées dans la DSP2.

Enfin, le protocole « 3D-Secure » étant supporté par les grands réseaux internationaux de cartes de paiement, il est susceptible d'apporter une protection aux porteurs et aux commerçants y compris dans le cas d'opérations transfrontalières.

2|3|2 Le mot de passe à usage unique (*One Time Password* – OTP)

La solution d'authentification forte la plus utilisée sur internet par les émetteurs du marché français pour les particuliers consiste à valider un paiement « 3D-Secure » avec un code à usage unique transmis par SMS sur le téléphone portable du titulaire de la carte (SMS OTP). Cette solution peut aussi être déclinée en transmettant l'OTP par courrier électronique ou par un serveur vocal [16].

Conformément à la définition de l'authentification forte, cette technique d'authentification s'appuie sur la connaissance des informations de la carte [17] et sur la possession du téléphone mobile dont l'émetteur a le numéro. Ces solutions sont donc compatibles avec la DSP2 sous réserve qu'il y ait bien un lien entre l'OTP et les données de la transaction.

Cependant, comme précisé dans le *Rapport annuel 2013* de l'Observatoire, cette technique présente plusieurs faiblesses en matière de sécurité :

- la présence d'un logiciel malveillant installé sur l'appareil connecté (téléphone, ordinateur, etc.) peut compromettre la sécurité du dispositif [18] ;
- la possibilité, sous certaines conditions [19], de désactiver la carte SIM du porteur légitime et d'activer une carte SIM différente mais pointant sur le même numéro peut faciliter la réalisation d'opérations frauduleuses ;
- le canal de communication utilisé lors de l'envoi du SMS n'est pas sécurisé, l'absence de chiffrement des données transmises par SMS permettant une interception des données en clair.

2|3|3 Le jeton d'authentification (*token*)

Lorsqu'ils n'ont pas la possibilité de recourir au SMS OTP, par exemple pour les clients ne disposant pas d'une ligne de téléphonie mobile ou pour la clientèle professionnelle, les émetteurs français distribuent généralement un dispositif matériel, appelé jeton d'authentification ou *token*, affichant

Jeton d'authentification simple

Jeton d'authentification avec clavier

16 Dans ce dernier cas, un serveur vocal appelle sur le téléphone du titulaire de la carte et lui dicte l'OTP à utiliser pour valider la transaction en cours.
17 C'est le critère de « connaissance » qui est retenu ici et non le critère de « possession » parce que les informations de la carte sont statiques, il n'est donc pas nécessaire d'avoir cette dernière en sa possession au moment du paiement.
18 D'une manière plus générale, l'utilisation du téléphone mobile pose un problème d'indépendance entre le canal de navigation sur internet et le canal de communication du *token* (SMS, *email* et serveur vocal).
19 Cf. chapitre 1, partie 4|3, Protection de la réémission des cartes SIM.

un code à validité temporaire et synchronisé avec un serveur d'authentification distant et incrémenté selon une fréquence prédéfinie (par exemple, toutes les 60 secondes). Ce code doit être saisi sur la page d'authentification « 3D-Secure » lors du processus de paiement par carte pour valider l'authentification du porteur.

Des dispositifs plus avancés, dotés d'un clavier numérique, permettent une interaction supplémentaire : dans ce cas, un code à usage unique valide ne peut être obtenu qu'après saisie, selon les cas, d'un code confidentiel connu seulement du porteur du dispositif, ou d'un code aléatoire généré par le serveur distant et affiché sur la page d'authentification au moment du paiement.

La sécurité de ce dispositif repose sur la connaissance des informations de la carte et sur la possession du *token* distribué par l'émetteur, et est donc conforme aux caractéristiques de l'authentification forte.

Cependant, il pose un double problème du fait de l'utilisation d'un *token* limité aux opérations de paiement :

- en situation de mobilité, les porteurs n'ont pas toujours le *token* avec eux ;

- le *token* est souvent conservé à proximité directe de l'ordinateur utilisé pour effectuer des paiements sur internet, sans la surveillance équivalente à celle d'une carte de paiement mise dans son portefeuille.

Enfin, pour plusieurs solutions de ce type, notamment celles n'utilisant pas de clavier, l'établissement d'un lien dynamique entre l'opération, le montant et le bénéficiaire donnés lors de l'authentification est *a priori* difficile à mettre en œuvre.

2|3|4 Le lecteur de carte physique

Partant du constat que la carte à puce n'a pas été conçue à l'origine pour sécuriser des opérations de vente à distance, certains acteurs ont été amenés à proposer des solutions reposant sur l'ajout d'une application dans la carte, qui s'utilise avec un lecteur de carte à puce portable et autonome, c'est-à-dire non connecté à un système de communication.

Dans ce type de dispositif, le client s'authentifie *via* le lecteur par l'insertion de sa carte et la saisie de son code confidentiel. En retour, le lecteur génère un code OTP qui s'affiche sur son écran et doit être saisi sur la page de paiement pour valider la transaction. Dans ce type de dispositif, l'authentification du porteur s'appuie sur la possession de la carte et la connaissance de son code confidentiel, comme pour un paiement de proximité, et constitue donc bien une authentification forte au sens de la DSP2.

Ces solutions, peu utilisées en France mais très courantes par exemple en Belgique, présentent toutefois un coût d'implémentation élevé, du fait de la mise à disposition d'un lecteur de carte à puce à chaque utilisateur. Par ailleurs, comme pour le *token*, cette solution contraint le porteur de la carte à avoir le lecteur à sa disposition au moment du paiement, ce qui constitue un frein au développement du e-commerce en situation de mobilité.

Lecteur autonome

Lecteur connecté

Afin de proposer une expérience client strictement équivalente à celle d'un terminal au point de vente, certains acteurs ont élaboré des solutions reposant sur l'utilisation d'un lecteur de carte à puce connecté à l'ordinateur. Cependant, ces solutions doivent pouvoir concilier plusieurs contraintes :

- atteindre un niveau de sécurité équivalent à un terminal de paiement électronique agréé [20],
- assurer une mise en œuvre simple pour tous les utilisateurs,
- garder un coût réaliste pour envisager un déploiement de la solution.

Au regard de la difficulté à répondre à ces contraintes, toutes les initiatives de ce type ont finalement été abandonnées en France.

2|3|5 Les limites à l'implémentation des solutions existantes

L'implémentation du dispositif « 3D-Secure » est parfois perçue comme une contrainte par les e-commerçants, dans la mesure où elle ajoute une étape intermédiaire supplémentaire dans le parcours client (renvoi vers le site de l'émetteur de la carte en vue d'authentifier le porteur) et est susceptible à ce titre d'impacter négativement le taux de conversion [21] des sites de e-commerce. Ainsi, le taux d'adoption de « 3D-Secure » par les commerçants atteint seulement 66 % après cinq ans de déploiement, et ce, bien que les statistiques démontrent que le taux d'échec des transactions authentifiées par « 3D-Secure » est strictement équivalent à celui des transactions qui ne le sont pas.

En outre, l'ajout de nouveaux équipements pour permettre la mise en œuvre du protocole « 3D-Secure » augmente les risques d'indisponibilité et constitue une source de coût d'exploitation supplémentaire.

Du point de vue ergonomique, ces solutions ne permettent pas de sécuriser les paiements par téléphone [22] ou par correspondance [23]. Elles posent également des difficultés pour les consommateurs réalisant leurs achats depuis des terminaux mobiles (bascule entre l'application utilisée pour faire l'achat et celle qui sert à la lecture des SMS).

Enfin, de façon générale, les limites rencontrées sur les implémentations actuelles de « 3D-Secure » ont conduit les émetteurs à envisager de nouvelles solutions offrant un niveau de sécurité adéquat, tout en préservant l'ergonomie des paiements tant pour les consommateurs que pour les commerçants.

2|4 Les futures solutions d'authentification

2|4|1 Les évolutions à venir du protocole « 3D-Secure »

Pour suivre l'évolution des usages et s'affranchir de certaines limitations inhérentes au protocole « 3D-Secure », les réseaux internationaux ont confié au consortium EMVCo. la charge de concevoir la deuxième version des spécifications du protocole, « 3D-Secure » 2.0. Les trois domaines de responsabilités (acquéreur, émetteur, interbancaire), d'où « 3D-Secure » tire son nom, restent à la base du protocole.

La nouvelle génération de « 3D-Secure » porte deux grandes caractéristiques :

- d'une part, elle intègrera nativement la communication d'informations supplémentaires pour permettre au domaine émetteur de faire une meilleur analyse de risque, puisqu'il pourra être alimenté à la fois par l'historique des transactions tenu par l'émetteur, par des données relatives au terminal d'initiation de la transaction (empreinte du terminal [24], ou *terminal footprint*) et par des informations partagées par le commerçant (par exemple : nouveau client,

20 En effet, ce niveau de sécurité est indispensable pour ne pas compromettre la sécurité des paiements de proximité.
21 Ce taux représente la part des visiteurs d'un site de e-commerce qui réalisent un achat.
22 Dans le cas d'un paiement réalisé en dictant les informations du paiement à un opérateur.
23 Dans le cadre d'un paiement réalisé par courrier postal ou par courrier électronique.
24 Procédé consistant à collecter des informations techniques de l'équipement considéré, aussi bien d'un point de vue matériel (identifiants/numéros de série des composants, etc.) que logiciel (type de système d'exploitation, versions de logiciels présents, etc.).

changement de l'adresse de livraison habituelle, etc.). Cette analyse multicritère permettra de détecter des transactions à risque pour lesquelles une authentification forte est nécessaire, ce qui permettra d'assurer un niveau de sécurité global élevé tout en levant les contraintes pour les transactions à faible niveau de risque ;

• d'autre part, elle intègrera le développement d'interfaces d'authentification intégrées aux applications mobiles des marchands, permettant de réaliser des achats dans un environnement homogène et ergonomique. Cette fonctionnalité permettra de surcroît de sécuriser les achats en recueillant les informations d'empreinte du terminal utilisé et de les transmettre au domaine émetteur en vue d'alimenter le dispositif d'évaluation d'un niveau de risque d'une transaction. Ce protocole adapté aux environnements mobiles sera complémentaire au protocole dédié aux navigateurs internet, et partagera une cinématique d'utilisation quasiment identique.

Une première version de ces spécifications sera rendue publique par le consortium EMVCo. en fin d'année 2016.

2|4|2 La mise en œuvre de solutions « émetteurs »

Les émetteurs et leurs prestataires ont développé des solutions dites « émetteurs » (ou *issuer only*) ne nécessitant aucune modification de l'interface de paiement standard (contrairement à « 3D-Secure »), c'est-à-dire ne nécessitant que la saisie d'un numéro de carte, d'une date d'expiration et d'un cryptogramme visuel. La sécurité de ces dispositifs réside alors dans la méthode d'authentification mise en œuvre, l'algorithme de génération de données à usage unique et la communication de ces dernières.

Les solutions en la matière reposent à ce stade sur la génération d'un cryptogramme à usage temporaire, appelé cryptogramme visuel dynamique, directement sur la carte elle-même : en effet, les progrès techniques permettent désormais d'intégrer dans une carte de paiement une micro-pile électrique alimentant un écran à base d'encre électronique, lequel se substitue au cryptogramme statique imprimé au dos de la carte, et génère un nouveau code à trois chiffres selon une fréquence prédéfinie (par exemple, toutes les heures). Ce dispositif permet de renforcer la sécurité des paiements sur internet sans nécessiter d'adaptation de la page de paiement du commerçant. Il faut noter que ces cartes pourraient s'avérer plus fragiles à l'usage que les cartes classiques et que leur production est également plus coûteuse.

Carte à cryptogramme visuel dynamique

Display card

Cette solution, qui relève du critère de « possession », renforce le niveau de sécurité des paiements à distance sur des sites non européens mais ne permet, à elle-seule, de se conformer ni à la définition de l'authentification forte, ni à l'article 97 de la DSP2. Cependant, la saisie en complément d'un simple mot de passe statique en présentant les éléments de la transaction au porteur suffit à répondre aux exigences européennes.

Dans ce contexte, un dispositif plus avancé, la « *display card* », qui intègre, en plus de l'écran et de la batterie, un clavier numérique permettant la saisie d'un code confidentiel dédié, pourrait répondre pleinement aux exigences de la DSP2. À ce jour, peu de déploiements effectifs de ce type de dispositif existent dans le monde, notamment en raison d'une industrialisation complexe au regard des exigences de fiabilité d'une carte de paiement.

2|4|3 Les solutions biométriques [25]

Plusieurs solutions fondées sur une authentification biométrique ont été développées ces dernières années. Les plus courantes mettent en œuvre :

- le lecteur d'empreinte digitale intégré au *smartphone* (pour les plus récents d'entre eux),
- le microphone du téléphone (reconnaissance vocale),
- l'appareil photo ou la caméra du téléphone mobile (reconnaissance faciale).

Ces différentes solutions, qui s'appuient sur la combinaison d'un élément de possession (le téléphone mobile) et d'inhérence (l'empreinte biométrique), apportent un confort d'utilisation reconnu par l'utilisateur, qui n'a plus besoin de se munir d'un dispositif dédié ou de retenir un mot de passe supplémentaire. Cependant, outre leur inadéquation aux paiements par téléphone [26] ou par correspondance, l'Observatoire a relevé dans son *Rapport annuel 2014* que le niveau de sécurité offert par ces dispositifs biométriques demeurait difficile à mesurer faute de standards d'évaluation équivalents à ceux existants pour des technologies éprouvées, et a invité les acteurs du marché à développer des référentiels de qualification permettant d'assurer un niveau de sécurité adéquat tout en protégeant les données biométriques des porteurs.

2|4|4 Les applications pour *smartphones*

En alternative à l'envoi d'un OTP par SMS, courrier électronique ou serveur vocal pour un paiement sur internet, certains émetteurs utilisent leur application de banque en ligne pour *smartphone* de façon à transmettre ou générer un OTP ou, plus généralement, authentifier l'utilisateur lors d'une transaction en lui demandant de valider qu'il est bien en train d'effectuer un paiement à distance [27]. Le fonctionnement de ces applications peut différer suivant les choix de l'émetteur, par exemple sur la nécessité ou non :

- d'allumer l'écran de son *smartphone* pour commencer l'authentification,
- de saisir un code confidentiel ou une empreinte biométrique pour accéder à l'application,
- de saisir un code sur la page de paiement du commerçant pour finaliser l'authentification.

Ces solutions permettent d'implémenter des mesures complémentaires pour sécuriser la transmission du code d'authentification, tout en gardant une cinématique proche de celle dont les utilisateurs ont l'habitude au travers du SMS OTP.

En partant de ce même constat, les opérateurs de téléphonie mobile ont développé un standard, *Mobile Connect*, pour la mise en place d'une application sécurisée sur la carte SIM dédiée à l'authentification de l'utilisateur et accessible à différents types de fournisseurs de service (service de paiement mais aussi transport en commun, billetterie de spectacle, etc.). L'activation de ce mode d'authentification, pour une carte SIM et un mobile donné, requiert une phase préalable d'enrôlement de l'utilisateur légitime du service.

2|4|5 La lecture de carte physique par l'antenne NFC d'un *smartphone*

Pour les cartes disposant d'une interface sans contact, il serait possible de mettre en œuvre la fonction de lecteur NFC des *smartphones* pour dialoguer avec la carte, et d'utiliser des mécanismes EMV pour vérifier l'authenticité et la validité de celle-ci. Cette cinématique, déjà expérimentée en alternative au SMS OTP dans un schéma « 3D-Secure », pourrait également s'appliquer à l'enregistrement d'une carte dans un portefeuille électronique (*wallet*).

En tout état de cause, pour assurer leur conformité avec la définition de l'authentification forte, ce type de dispositif fondé sur deux éléments de possession (carte et *smartphone*) doit être assorti d'une

25 Cf. Chapitre 3 du *Rapport annuel 2014*.
26 L'utilisation du téléphone mobile pose un problème d'indépendance entre le canal de navigation sur internet et le canal de transmission du code à usage unique.
27 Cette validation peut faire l'objet d'une saisie de code confidentiel (différent du code PIN de la carte) ou d'une reconnaissance biométrique, généralement par empreinte digitale.

authentification complémentaire par un élément de connaissance (par exemple, saisie d'un mot de passe) ou par une reconnaissance biométrique.

2|4|6 Les autres techniques d'échange de données

Pour les paiements sur internet, certains acteurs ont développé des technologies d'échange de données entre une page de paiement et un dispositif autonome, tels qu'un téléphone mobile ou un lecteur de carte par exemple, en s'appuyant sur des codes-barres à deux dimensions (QR *code*, Datamatrix, *Flash code*, etc.) ou sur des animations. Le porteur de la carte est invité à photographier l'image située sur la page de paiement avec son téléphone mobile, lequel génère alors un code OTP à saisir pour valider la transaction.

Ce type de dispositif permet de générer un OTP en s'appuyant sur les données de la transaction, et est donc à cet égard conforme à la DSP2. Il suppose toutefois pour le porteur de disposer de deux terminaux distincts, et se prête donc difficilement aux exigences du m-commerce.

2|5 Les mesures annexes aux méthodes d'authentification

Au-delà des mécanismes d'authentification du porteur, d'autres mesures peuvent être mises en place par les acteurs de la chaîne des paiements en vue de réduire le risque de fraude ou la sensibilité des données échangées.

2|5|1 La carte virtuelle dynamique

Plusieurs émetteurs français proposent une solution de carte virtuelle dynamique à leurs porteurs, parfois depuis plus de dix ans. Celle-ci permet à un porteur de ne pas saisir les véritables informations de sa carte lors d'un paiement à distance, en substituant certaines données par d'autres à validité limitée (numéro de carte, date d'expiration et cryptogramme visuel). Pour ce faire, un environnement dédié, généralement accessible depuis la banque en ligne du porteur, lui permet de générer un ensemble de numéros uniques et valables pour une seule transaction ou pour un montant limité qu'il pourra saisir à la place des données présentes sur le support physique de sa carte. Le développement récent de techniques dites de « tokenisation » a permis d'automatiser la génération de tels numéros de carte de substitution.

L'accès à l'espace de gestion des cartes virtuelles dynamiques est protégé par un mécanisme d'authentification - parfois celui de la banque en ligne du porteur. L'accès à des fonctions sensibles de cet espace, comme la génération de nouvelles cartes virtuelles, doit toutefois faire l'objet d'une authentification forte pour que le dispositif soit pleinement conforme au cadre général défini par la DSP2.

2|5|2 Les outils d'évaluation et de gestion du risque

En complément de l'authentification forte du porteur, des outils d'évaluation et de gestion du niveau de risque des transactions ont été mis en place par différents intervenants du cycle de paiement (systèmes de paiement par carte, émetteurs, acquéreurs, mais aussi parfois les commerçants ou leurs prestataires d'acceptation). Ces systèmes participent à la détection des tentatives de fraude, et permettent de juger du niveau d'authentification à activer pour une transaction donnée.

Comme indiqué précédemment, dans le cadre des nouvelles spécifications du protocole « 3D-Secure », les émetteurs disposeront de nouveaux éléments leur permettant d'affiner le niveau de risque d'une transaction.

Il faut noter cependant que ces mesures entraînent généralement le traitement de données personnelles, telles que l'historique des achats d'un client, et qu'elles nécessitent de ce fait une déclaration, voire une autorisation, auprès de la Commission nationale Informatique et Libertés [28].

28 La protection des données personnelles dans le cadre des traitements de lutte contre la fraude a fait l'objet d'une étude publiée dans le *Rapport annuel 2013* de l'Observatoire (chapitre 4).

2|6 Les recommandations de l'Observatoire relatives au développement de nouvelles solutions de sécurisation des paiements à distance

Les nouvelles solutions de sécurisation des paiements à distance conçues et développées par les acteurs du marché permettent de répondre à certaines limites des solutions existantes, notamment en matière d'ergonomie pour le porteur de la carte et de facilité d'implémentation pour les commerçants. Leur mise en œuvre, associée à d'autres techniques d'authentification pour celles qui ne répondraient pas à elles seules à la définition de l'authentification forte telle que définie dans la DSP2, sont susceptibles de permettre un renforcement de la sécurité des paiements en Europe et au-delà. À ce titre, l'Observatoire invite les acteurs à poursuivre le développement de ces nouvelles solutions, qui s'inscrivent dans le prolongement à la fois des exigences règlementaires en matière d'authentification des paiements, et de la stratégie nationale des paiements.

L'Observatoire souligne la nécessité de disposer d'une évaluation globale du niveau de sécurité offert par ces solutions, ainsi que des contraintes qu'elles génèrent pour leurs utilisateurs (ergonomie pour les consommateurs, implémentation et gestion pour les commerçants), tout en insistant sur le besoin de protéger contractuellement les porteurs et les commerçants des risques résiduels durant les phases d'expérimentation.

Du point de vue de l'appropriation par les utilisateurs, l'Observatoire invite les acteurs à développer une offre d'authentification claire et lisible, en veillant à privilégier un nombre réduit de solutions communes et offrant un niveau de sécurité adéquat au regard de la réglementation. Une attention particulière devra être portée au caractère universel des solutions mises en œuvre, en proposant le cas échéant des offres alternatives pour les porteurs qui en seraient exclus.

Par ailleurs, l'Observatoire rappelle son attachement à la mise en place de mesures de protection complémentaires aux dispositifs d'authentification, telles que la mise en place de systèmes d'évaluation du niveau de risque d'une transaction permettant d'adapter le niveau d'authentification requis lors du paiement, et le recours à des démarches de « tokenisation » qui permettent d'éviter tout risque de contamination à d'autres modes d'utilisation de la carte en cas d'interception des données.

L'Observatoire rappelle que l'usage de la biométrie comme composante de dispositifs d'authentification forte est soumis aux recommandations émises dans son *Rapport annuel 2014*.

Enfin, l'Observatoire souligne que la mise en place de mesures permettant de restreindre la fraude sur les paiements à distance en France et en Europe est susceptible de provoquer un report des tentatives de fraude sur d'autres opérations, notamment vers les paiements transfrontaliers, et invite par conséquent les acteurs à prendre en compte ce risque supplémentaire dans les mesures de protection envisagées.

Les cartes de paiement en Europe : évolutions récentes et défis pour l'avenir

Synthèse de la conférence organisée par la Banque de France les 18 et 19 janvier 2016

La Banque de France a organisé les 18 et 19 janvier 2016 à Paris une conférence internationale consacrée aux dernières évolutions et aux défis futurs dans le domaine des cartes de paiement en Europe.

Le gouverneur de la Banque de France, François Villeroy de Galhau, a souligné lors de son allocution d'ouverture les grands enjeux qui traversent à l'heure actuelle le marché des cartes de paiement :

• bien que bénéficiant d'une position prédominante dans le marché des paiements scripturaux, résultat d'un travail de plusieurs années des différentes parties prenantes pour construire un moyen de paiement sûr, efficace et facile à utiliser, les cartes de paiement sont confrontées à un contexte de fortes évolutions liées à l'émergence de nouveaux acteurs et au changement des habitudes de paiement des utilisateurs ;

• à cette situation s'ajoutent en Europe des évolutions réglementaires importantes, suite à l'adoption de la directive révisée (UE) 2015/2366 sur les services de paiement, mais surtout du règlement (UE) 2015/751 relatif aux commissions d'interchange sur les opérations de paiement par carte, qui contribuent à remodeler le modèle économique du marché des cartes de paiement en Europe ;

• face à ces transformations, les autorités publiques doivent, dans leur fonction de catalyse du marché, plus que jamais viser à renforcer la coopération entre les parties prenantes, au niveau européen aussi bien qu'au niveau national, afin de permettre l'apparition de solutions harmonisées. Dans leur fonction de surveillance, les autorités doivent viser à favoriser l'innovation tout en maintenant une exigence de sécurité au moins aussi élevée que celle qui existe aujourd'hui. Ceci passe notamment par l'établissement d'une surveillance proportionnée au profil de risque des activités fournies, et non fondée uniquement sur la nature des prestataires. Ce principe doit permettre l'établissement d'une concurrence non faussée entre tous les acteurs.

1| L'état des lieux des paiements par carte : une situation paradoxale

1|1 Une position prédominante, avec des réserves de croissance

La carte bénéficie dans le domaine des paiements scripturaux, en Europe et plus particulièrement en France, d'une position prédominante. Ainsi, en 2014, les cartes de paiement ont été utilisées pour plus de 47 milliards d'opérations au sein de l'Union européenne (UE), soit un niveau presque identique au nombre cumulé de transactions impliquant des virements et des prélèvements. En France, les cartes de paiement ont été utilisées dans plus de 50 % des opérations de paiements scripturaux, pour un total de près de 9,5 milliards d'opérations en 2014, contre seulement 3 milliards en 2001.

La carte connaît ainsi un succès indéniable appelé à perdurer tant en Europe, où la part d'utilisation de la monnaie fiduciaire représente encore dans certains pays près de 70 % des transactions, que dans le reste du monde, par exemple aux États-Unis où le passage à la technologie EMV [1] va permettre de renouveler près d'un milliard de cartes. Le développement de nouvelles solutions de paiement assises sur les cartes de paiement physiques ou dématérialisées (sans contact, portefeuilles

1 EMV (Europay MasterCard Visa) : standard géré par le consortium international EMV Co (réunissant les principaux systèmes de paiement par carte) et définissant un ensemble de spécifications techniques fonctionnelles pour les cartes de paiement à puce.

électroniques, paiements mobiles, utilisation des mobiles comme terminaux de paiement, etc.) devrait également permettre de renforcer la prééminence de cet instrument dans les prochaines années.

Au-delà des chiffres et des perspectives de croissance, les différentes interventions ont permis de souligner le fait que la carte de paiement constitue, y compris pour les nouveaux entrants sur le marché, un modèle de réussite à imiter.

1|2 Une remise en cause forte

La session consacrée à l'innovation a permis de constater que malgré sa position dominante sur le marché des paiements scripturaux, la carte de paiement fait actuellement l'objet d'une forte remise en cause en raison de trois grandes séries de facteurs :

• les changements d'habitude des consommateurs, qui recourent de façon croissante au commerce en ligne. La carte a ainsi été adaptée à de nouveaux usages (paiement à distance notamment), de nouveaux canaux d'initiation de paiement (internet, applications, etc.) et de nouveaux supports (ordinateurs, mobiles, tablettes, etc.) pour lesquels elle n'avait pas été initialement conçue. Cette situation, en plus de générer de nouveaux risques de sécurité (cf. partie 2), met également en avant les limites de la carte de paiement « physique » dans un commerce de plus en plus dématérialisé ;

• l'apparition d'entreprises capitalisant sur les nouvelles technologies financières (*fintechs*) sur le marché des cartes de paiement, qu'il s'agisse des GAFA [2] ou d'acteurs de plus petite taille spécialisés dans certains services (portefeuilles électroniques, paiements mobiles, etc.), qui viennent concurrencer les parties prenantes traditionnelles et bouleverser les stratégies établies ;

• l'émergence de nouvelles technologies de paiement assises sur d'autres instruments de paiement que la carte. À ce titre, le développement en cours d'une solution paneuropéenne de paiements instantanés fondée sur le virement SEPA, qui devrait être opérationnelle en novembre 2017, constitue une évolution majeure qui pourrait venir à terme concurrencer la carte. À plus long terme, l'application de la technologie *blockchain*, issue des monnaies virtuelles, au domaine des paiements pourrait également constituer une alternative aux systèmes de paiement par carte, sous réserve toutefois que des gages de sécurité et de capacité à traiter des opérations de masse puissent être apportés.

Ces différents facteurs sont sources de déstabilisation des acteurs de marché existants, qui se trouvent soumis à une double concurrence, au sein du marché des cartes lui-même d'une part, et en provenance des autres instruments de paiement scripturaux d'autre part. Cette situation crée de fortes tensions sur les modèles commerciaux et économiques établis, qui doivent par ailleurs s'adapter à un environnement en mouvement.

2| Un environnement en mouvement

2|1 Les changements du cadre réglementaire et leurs conséquences

Durant ces vingt dernières années, tant aux niveaux international que national, les autorités de la concurrence ont engagé de nombreuses procédures à l'encontre des systèmes de paiement par carte, qui ont notamment abouti à la baisse des commissions multicanales d'interchange. Ainsi, dès 2007, la commission versée par la banque du commerçant (l'acquéreur) à la banque du porteur de la carte (l'émetteur) a été jugée comme une pratique restreignant la concurrence par la Commission européenne puis par les tribunaux de l'Union européenne [3].

Pour résoudre les problèmes de concurrence, la Commission européenne a accepté les engagements pris par Visa et MasterCard de baisser les commissions multilatérales d'interchange sur les opérations transfrontalières (et certaines opérations nationales) [4].

2 Google, Apple, Facebook, Amazon.

3 Affaire COMP/34.579, MasterCard, décision de la Commission du 19 décembre 2007. Cette décision a par la suite été confirmée par le Tribunal de l'UE en 2012 (Arrêt du Tribunal du 24 mai 2012 dans l'affaire T-111/08, MasterCard e.a./Commission) et par la Cour de Justice de l'UE en 2014 (Arrêt de la Cour du 11 septembre 2014 dans l'affaire C-382/12 P, MasterCard e.a./Commission).

D'autres actions au niveau national se sont également soldées par un encadrement du niveau de ces commissions, par exemple, en France où le Groupement des Cartes Bancaires s'était engagé en 2011 à appliquer un taux de 0,28 % en moyenne annuelle pendant une durée de quatre ans [5].

C'est dans ce contexte que la Commission européenne a publié, le 24 juillet 2013, une proposition de règlement relatif au plafonnement des commissions d'interchange ainsi qu'une proposition de révision de la directive concernant les services de paiement. Le premier texte a été adopté le 29 avril 2015 (règlement (UE) 2015/751) : il prévoit des dispositions qui limitent le niveau des commissions d'interchange (à 0,2 % du montant de la transaction pour les transactions par carte de débit et 0,3 % pour les transactions par carte de crédit), entrées en vigueur le 9 décembre 2015, et des règles dites « commerciales » destinées à renforcer la concurrence et la transparence [6], qui entrent en vigueur progressivement jusqu'au 9 décembre 2016. Le second texte a été adopté le 25 novembre 2015 (directive (UE) 2015/2366) et va, notamment, généraliser l'application de mesures d'authentification forte du payeur dans l'ensemble de l'Union européenne à horizon fin 2018.

Parmi les enjeux de mise en œuvre de ce nouveau cadre règlementaire, l'un concerne principalement la France, où la majorité des cartes de paiement émises sont dites universelles, c'est-à-dire qu'elles ne permettent pas de différencier aisément une transaction de débit d'une transaction de crédit. Afin que le secteur français des cartes de paiement ait le temps de faire évoluer son modèle, la France a levé l'option prévue à l'article 16 du règlement permettant d'appliquer un taux maximum de 0,23 % de commission multilatérale d'interchange sur les transactions effectuées avec des cartes universelles durant une période transitoire qui se terminera le 9 décembre 2016 [7]. Après cette date, les acteurs français devront être capables d'appliquer les différents plafonds de taux prévus au règlement en fonction de la nature de chaque transaction.

Autre disposition dont la mise en œuvre s'avère complexe, l'article 8.6 du règlement prévoit que si le commerçant a la possibilité de présélectionner une marque ou une application de paiement par carte, le payeur doit avoir la faculté d'en sélectionner une autre au moment où il réalise son paiement, dans la limite des marques et des applications acceptées par le commerçant. La mise en œuvre de cette obligation nécessite la mise à jour de l'ensemble du parc de terminaux de paiement des commerçants, et pose des difficultés particulières dans le cas du paiement sans contact ; en effet, cette disposition nécessite l'ajout d'une étape de sélection par le payeur sur le terminal, alors même que ce type de paiement a été conçu pour fluidifier le paiement et réduire au minimum les interactions entre le payeur et le terminal de paiement. À ce titre, les acteurs du secteur de la carte craignent que cette obligation ne constitue un frein au développement du paiement sans contact, et appellent les régulateurs à définir des modalités de mise en œuvre adaptées, telles que par exemple la possibilité d'une sélection par défaut paramétrée par le commerçant pour le mode sans contact, afin de maintenir l'ergonomie actuelle de ce mode de paiement.

Enfin, si la généralisation de l'authentification forte du payeur prévue à l'article 97.1 de la directive pour les paiements en ligne est accueillie favorablement par les acteurs du marché, ces derniers ont souligné que le renforcement de la sécurité ne devait pas se traduire par des contraintes excessives en termes d'ergonomie, qui nuiraient alors au développement du secteur et de l'innovation. Les systèmes de cartes de paiement se sont ainsi déclarés particulièrement attentifs aux travaux de l'Autorité bancaire européenne, chargée d'élaborer, en collaboration avec la Banque centrale européenne (BCE), le projet de norme technique de réglementation prévu à l'article 98.1 de la directive, et qui précisera notamment les exemptions à l'obligation d'appliquer des mesures d'authentification forte. Ces exemptions devront être fondées sur les critères définis à l'article 98.3 de la directive, et qui portent sur le niveau de risque de la transaction, le montant et/ou le caractère récurrent de l'opération et le moyen utilisé pour exécuter l'opération.

4 En 2009, MasterCard s'est engagé à plafonner les CMI transfrontalières « consommateurs » à 0,2 % pour les cartes de débit et 0,3 % pour les cartes de crédit ; en 2010, Visa Europe a pris des engagements similaires. En 2013, Visa Europe a pris de nouveaux engagements, concernant les opérations transfrontalières par carte de crédit dans certains pays.

5 Cf. Décision de l'Autorité de la Concurrence 11-D-11 du 7 juillet 2011. Le 18 juin 2015, le Groupement des Cartes Bancaires a reconduit ses engagements jusqu'à l'entrée en vigueur du règlement (UE) 2015/751.

6 Ces règles concernent notamment la séparation entre l'instance de gouvernance d'un système de paiement par carte et les entités en charge techniquement de traiter les transactions de paiement (*processing*).

7 Cf. décret n° 2015-1591 du 7 décembre 2015.

Cette évolution du cadre réglementaire devrait conduire à un renforcement de la concurrence au sein de l'Union européenne entre tous les systèmes de cartes, les émetteurs et les acquéreurs. En particulier, les porteurs de carte auront le choix d'utiliser une marque ou une application donnée lors du paiement. Les commerçants recevront quant à eux davantage d'informations sur l'ensemble des commissions facturées par leur prestataire de services de paiement pour chaque transaction, en application des articles 9 et 12 du règlement. Cependant, ce nouveau cadre se traduisant par une baisse des revenus pour les acteurs bancaires, les intervenants considèrent qu'une augmentation des frais à la charge des porteurs de cartes n'est pas à exclure. Une telle augmentation a déjà été constatée dans les pays où les commissions multilatérales d'interchange sont encadrées ; elle est généralement justifiée par les acteurs du secteur bancaire au titre de la nécessité de continuer à investir dans l'innovation et la lutte contre la fraude.

2|2 Les nouvelles tendances technologiques du paiement par carte

La session consacrée aux nouvelles tendances technologiques a permis de fournir un aperçu détaillé des évolutions envisagées par les acteurs du marché du paiement par carte.

En premier lieu, l'adoption de plus en plus large des *smartphones* et des équipements connectés poussent les acteurs à développer des solutions de paiement adaptées à ces nouveaux outils. En particulier, de plus en plus de fabricants de terminaux mobiles et d'éditeurs de systèmes d'exploitation pour mobile intègrent désormais des éléments de sécurité dans leurs produits pour fournir des solutions de type portefeuille électronique destinées à faciliter le paiement en ligne sur les sites marchands de e-commerce et de m-commerce, et à permettre en parallèle le paiement de proximité en s'appuyant notamment sur les technologies actuellement déployées pour les paiements par carte (telles que le sans contact NFC [8] EMV).

En matière de sécurité, la tendance la plus notable concerne le développement de solutions permettant de protéger les données de carte en substituant le numéro de la carte par un code à usage unique (*token*) lors du paiement. Ces solutions de « tokenisation », qui reposent sur des infrastructures déployées par les réseaux d'émetteurs de cartes, visent à diminuer le niveau de sensibilité des données qui sont collectées par les commerçants traditionnels et les commerçants en ligne lorsqu'ils acceptent les paiements par carte. Ainsi, un *token* qui aura été utilisé lors d'une transaction ne pourra généralement plus être réutilisé ultérieurement. Cette approche nouvelle permet par conséquent de réduire l'impact d'une compromission de ces données.

Enfin, on observe un recours de plus en plus large à la biométrie pour authentifier le porteur de la carte. La biométrie pourrait devenir une alternative de plus en plus fréquente à la saisie du code confidentiel, voire un substitut à la signature manuscrite là où ce mode d'authentification est encore utilisé.

Les acteurs du marché notent cependant que l'acceptation en point de vente physique de ces nouvelles solutions nécessite l'adaptation des terminaux de paiement. Celle-ci peut s'avérer complexe et coûteuse compte-tenu des contraintes sécuritaires auxquelles ces derniers sont soumis. On constate par ailleurs l'apparition de solutions adaptées aux petites entreprises et aux professionnels indépendants, à des prix qui leurs sont accessibles, qui peuvent transformer un *smartphone* en terminal d'acceptation, tout en restant conformes aux requis sécuritaires habituels pour ces équipements. De cette manière, ces acteurs peuvent accepter des paiements par carte ou par mobile tout en profitant de services annexes à valeur ajoutée adaptés à leurs besoins.

2|3 Les travaux de standardisation en cours

Plusieurs organismes de normalisation et de standardisation travaillent à la formulation de règles communes sur l'ensemble de la chaîne de

8 NFC (*Near Field Communication*) : technologie de communication sans contact à courte distance.

paiement, comme l'organisation internationale de normalisation ISO, ou pour des champs d'application plus restreints adaptés aux intérêts des participants :

• l'institut européen des normes de télécommunications ETSI sur les services mobiles,

• l'organisme de standardisation W3C sur les interfaces des sites internet,

• le consortium industriel FIDO Alliance sur l'identification et l'authentification des personnes,

• NEXO pour l'intégration des paiements dans les chaînes de traitement automatisées des commerçants.

En Europe, l'actualité principale concerne la prise en compte des nouvelles exigences réglementaires qui découlent de la révision de la directive européenne sur les services de paiement. Il s'agit en particulier d'inclure les nouveaux acteurs que sont les prestataires de services d'initiation de paiement et de définir les spécifications de l'interface de communication qui leur permettra d'échanger de manière sécurisée avec les émetteurs de cartes et les teneurs de comptes.

Plusieurs organisations, comme par exemple NEXO (avec la norme SEPA-Fast) pour ce qui concerne les terminaux de paiement électronique, ont déjà annoncé l'adaptation prochaine de leurs spécifications pour se conformer à ces exigences. Les participants du colloque se sont accordés pour considérer qu'un effort d'harmonisation restait cependant nécessaire entre les différentes parties, que cela vise les fonctionnalités offertes ou les règles sécuritaires appliquées.

3| Les défis de sécurité à relever

3|1 Un haut niveau de sécurité des paiements de proximité…

Plusieurs intervenants ont évoqué le haut niveau de sécurité offert par les cartes de paiement pour les transactions au point de vente, en soulignant que les taux de fraude observés en France sont comparables à ceux des autres pays dans lesquels le paiement par carte à puce a atteint son niveau de maturité.

Ainsi, depuis la mise en œuvre en Europe des spécifications EMV pour les cartes à puce, la fraude sur les cartes de paiement a diminué de façon continue sur les paiements de proximité et sur les automates de retrait, pour passer de 54 % des montants fraudés en 2008 à 34 % en 2013. En outre, à part quelques exceptions de fraude constatées sur des automates équipés uniquement de lecteurs de pistes magnétiques tels que les péages routiers, la fraude aux cartes de paiement provient aujourd'hui essentiellement du vol ou de la perte des cartes de paiement, du fait du caractère infalsifiable des cartes à puce EMV.

Par ailleurs, il a été relevé que la migration des cartes et des terminaux de paiement à la norme internationale EMV de l'Asie et des États-Unis était en retard par rapport à l'Europe, mais progressait désormais très rapidement. Les voyageurs français et européens devraient donc pouvoir bénéficier progressivement dans ces zones géographiques de conditions de sécurité équivalentes à celles ayant cours en Europe (*i.e.* lecture de la puce de la carte et saisie du code confidentiel).

3|2 …mais une vulnérabilité persistante pour les paiements à distance

La sécurisation des transactions de proximité a entraîné un report de la fraude sur les paiements par internet, qui supportent désormais les deux-tiers de la fraude globale ; la progression de cette fraude suit depuis plusieurs années le mouvement de croissance des transactions en ligne, de plus de 10 % par an. Sur ce type de transactions, le recours aux dispositifs d'authentification renforcée du porteur de la carte, couplé au développement de dispositifs d'évaluation du niveau de risque des transactions, a montré toute son efficacité puisqu'une première baisse constatée au deuxième trimestre 2015 en France s'est poursuivie au cours des trimestres suivants.

Néanmoins, il a été souligné que le protocole « 3D-Secure », utilisé majoritairement pour l'authentification du porteur, est aujourd'hui la cible des fraudeurs, lesquels ont montré récemment leur capacité à mener des attaques en utilisant différentes méthodes telles que l'hameçonnage (*phishing*) [9],

9 Également dénommé hameçonnage, technique de vol de données sensibles (comme les numéros de carte de paiement, cryptogramme visuel, etc.) au moyen d'une campagne d'*emailing* par exemple, en usurpant l'identité d'une société ou d'une institution.

l'exploitation de méthodes d'authentification faibles (par exemple, mot de passe statique) ou de failles au niveau du processus d'enrôlement du payeur, ou encore l'attaque des canaux de transmission des mots de passe (piratage de box ADSL, usurpation de carte SIM, etc.).

Des mesures complémentaires de sécurisation devraient à l'avenir renforcer la lutte contre la fraude ; à ce titre, l'organisme en charge du maintien des spécifications EMV, EMV Co, a indiqué qu'il travaillait notamment sur l'harmonisation des règles concernant la mise en œuvre de la « tokenisation » et de l'acceptation des paiements par mobile. EMV Co a ainsi prévu de publier dans les mois à venir des spécifications sur les cartes de nouvelle génération et de mettre à jour des spécifications du standard « 3D-Secure » qui sécurise les paiements sur internet.

3|3 Le rôle central de la cybersécurité

Les moyens de paiement constituent une des principales cibles du cybercrime. Le caractère protéiforme de cette criminalité, faisant intervenir des acteurs aussi bien isolés que des organisations hautement structurées complexifie la lutte contre la cybercriminalité liée aux moyens de paiement. Le plus souvent, la fraude est la résultante de l'intervention de plusieurs acteurs dont les responsabilités se limitent à des domaines de compétence bien précis :

• les développeurs en charge de l'élaboration des logiciels malveillants de type *botnet*, *ransomware*, déni de service, etc. ;

• les managers d'infrastructures et fournisseurs de services permettant l'hébergement des logiciels malveillants et leur déploiement ;

• les intermédiaires volontaires et involontaires (mules) ;

• les revendeurs de données de type carte ou autre information de paiement transmises à des réseaux d'utilisateurs en vue de commettre des fraudes aux moyens de paiement simples ou plus élaborées de type fraude au président.

La coordination entre des organismes tels Europol et les autorités nationales permet de démanteler efficacement des réseaux de fraude agissant au niveau international, par exemple en plaçant des terminaux de paiement contrefaits auprès de commerçants ou en piégeant des distributeurs automatiques de billets. Les autorités judiciaires notent également que le *phishing* constitue l'un des moyens les plus utilisés par les cybercriminels pour obtenir des informations, que ce soit par la diffusion massive de courriels frauduleux ou l'hébergement de pages web copiant des sites légitimes.

L'autre facteur de difficulté dans la lutte contre les cyberattaques provient de la diversité des motivations de leurs auteurs. Si le plus souvent l'intérêt financier domine, les attaques peuvent également résulter de facteurs politiques ou liés à l'intelligence économique. Enfin, les nouveaux acteurs et les nouvelles solutions (initiation de paiements depuis des *smartphones* par exemple) intervenant dans la chaîne des paiements constituent des cibles d'intérêt pour les cyberfraudeurs, et peuvent participer au développement des activités de blanchiment et de financement du terrorisme.

4| Conclusion : quelles sont les nouvelles stratégies pour l'industrie ?

Face aux évolutions profondes que connaît le secteur des cartes de paiement depuis plusieurs années, les futures stratégies du marché devraient s'orienter autour de plusieurs axes forts :

• la poursuite du développement et de la mise en œuvre des innovations. Les différents intervenants ont souligné à cet égard le besoin de continuer le déploiement des paiements sans contact et des paiements mobiles, en soulignant l'impact positif de ces innovations sur les volumes de vente des commerçants. Le développement de l'innovation implique également la mise en œuvre d'un cadre juridique assurant une concurrence non faussée entre les acteurs établis et les nouveaux entrants ;

• le renforcement de la « coopétition » entre les parties prenantes au niveau européen pour construire des services harmonisés et éviter la fragmentation du marché. Le besoin de standardisation et d'interopérabilité entre les structures dans le domaine

des cartes de paiement a ainsi été fortement souligné. Il s'accompagne de la nécessité de construire des acteurs de taille européenne, à même de contrebalancer le pouvoir des *schemes* internationaux. Plusieurs intervenants ont dans ce cadre appelé, au niveau européen, à l'approfondissement du projet SEPA pour les cartes (SEPA *for cards*) ;

• la refonte des modèles commerciaux et économiques des acteurs, dans un contexte où le prix des transactions devrait continuer à baisser pour approcher d'une quasi-gratuité. Cette baisse des revenus directs liés aux paiements devrait pousser les acteurs à rechercher de nouvelles opportunités de gains, reposant plutôt sur l'offre de services annexes aux paiements (assurances, crédits, offres de fidélité, etc.). Cette évolution pourrait entraîner une reconfiguration importante des acteurs établis, qui devront s'adapter à ces nouvelles conditions.

Encadré

Programme de la conférence

Discours d'ouverture
François Villeroy de Galhau, gouverneur, Banque de France

Présentations introductives
Yves Mersch, membre du Directoire, Banque centrale européenne
Mario Nava, directeur en charge des Institutions financières, Commission européenne

Thème I : Les cartes de paiement en Europe : un secteur en évolution

Table ronde : Les conséquences des nouveaux cadres règlementaires pour le marché des cartes en Europe
Modérateur : Benjamin May, avocat associé, Aramis Law
Rita Wezenbeek, responsable de l'unité Antitrust, Systèmes de paiement, Commission européenne
Gilbert Arira, administrateur, Cartes Bancaires
Scott McInnes, conseiller senior, MasterCard
Jörn-Jakob Röber, conseiller senior, Visa

Table ronde : Les dernières tendances en matière d'innovation dans le domaine des cartes de paiement : évolution ou révolution ?
Modérateur : Dirk Schrade, adjoint au chef du département des Systèmes de paiement et de règlement, Banque fédérale d'Allemagne
Matthieu Andrade, manager senior, Samsung Pay Europe
Claude Brun, président du Cards Working Group, European Payment Council
Marc Kekicheff, membre du Board of Managers, EMV Co.
Magnus Nilsson, co-fondateur et responsable opérationnel, iZettle

Présentation : L'élaboration des textes règlementaires prévus par la deuxième directive européenne sur les services de paiement
Dirk Haubrich, responsable de la Protection des consommateurs, de l'Innovation financière et des Paiements, Autorité bancaire européenne

.../...

Thème II : La lutte contre la fraude dans les paiements par carte

Présentation : Les enjeux de cybersécurité dans les domaines de la banque et de la finance
Andreas Mitrakas, responsable de l'unité de la Qualité et de la Gestion des données, Agence européenne de la Sécurité des Réseaux et de l'Information (ENISA)

Table ronde : Les tendances récentes en matière de développement de la fraude aux cartes de paiement
Modérateur : Denis Beau, directeur général de la Stabilité financière et des Opérations, Banque de France
Jeremy King, directeur international, PCI SSC
Gabriel Leperlier, responsable des Activités de conseil aux professionnels pour l'Europe, Verizon
Antoine Sautereau, directeur des Opérations, Cartes Bancaires

Présentation : Cybercrime et cyberfraude
Colonel Eric Freyssinet, conseiller du gouvernement sur les cybermenaces, ministère français de l'Intérieur

Thème III : Les évolutions stratégiques dans le domaine des cartes de paiement

Présentation : Paiements – autre temps, autres mœurs
Javier Santamaria, président de l'EPC et vice-président de Banco Santander

Table ronde : Les enjeux de standardisation
Modérateur : Ugo Bechis, conseiller e-paiements et SEPA, UBI Banca
Margot Dor, directeur des Partenariats et des Relations européennes, ETSI
Arnaud Crouzet, secrétaire général, NEXO
Gert Huizinga, consultant senior sur les solutions cartes, ING

Table ronde : Quelle stratégie pour le développement du marché des cartes en Europe ?
Modérateur : Helmut Wacket, responsable de la division d'Intégration du marché, Banque centrale européenne
Narinda You, vice-présidente, European Payment Council
Vitor Bento, président, European Card Payment Association
Marc Espagnon, responsable de la direction des Moyens de paiement, BNP Paribas
Frédéric Mazurier, directeur général délégué, Carrefour Banque

Allocution de clôture
Denis Beau, directeur général de la Stabilité financière et des Opérations, Banque de France

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 R141-1, R141-2 et R142-22 à R142-27 du *Code monétaire et financier*.

Cartes concernées

L'ancien article L132-1 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 L521-1 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 L521-1 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 L511-7, l'article L525-6 et le II *in fine* de l'article L521-3 du *Code monétaire et financier*.

4 Ces cartes sont dispensées d'agrément par le II de l'article L511-7, l'article L525-5 et le I de l'article L521-3 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 L315-1 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 L133-3 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 L141-4 et R141-1 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 L314-1 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 R141-2 du *Code monétaire et financier*, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

Composition

L'article R142-22 du *Code monétaire et financier* détermine la composition de l'Observatoire. Conformément à ce texte, l'Observatoire comprend :

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel et de résolution ou son représentant ;
- 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 François Villeroy de Galhau, gouverneur de la Banque de France, assure cette fonction depuis le 10 décembre 2015.

Modalités de fonctionnement

Conformément à l'article R142-23 et suivants du *Code monétaire et financier*, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté 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 au ministre chargé 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 le ministre chargé des Finances le saisissent 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 R142-25 du *Code monétaire et financier*, et doivent donc conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. À cette fin, l'Observatoire a inscrit dans son règlement intérieur l'obligation incombant aux membres de s'engager auprès du président à veiller strictement au caractère confidentiel des documents de travail.

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 des Finances et des Comptes publics. Le dernier arrêté de nomination date du 10 décembre 2015.

Président

François VILLEROY DE GALHAU
Gouverneur de la Banque de France

Représentants des assemblées

Michèle ANDRÉ
Sénatrice
Philippe GOUJON
Député

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

Nicolas PELIGRY
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 :
  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 :
  Philippe ARMAND
  Yuksel AYDIN

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

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

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

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

- Le directeur des Affaires criminelles et des Grâces ou son représentant :
  Emmanuelle CROCHET

Sur proposition du ministre de l'Intérieur :

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

Sur proposition du ministre de la Défense :

- Le directeur général de la Gendarmerie nationale ou son représentant :
  Nicolas DUVINAGE
  Thomas SOUVIGNET

A12

Représentants des émetteurs de cartes de paiement

Gilbert ARIRA
Administrateur
Groupement des Cartes Bancaires
Jean DIACONO
Administrateur
American Express France
Willy DUBOST
Directeur Systèmes et Moyens de paiement
Fédération bancaire française
Isabelle GUITTARD-LOSAY
Conseiller senior
BNP Paribas Personal Finance
Frédéric MAZURIER
Directeur général délégué
Carrefour Banque
Gérard NEBOUY
Directeur général
Visa Europe France
Christine PUYHARDY
Directrice de la Règlementation, des Partenariats et des Relations externes
La Banque Postale
Caroline SELLIER
Directeur Risk management et Lutte contre la fraude
Natixis Paiements
Bart WILLAERT
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

Gérard DEBENEIX
Confédération Nationale du Logement (CNL)
Bernard FILLIAT
Association pour l'Information et la Défense des consommateurs salariés (INDECOSA – CGT)
Hervé MONDANGE
Association Force Ouvrière Consommateurs (AFOC)
Ariane POMMERY
Responsable du service juridique – Association de défense d'éducation et d'information du consommateur (ADEIC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Représentants des organisations professionnelles de commerçants

Jean-Michel CHANAVAS
Délégué général – Mercatel
Vincent DEPRIESTER
Directeur – Casino Services
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
Philippe SOLIGNAC
Vice-président – Chambre de commerce et d'industrie de Paris

Personnalités qualifiées en raison de leurs compétences

Eric BRIER
Chief Security Officer
Ingenico
Stéphane GREGOIRE
Chef du service des Affaires économiques
Commission nationale de l'Informatique et des Libertés (CNIL)
David NACCACHE
Professeur
École normale supérieure

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 ;

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

Total des cartes en circulation en 2015 : 84,2 millions,

- dont 71,7 millions de cartes de type « interbancaire » (« CB », MasterCard, Visa) ;

- et 12,5 millions de cartes de type « privatif ».

Cartes mises en opposition [1] en 2015 : environ 870 000.

Les transactions nationales sont celles qui mettent en jeu un émetteur français et un commerçant accepteur français. Jusqu'en 2009, les transactions internationales étaient de deux types : émetteur français/accepteur étranger et émetteur étranger/accepteur français. À partir de 2010, l'Observatoire distinguant les transactions internationales avec la zone SEPA de celles avec le reste du monde, les transactions internationales sont donc désormais de quatre types : émetteur français/accepteur étranger hors SEPA, émetteur étranger hors SEPA/accepteur français, émetteur français/accepteur étranger SEPA, émetteur étranger SEPA/accepteur français.

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

Tableau 1

Le marché des cartes de paiement en France en 2015 – 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	8 642,17	356,87	186,19	10,59	49,18	4,17
Paiements à distance hors internet	17,19	1,99	22,24	1,19	2,01	0,36
Paiements à distance sur internet	839,24	62,51	156,02	8,83	36,51	2,06
Retraits	1 465,56	121,33	31,02	3,46	20,91	3,09
Total	**10 964,16**	**542,70**	**395,47**	**24,07**	**108,61**	**9,68**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,91	11,55	4,62	0,67	5,12	0,89
Paiements à distance hors internet	4,26	0,46	2,90	0,15	0,29	0,05
Paiements à distance sur internet	6,99	1,00	3,34	0,57	0,86	0,14
Retraits	2,89	0,26				
Total	**118,04**	**13,26**	**10,85**	**1,39**	**6,26**	**1,08**
Total général	**11 082,20**	**555,96**	**406,32**	**25,46**	**114,87**	**10,76**

Source : Observatoire de la sécurité des cartes de paiement.

Tableau 2

Le marché des cartes de paiement en France en 2015 – 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	8 642,17	356,87	196,54	12,95	76,97	8,90
Paiements à distance hors internet	17,19	1,99	4,11	0,99	1,97	0,88
Paiements à distance sur internet	839,24	62,51	43,46	4,67	16,43	2,77
Retraits	1 465,56	121,33	22,38	3,63	8,69	2,04
Total	**10 964,16**	**542,70**	**266,49**	**22,25**	**104,06**	**14,58**
Cartes de type « privatif »						
Paiements de proximité et sur automate	103,91	11,55	10,93	1,70	9,69	4,68
Paiements à distance hors internet	4,26	0,46	0,61	0,05	0,21	0,05
Paiements à distance sur internet	6,99	1,00	1,55	0,20	0,45	0,11
Retraits	2,89	0,26			0,63	0,30
Total	**118,04**	**13,26**	**13,09**	**1,95**	**10,99**	**5,14**
Total général	**11 082,20**	**555,96**	**279,58**	**24,20**	**115,06**	**19,72**

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 2015 – 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	512,0	32 076,0	71,1	7 310,3	117,5	24 208,4
Cartes perdues ou volées	497,6	31 428,2	51,9	4 112,6	19,3	4 123,7
Cartes non parvenues	6,8	456,3	0,6	59,3	0,1	9,7
Cartes altérées ou contrefaites	6,4	104,0	6,9	1 286,8	84,5	17 101,3
Numéro de carte usurpé	0,2	35,2	8,8	1 478,0	8,7	2 006,9
Autres	0,9	52,3	3,0	373,5	5,0	966,7
Paiements à distance hors internet	49,1	4 692,7	206,3	18 561,2	47,2	9 232,4
Cartes perdues ou volées	0,3	20,7	22,5	2 473,0	6,4	1 393,0
Cartes non parvenues	0,0	0,0	0,0	3,9	0,0	0,7
Cartes altérées ou contrefaites	0,0	1,0	4,2	547,7	2,0	502,8
Numéro de carte usurpé	48,7	4 669,7	178,9	15 502,5	38,5	7 317,0
Autres	0,0	1,3	0,6	34,1	0,3	18,9
Paiements à distance sur internet	1 366,7	144 099,6	1 294,2	87 390,1	196,5	20 605,7
Cartes perdues ou volées	0,6	124,2	106,7	7 809,4	18,2	2 021,2
Cartes non parvenues	0,0	0,1	0,2	11,2	0,1	5,4
Cartes altérées ou contrefaites	0,0	3,3	24,1	2 399,8	4,9	547,2
Numéro de carte usurpé	1 366,1	143 970,8	1 160,8	76 960,2	172,8	17 979,3
Autres	0,0	1,2	2,4	209,5	0,6	52,7
Retraits	132,4	39 582,1	4,8	1 138,5	105,5	18 126,8
Cartes perdues ou volées	130,8	39 268,4	3,7	890,5	6,6	1 136,7
Cartes non parvenues	0,7	206,3	0,1	28,4	0,0	6,2
Cartes altérées ou contrefaites	0,0	5,6	0,7	148,6	96,6	16 626,0
Numéro de carte usurpé	0,0	2,7	0,1	12,1	1,1	171,1
Autres	0,8	99,1	0,2	59,0	1,1	186,8
Total	**2 060,2**	**220 450,3**	**1 576,3**	**114 400,1**	**466,7**	**72 173,2**

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 2015 – 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	512,0	32 076,0	40,6	4 564,2	108,2	20 857,0
Cartes perdues ou volées	497,6	31 428,2	23,2	2 170,7	16,8	3 685,2
Cartes non parvenues	6,8	456,3	0,9	91,0	0,5	118,1
Cartes altérées ou contrefaites	6,4	104,0	5,5	414,3	76,4	13 794,2
Numéro de carte usurpé	0,2	35,2	9,8	1 696,8	13,6	2 914,8
Autres	0,9	52,3	1,2	191,5	0,9	344,7
Paiements à distance hors internet	49,1	4 692,7	29,2	7 354,3	25,7	10 198,1
Cartes perdues ou volées	0,3	20,7	1,3	172,8	1,3	338,5
Cartes non parvenues	0,0	0,0	0,0	4,8	0,0	14,8
Cartes altérées ou contrefaites	0,0	1,0	1,7	334,8	3,6	1 302,6
Numéro de carte usurpé	48,7	4 669,7	25,9	6 824,8	20,5	8 394,4
Autres	0,0	1,3	0,2	17,1	0,3	147,8
Paiements à distance sur internet	1 366,7	144 099,6	118,1	22 767,6	145,2	31 951,2
Cartes perdues ou volées	0,6	124,2	2,1	217,5	5,0	1 063,4
Cartes non parvenues	0,0	0,1	0,1	24,7	0,2	47,6
Cartes altérées ou contrefaites	0,0	3,3	2,2	379,1	11,8	2 422,8
Numéro de carte usurpé	1 366,1	143 970,8	112,7	21 980,6	126,4	28 125,7
Autres	0,0	1,2	1,0	165,7	1,8	291,7
Retraits	132,4	39 582,1	3,4	891,6	2,9	1 620,9
Cartes perdues ou volées	130,8	39 268,4	3,0	797,7	0,8	262,5
Cartes non parvenues	0,7	206,3	0,0	14,5	0,0	1,3
Cartes altérées ou contrefaites	0,0	5,6	0,2	45,9	1,5	340,3
Numéro de carte usurpé	0,0	2,7	0,1	19,5	0,0	11,2
Autres	0,8	99,1	0,1	14,0	0,6	1 005,7
Total	**2 060,2**	**220 450,3**	**191,4**	**35 577,7**	**282,1**	**64 627,3**

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 2015 – 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	4,64	2 573,70	1,72	682,89	5,52	1 574,87
Cartes perdues ou volées	1,04	399,08	0,21	89,63	0,43	156,19
Cartes non parvenues	0,71	494,44	0,14	57,66	0,04	7,07
Cartes altérées ou contrefaites	0,34	74,38	0,39	123,33	3,63	815,24
Numéro de carte usurpé	0,43	137,83	0,88	383,55	1,41	596,16
Autres	2,11	1 467,97	0,10	28,73	0,01	0,21
Paiements à distance hors internet	1,22	382,21	3,84	148,85	1,19	241,39
Cartes perdues ou volées	0,05	11,72	0,01	0,86	0,01	0,76
Cartes non parvenues	0,00	0,98	0,00	0,00	0,00	0,00
Cartes altérées ou contrefaites	0,01	0,38	0,03	3,79	0,05	8,44
Numéro de carte usurpé	1,11	329,03	3,77	143,09	1,12	226,13
Autres	0,05	40,10	0,03	1,11	0,01	6,05
Paiements à distance sur internet	4,74	1 186,75	16,94	1 617,68	2,61	468,30
Cartes perdues ou volées	0,20	38,09	0,17	14,64	0,02	5,07
Cartes non parvenues	0,06	4,84	0,01	1,93	0,00	0,03
Cartes altérées ou contrefaites	0,03	3,71	0,10	30,53	0,08	15,97
Numéro de carte usurpé	4,23	1 037,68	16,58	1 527,55	2,49	443,32
Autres	0,22	102,42	0,08	43,03	0,02	3,91
Retraits	1,38	243,41	–	–	–	–
Cartes perdues ou volées	1,30	198,90	–	–	–	–
Cartes non parvenues	0,05	10,02	–	–	–	–
Cartes altérées ou contrefaites	0,03	34,49	–	–	–	–
Numéro de carte usurpé	0,00	0,00	–	–	–	–
Autres	0,00	0,00	–	–	–	–
Total	**11,97**	**4 386,07**	**22,50**	**2 449,42**	**9,32**	**2 284,56**

Source : Observatoire de la sécurité des cartes de paiement.

Tableau 6

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » en 2015 – 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	4,64	2 573,70	0,55	211,54	3,50	1 888,78
Cartes perdues ou volées	1,04	399,08	0,06	43,38	0,57	313,46
Cartes non parvenues	0,71	494,44	0,17	54,43	0,01	2,90
Cartes altérées ou contrefaites	0,34	74,38	0,06	10,83	2,49	1 351,82
Numéro de carte usurpé	0,43	137,83	0,09	57,38	0,36	152,95
Autres	2,11	1 467,97	0,17	45,52	0,06	67,65
Paiements à distance hors internet	1,22	382,21	0,53	321,38	1,16	622,24
Cartes perdues ou volées	0,05	11,72	0,00	0,59	0,02	6,96
Cartes non parvenues	0,00	0,98	0,00	0,00	0,00	2,11
Cartes altérées ou contrefaites	0,01	0,38	0,02	2,39	0,11	34,00
Numéro de carte usurpé	1,11	329,03	0,50	310,75	1,00	540,69
Autres	0,05	40,10	0,01	7,65	0,04	38,49
Paiements à distance sur internet	4,74	1 186,75	2,60	808,08	9,85	2 525,34
Cartes perdues ou volées	0,20	38,09	0,01	4,53	0,25	49,76
Cartes non parvenues	0,06	4,84	0,00	0,35	0,16	29,95
Cartes altérées ou contrefaites	0,03	3,71	0,11	22,12	0,70	140,24
Numéro de carte usurpé	4,23	1 037,68	2,46	774,02	8,65	2 272,98
Autres	0,22	102,42	0,01	7,07	0,10	32,40
Retraits	1,38	243,41	–	–	–	–
Cartes perdues ou volées	1,30	198,90	–	–	–	–
Cartes non parvenues	0,05	10,02	–	–	–	–
Cartes altérées ou contrefaites	0,03	34,49	–	–	–	–
Numéro de carte usurpé	0,00	0,00	–	–	–	–
Autres	0,00	0,00	–	–	–	–
Total	**11,97**	**4 386,07**	**3,67**	**1 341,00**	**14,52**	**5 036,36**

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, etc. 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, etc.),

  – 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, etc.),

  – 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, etc.

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, etc.).
2 Tel que défini à l'article L132-1 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, etc. ;
• approvisionnement d'un compte, vente de particulier à particulier : sites de vente en ligne entre particuliers, etc. ;
• assurance ;
• commerce généraliste et semi-généraliste : textile/habillement, grand magasin, généraliste vente sur catalogue, vente privée, etc. ;
• équipement de la maison, ameublement, bricolage ;
• jeu en ligne ;
• produits techniques et culturels : matériel et logiciel informatiques, matériel photographique, livre, CD/DVD, etc. ;
• santé, beauté, hygiène ;
• services aux particuliers et aux professionnels : hôtellerie, service de location, billetterie de spectacle, organisme caritatif, matériel de bureau, service de messagerie, etc. ;
• téléphonie et communication : matériel et service de télécommunication/téléphonie mobile ;
• voyage, transport : ferroviaire, aérien, maritime ;
• divers.

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

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

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

Secrétariat de rédaction
Jean-Luc Bontems, Véronique Bugaj, Paul Capocci, Guylène Chotard, Florian Dintilhac, Jérôme Fanouillère, Julien Lasalle, Antoine Lhuissier, Catherine Marzolf, Lucas Nozahic, Chiraz Plantureux, Alexandre Stervinou, Mathieu Vileyn

Réalisation
Direction de la Communication
de la Banque de France

Opérateurs PAO
Nicolas Besson, Angélique Brunelle, Alexandrine Dimouchy, Christian Heurtaux, Aurélien Lefèvre, 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