2011 | 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 : 11-2324

Rapport annuel 2011
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Monsieur le ministre de l'Économie, des Finances et du Commerce extérieur
Monsieur le président du Sénat
Monsieur le président de l'Assemblée nationale

par

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

SOMMAIRE

CHAPITRE 4 : LA COOPÉRATION INTERNATIONALE EN MATIÈRE DE LUTTE CONTRE LA FRAUDE 47

ANNEXES

L'Observatoire de la sécurité des cartes de paiement, mentionné au I de l'article L. 141-4 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* [1].

Conformément à l'alinéa 6 de cet article, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre de l'Économie, des Finances et du Commerce extérieur et transmis au Parlement. Il comprend cette année :

- *un état des lieux de la sécurisation des paiements par carte sur Internet (1re partie) ;*
- *une présentation des statistiques de fraude pour 2011 (2e partie) ;*
- *une synthèse des travaux conduits en matière de veille technologique (3e partie), avec deux sujets traités : l'utilisation du mobile comme terminal de paiement et l'utilisation de portefeuilles électroniques afin d'initier des ordres de paiement par carte ;*
- *une étude sur la coopération internationale en matière de lutte contre la fraude (4e partie) ;*
- *enfin, une nouvelle annexe qui rappelle les conseils de prudence aux porteurs en matière de bonnes pratiques lors d'une opération de paiement chez un commerçant, sur Internet, ou encore lors d'un retrait (cf. annexe 1).*

1 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.

Le neuvième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2011, comprend cette année quatre parties dont les principales conclusions sont reprises ci-après.

1re partie : sécurisation des paiements par carte sur Internet

L'enquête d'opinion menée pour la deuxième année consécutive par l'Observatoire et les statistiques transmises par les établissements bancaires et leurs prestataires techniques montrent de réelles avancées en termes de sécurisation des opérations de paiement par carte sur Internet en 2011.

Pour autant, à ce jour, seulement 23 % des transactions de paiement sur Internet sont sécurisées par des dispositifs d'authentification non rejouable, alors même que ces dispositifs ont prouvé leur efficacité auprès de certains e-commerçants et que ces derniers sont bien accueillis par les consommateurs. Ainsi, la généralisation progressive de l'authentification non rejouable et donc de « 3D-Secure » auprès des e-commerçants, notamment les sites les plus fréquentés, avec un déclenchement reposant sur une analyse de risques, reste une priorité pour l'Observatoire.

*Il est à noter que ces recommandations sont en ligne avec les conclusions du rapport Pauget-Constans sur l'avenir des moyens de paiement en France et avec celles du projet de rapport du Forum européen sur la sécurité des moyens de paiement (*SecuRe Pay*), lesquelles préconisent au niveau européen la généralisation de l'authentification non rejouable du porteur en fonction du risque de la transaction lors d'un paiement sur Internet.*

2e partie : statistiques de fraude pour l'année 2011

Le taux de fraude s'établit pour l'année 2011 à 0,077 %, en légère augmentation pour la quatrième année consécutive, correspondant à un montant total de fraude de 413,2 millions d'euros (contre 0,074 % et 368,9 millions d'euros en 2010).

Alors que la fraude à l'international est en léger recul, cette hausse de la fraude s'explique au niveau national par deux tendances principales :

- *une augmentation de la fraude sur les paiements à distance, et notamment sur le canal Internet. Ainsi, le taux de fraude sur les paiements à distance atteint 0,321 %. On notera en particulier que le taux de fraude sur les paiements sur Internet continue d'augmenter pour s'établir à 0,341 %. L'augmentation est plus modérée pour les paiements à distance effectués par courrier ou par téléphone. L'ensemble des paiements à distance, qui représente 8,4 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude. L'évolution défavorable de la fraude sur ce canal de paiement conduit l'Observatoire à insister pour que ses recommandations relatives à l'adoption de dispositifs permettant l'authentification non rejouable du porteur de la carte, tels que « 3D-Secure », soient mises en œuvre par les e-commerçants, notamment les plus grands d'entre eux, pour les paiements les plus risqués ;*

- *une hausse du taux de fraude sur les paiements de proximité qui s'établit désormais à 0,015 % (contre 0,012 % en 2010). Cette tendance s'accompagne d'une poursuite de l'augmentation du taux de fraude sur les retraits qui atteint désormais 0,029 %. L'augmentation de la fraude sur*

ces transactions, qui reste néanmoins à un niveau très faible, intervient après plusieurs années de baisse. Elle s'explique en particulier par une augmentation des vols de carte avec code confidentiel. Face à ces tendances, l'Observatoire réitère ses conseils de prudence aux porteurs et rappelle les bonnes pratiques à suivre lors d'une opération de paiement chez un commerçant, sur Internet, ou encore lors d'un retrait (cf. annexe 1).

Par ailleurs et pour la deuxième année consécutive, l'Observatoire est en mesure de distinguer les taux de fraude des transactions internationales réalisées en Europe (zone SEPA) de celles réalisées hors Europe (hors zone SEPA). Les résultats constatés (des taux de fraude hors Europe près de deux fois et demie supérieurs au taux relevé en Europe pour des cartes émises en France, et des cartes étrangères émises hors Europe fraudées sept fois plus que celles émises en Europe) démontrent le bénéfice des efforts importants entrepris en Europe ces dernières années pour lutter contre la fraude, notamment en généralisant l'usage des cartes à puce au standard EMV aux points de vente et de retrait.

3e partie : travaux de veille technologique autour de la sécurité du téléphone mobile en tant que terminal de paiement et des nouvelles solutions de paiement sur Internet (portefeuilles électroniques)

Le mobile comme terminal de paiement. *Le marché des terminaux de paiement connaît de nombreuses évolutions depuis quelques mois, avec l'apparition d'offres reposant sur l'utilisation d'appareils mobiles évolués, notamment les* smartphones*. Les* smartphones *étant par essence multi-applicatifs, multi-tâches et dépourvus à ce jour d'éléments de sécurité, ils apparaissent de prime abord peu adaptés aux requis habituellement exigés sur les terminaux de paiement traditionnels, dédiés à cette fonction. L'utilisation d'un terminal de paiement mobile dans la chaîne d'acceptation ne peut donc être actuellement envisagée que concomitamment à l'adoption de mesures permettant de garantir un niveau de sécurité équivalent à celui prévalant pour les terminaux de paiement traditionnels.*

Portefeuille électronique et paiement par carte. *Dans un contexte de fort développement du commerce électronique, des solutions de paiement qualifiées d'alternatives sont apparues revêtant notamment la forme d'un portefeuille électronique. L'émergence des portefeuilles électroniques contribue à la diversification des offres de paiement en apportant aux utilisateurs des moyens adaptés à leurs usages. La multiplication de ces offres ne doit cependant pas se faire au détriment de la sécurité des moyens de paiement, au risque de compromettre d'une part la confiance dans les instruments de paiement actuels, et d'autre part de voir la fraude se déporter vers des solutions qui seraient moins sécurisées. Dans ces conditions, l'Observatoire recommande la protection des données sensibles (dont celles liées aux cartes de paiement) par l'ensemble des acteurs impliqués, le recours par le gestionnaire du portefeuille électronique à un mécanisme d'authentification non rejouable du porteur par l'émetteur au moment de l'enregistrement de la carte dans le portefeuille, une analyse de risque par le gestionnaire de portefeuilles électroniques conduisant au déclenchement d'une authentification non rejouable pour les paiements considérés comme risqués et la mise en place de règles claires quant à la gestion des instruments et opérations de paiement, notamment la définition et le partage des responsabilités entre les utilisateurs, les marchands et les gestionnaires de telles solutions.*

4e partie : la coopération internationale en matière de lutte contre la fraude

L'Observatoire a souhaité cette année réaliser un état des lieux des acteurs prenant part à la lutte contre la fraude sur le territoire et présenter les circuits de coopération existants à l'international. Il ressort de cette étude que si les acteurs se sont organisés dans leurs domaines respectifs avec des résultats tangibles et que des structures de coopération existent, à la fois au niveau national, européen ou international, des axes d'amélioration sont possibles. Il conviendrait notamment de garantir l'échange opérationnel de données de fraude aidant à la détection de points de compromission, de finaliser une approche commune, notamment en termes de gouvernance, en ce qui concerne la certification des terminaux d'acceptation et d'assurer une harmonisation des exigences sécuritaires par les autorités de régulation bancaire au niveau international.

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

La fraude sur les paiements à distance, qui représente en 2011 129,6 millions d'euros (pour un taux de fraude de 0,321 %), et les moyens mis en œuvre par les acteurs de la chaîne de paiement afin de s'en prémunir, font l'objet d'un suivi régulier par l'Observatoire. Parmi les mesures recommandées par ce dernier, la généralisation progressive de l'authentification non rejouable du porteur pour les paiements sur Internet, à chaque fois que cela est possible et pertinent, occupe une place prépondérante.

Ce chapitre présente l'état d'avancement de la mise en œuvre de cette recommandation (§ 1). Les modalités de son déploiement par les banques et les commerçants ainsi que les coûts y afférents sont ensuite abordés (§ 2). La mise en œuvre de l'authentification non rejouable s'inscrivant désormais à l'échelle européenne sous l'impulsion du nouveau forum sur la sécurité des moyens de paiement – *SecuRe Pay*, la dernière partie lui est consacrée (§ 3).

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

1|1 État d'avancement du déploiement de « 3D-Secure »

Afin de suivre le déploiement de solutions d'authentification non rejouable par les émetteurs et d'identifier les éventuelles difficultés ou axes d'amélioration, l'Observatoire réalise depuis 2011 des campagnes semestrielles de collecte de données statistiques auprès des établissements bancaires et de leurs prestataires techniques, qui permettent de mesurer l'évolution quantitative et qualitative de la mise en œuvre de l'authentification non rejouable. Les données collectées par l'Observatoire montrent ainsi une nette amélioration du taux de déploiement de tels dispositifs, tant par les émetteurs que par les commerçants, au cours de l'année 2011.

1|1|1 84 % des porteurs sont désormais équipés d'un dispositif d'authentification opérationnel

La quasi-totalité des porteurs est désormais équipée d'au moins un dispositif d'authentification non rejouable, conformément aux recommandations émises par l'Observatoire. Parmi ceux-ci, le dispositif d'authentification par SMS reste largement majoritaire [1].

Le taux d'activation [2] de ces dispositifs par les porteurs a progressé de 67 % à 84 % de la population totale des acheteurs en ligne en un an. Des disparités entre émetteurs subsistent, en raison de la complexité plus ou moins élevée du processus d'activation proposé par ces derniers. Un accompagnement des utilisateurs vers ces nouveaux dispositifs par l'ensemble des acteurs concernés reste ainsi nécessaire (cf. 1.2.3).

1|1|2 Le taux d'échec sur les transactions sécurisées reste stable, aux alentours de 20 %

Le taux d'échec sur les transactions se situe aux alentours de 20 %. Ce taux, qui peut paraître élevé de prime abord, ne tient toutefois pas compte des échecs suivis d'une nouvelle tentative plus fructueuse ainsi que des tentatives de fraude. Là encore des situations très contrastées subsistent entre émetteurs, la Banque de France traitant en bilatéral les cas les moins satisfaisants. L'Observatoire reste attentif à la diminution progressive de ce taux d'échec.

1 Certains établissements ont mis en place des solutions reposant sur un « *token* », un lecteur de cartes ou un courriel adossé à la saisie d'un code unique disponible sur une carte matricielle. On se reportera au rapport 2009 de l'Observatoire, chapitre 4 (p.51-52), pour une description plus complète de ces dispositifs d'authentification.

2 L'activation du dispositif, par exemple dans le cadre du SMS, nécessite que le porteur communique à sa banque le numéro de téléphone portable sur lequel il souhaite recevoir les codes à usage unique.

1|1|3 La part des transactions authentifiées *via* « 3D-Secure » progresse significativement grâce à la migration d'un acteur majeur du e-commerce

Si la proportion de commerçants permettant l'authentification forte des cyberacheteurs apparaît stable à environ 50 %, la part des transactions authentifiées *via* « 3D-Secure » progresse en valeur de 17,9 % à 23 % en montant sur un an.

Un acteur majeur du commerce en ligne, Voyages-SNCF.com, a en effet contribué très significativement à la progression de ces statistiques en adoptant « 3D-Secure » dès juillet 2011. Dans un premier temps, il a ciblé certaines transactions particulièrement risquées, puis a élargi progressivement le champ d'application de ces mesures de sécurité. Ces chiffres, arrêtés à l'automne 2011, devraient encore progresser au cours de l'année 2012 en raison du déploiement accéléré de « 3D-Secure » par cet acteur à partir du troisième trimestre 2011.

1|2 La perception des dispositifs d'authentification non rejouable par les cyberacheteurs français

L'Observatoire a souhaité actualiser, en 2011, les résultats du sondage réalisé dans le cadre de son rapport 2010, et destiné à évaluer la perception des porteurs sur les dispositifs d'authentification non rejouable [3]. Le dispositif le plus utilisé reste l'envoi d'un code par SMS, conformément aux données collectées auprès des émetteurs. Les dispositifs utilisés bénéficient d'une notoriété accrue et la part des utilisateurs d'au moins un dispositif progresse sensiblement, en lien avec le déploiement progressif de « 3D-Secure » notamment sous l'impulsion de Voyages-SNCF.com.

1|2|1 Le paiement par carte sur Internet est perçu comme sûr par 77 % des cyberacheteurs

Le paiement par carte est perçu comme un moyen sûr de régler ses achats en ligne, même si la part des utilisateurs inquiets progresse sensiblement par rapport à l'année précédente (de 23 à 33 %). On notera que ce sentiment d'inquiétude diminue avec la fréquence d'achat et l'utilisation d'au moins un dispositif d'authentification non rejouable.

Ces résultats traduisent un besoin des interrogés de se sentir rassurés lorsqu'ils achètent en ligne et valident l'action de l'Observatoire, qui vise à promouvoir la mise en œuvre de dispositifs d'authentification renforcée du porteur.

1|2|2 Une notoriété grandissante des dispositifs d'authentification renforcée pour sécuriser les achats par carte en ligne

Plus de huit cyberacheteurs sur dix (83 %) indiquent avoir déjà entendu parler de dispositifs d'authentification pour sécuriser leurs achats par carte sur Internet (contre 79 % en 2011). La notoriété de ces dispositifs apparaît donc bien établie et même confortée au sein de la population des cyberacheteurs.

Même si la part des cyberacheteurs déclarant avoir reçu des informations de leur banque progresse de 39 à 44 %, son faible niveau justifie les attentes de ces derniers en matière de communication (cf. 1.2.3). En revanche, l'information apparaît toujours claire lorsqu'elle est transmise par les acteurs concernés, ce sentiment se trouvant même renforcé d'une année sur l'autre (de 84 à 89 %).

1|2|3 La facilité d'utilisation reste un élément clé

Des dispositifs toujours jugés très majoritairement faciles à utiliser...

Seuls 8 % des utilisateurs déclarent trouver au moins un des dispositifs d'authentification non rejouable difficile à utiliser. Ce pourcentage est stable par rapport à l'année précédente. Les mini-lecteurs de cartes et les cartes matricielles sont toujours perçus comme les dispositifs les moins faciles à utiliser.

... mais qui nécessitent toujours un accompagnement à la première utilisation ou ultérieurement

L'envoi de code par SMS est jugé le dispositif le plus facile à utiliser. Les banques ont en effet clairement et majoritairement communiqué sur ce dernier.

3 Cette enquête à été réalisée par LH2. Le dispositif méthodologique est identique à celui de l'enquête similaire réalisée dans le cadre du rapport 2010 (cf. p. 35).

Par rapport à l'enquête précédente, on note une forte progression des difficultés liées à la compréhension du fonctionnement du dispositif (de 26 à 40 %) ou à son accès (de 27 à 32 %). Ces difficultés ne restent toutefois bloquantes que pour moins de 10 % des utilisateurs, lesquels ressentent moins de difficultés lors des tentatives ultérieures.

Ces résultats montrent enfin qu'un accompagnement des utilisateurs vers ces nouveaux dispositifs par l'ensemble des acteurs concernés reste nécessaire. Parmi les acteurs perçus comme les plus pertinents pour communiquer sur ces nouveaux dispositifs, les banques occupent plus que jamais une place de choix (elles sont désormais considérées comme tels par 80 % des interrogés, devant les e-commerçants à hauteur de 49 %).

1|2|4 Des dispositifs qui renforcent la sécurité, avantageant les sites marchands

Un rapport bénéfices/désagréments toujours largement en faveur de la sécurité

Près de 90 % des interrogés estiment que ces dispositifs renforcent significativement la sécurité des paiements par carte bancaire sur Internet. Seul un sur cinq estime gênant le délai supplémentaire entraîné par ces nouveaux dispositifs.

Globalement, 84 % des utilisateurs disent se sentir plus en sécurité lorsqu'ils effectuent leurs achats par carte en ligne avec ces nouveaux dispositifs, contre 76 % en 2011.

Pour les utilisateurs, ces dispositifs n'apparaissent pas comme un handicap pour les sites, mais au contraire comme un argument pouvant les conforter

Si la part des utilisateurs susceptibles d'acheter autant ou davantage sur Internet avec ces dispositifs de sécurité est stable sur 2011 (97 %), ceux désirant acheter davantage sont en revanche deux fois plus nombreux et représentent désormais 35 % des utilisateurs.

L'importance de la sécurité dans le choix du site progresse également sensiblement : 23 % déclarent qu'ils feront leurs achats exclusivement sur des sites d'e-commerce présentant un tel dispositif (17 % en 2011) et 57 % qu'ils les favoriseront (contre 54 % en 2011).

L'ensemble de ces résultats confirme l'intérêt des porteurs pour des dispositifs leur assurant une sécurité renforcée lors des achats sur Internet et une communication leur permettant de les utiliser dès le premier achat. Cette communication doit reposer en priorité sur les banques et les commerçants, lesquels sont également chargés de déployer ces dispositifs en s'appuyant sur les infrastructures proposées par les systèmes de paiement par carte. Le point suivant examine la mise en œuvre d'un tel projet ainsi que ses impacts en termes organisationnels, techniques et financiers pour les acteurs considérés.

2| Les coûts liés à la mise en œuvre de l'authentification non rejouable

Dans la continuité de l'enquête de coûts sur le déploiement d'EMV présentée dans son rapport 2010, l'Observatoire a souhaité évaluer quelles étaient les incidences pour les émetteurs et les commerçants [4] du déploiement de dispositifs d'authentification non rejouable afin de sécuriser les paiements par carte en ligne.

2|1 Un projet de taille pour les banques, plus difficile à mesurer par les commerçants

2|1|1 Les banques ont suivi des chemins variés dans la mise en œuvre de l'authentification non rejouable

Les établissements interrogés ont tous souligné l'importance des moyens humains mis à contribution, tant durant les différentes phases du projet (études préalables, développement, rédaction et suivi des

4 Les organismes suivants ont participé à l'enquête : BPCE, Crédit Agricole SA, Crédit Mutuel-CIC, Société Générale, La Banque Postale, LCL, GIE Cartes Bancaires, MasterCard, Voyages-SNCF, Air France. Parmi ceux-ci, les systèmes de paiement par carte interrogés se sont toutefois déclarés non concernés.

procédures, gestion globale du projet, formations internes…), qu'à l'issue du déploiement avec la mise en place d'équipes spécifiques de lutte contre la fraude ou de support technique pour les utilisateurs.

Les coûts liés à la mise en place de l'authentification non rejouable sont toutefois majoritairement (à hauteur de 80 à 90 %) imputables aux solutions techniques déployées :

• de nouveaux serveurs d'authentification des porteurs ont en effet dû être introduits, appelés « *Access Control Servers* » ou ACS. Les banques ont toutefois suivi des stratégies diverses en la matière, certaines ayant développé ces serveurs en interne alors que d'autres ont opté pour l'externalisation complète de la solution. La structure des coûts engendrés lors de cette phase du projet est donc très variable entre les établissements interrogés : alors que les dépenses d'investissement sont importantes dans le premier cas, elles sont faibles dans le second, mais compensées par des dépenses de fonctionnement ultérieures plus élevées ;

• l'équipement des porteurs en solutions techniques d'authentification non rejouable constitue l'autre poste de dépenses important : certaines solutions engendrent des coûts de fabrication importants (généralement pris en charge en grande partie par les émetteurs), comme les *tokens*, d'autres, comme le SMS, leur font subir des coûts récurrents qui peuvent être conséquents (cf. 2.2.1).

L'ensemble des établissements interrogés se rejoint en revanche sur l'importance des moyens dédiés à la communication, à destination :

• des porteurs, en utilisant tous les canaux disponibles (envoi de plaquettes, communication en ligne et en agence) ;

• des commerçants, afin de préciser notamment la nature et la portée du transfert de responsabilité attaché à la mise en œuvre de telles solutions.

L'effort en matière de communication doit être maintenu car attendu de tous.

2|1|2 Les commerçants intègrent ce projet dans des coûts plus globaux

Les commerçants participant à l'enquête ont éprouvé plus de difficultés à isoler les dépenses spécifiques à ce projet : les dépenses liées au support clientèle ou à la communication, qui en représentent une large part, sont en effet généralement intégrées dans les coûts globaux des centres d'appels ou des actions de marketing plus générales.

Comme pour les banques, les dépenses de nature plus technique (déploiement des dispositifs de type « 3D-Secure ») dépendent étroitement du choix opéré par les commerçants en matière d'externalisation de leur solution monétique. Certains commerçants ont en effet développé leur propre plate-forme de paiement (d'où des coûts de développement plus importants lors de l'intégration de « 3D-Secure » sur le site), d'autres font reposer leur solution sur des plates-formes gérées par des prestataires externes, ce qui engendre des coûts plus importants ultérieurement.

2|2 Des effets tangibles, tant financiers qu'organisationnels

2|2|1 Un effet réel sur la fraude, assorti d'un surcoût qui valide une approche par les risques

Les structures de coûts différentes entre établissements rendent difficile toute agrégation comme vu ci-dessus. En revanche, les établissements interrogés s'accordent sur le surcoût par transaction selon que celle-ci fait l'objet d'une authentification non rejouable du porteur, d'une authentification faible, ou qu'elle n'est pas authentifiée.

Ainsi, la mise en place d'une authentification faible engendre selon les établissements un surcoût de l'ordre de 2,5 à 5 centimes d'euro par transaction par rapport à une transaction non authentifiée. Une authentification forte du porteur leur coûterait entre 10,5 et 11 centimes de plus qu'une transaction authentifiée de façon faible. Ces données restent

toutefois variables entre établissements selon la méthode d'authentification proposée.

Ce surcoût justifie l'approche par les risques préconisée par l'Observatoire, laquelle conduit les établissements à déclencher une authentification renforcée du porteur en fonction du risque estimé lié à la transaction en cours.

L'impact de l'authentification renforcée du porteur sur le taux de fraude est, quant à lui, significatif quelle que soit la méthode retenue : même si les banques éprouvent des difficultés à isoler les effets de ce projet des autres mesures de lutte contre la fraude (tel le *scoring* des transactions), elles observent une diminution de la fraude sur les transactions à distance de 70 à 90 % selon les émetteurs (chiffres confirmés par les commerçants). La fiabilisation des bases internes de numéros de téléphone ou de courriels, qui fait partie intégrante du processus d'enrôlement des clients, rend par ailleurs plus efficaces les processus d'alerte en cas de fraude suspectée ou avérée, et permet donc une meilleure réactivité des acteurs concernés.

Les établissements bancaires soulignent en outre l'effet bénéfique d'un tel projet en termes d'image, grâce à une confiance accrue de leurs clients et une perception de sécurité plus élevée.

2|2|2 Un projet qui offre des perspectives aux commerçants, sans impact sur leur volume d'activité

Les commerçants ayant participé à l'enquête, à savoir Voyages-SNCF et Air France, soulignent que la mise en œuvre de « 3D-Secure » n'a globalement pas eu d'impact sur leur chiffre d'affaires.

Ils constatent en revanche qu'elle leur offre de réelles perspectives en termes financiers et commerciaux :

• les commerçants interrogés ont constaté une baisse des commissions payées à leur banque acquéreur ;

• la sécurisation accrue des transactions permet en outre aux commerçants d'élargir leur gamme de produits disponibles en ligne vers des produits plus onéreux ou entièrement dématérialisés, traditionnellement plus sujets à la fraude.

2|3 L'authentification renforcée prendra d'autres formes dans les années à venir

2|3|1 Les banques proposeront d'autres dispositifs

Deux enjeux importants engagent aujourd'hui une réflexion au niveau des banques :

• tout d'abord, la croissance du commerce électronique à partir de téléphones mobiles connectés sur Internet est anticipée par l'ensemble des acteurs de la chaîne de paiement. Dans ce contexte, les solutions de sécurité reposant sur la réception d'un code non rejouable sur le téléphone sont réputées moins efficaces et moins ergonomiques. Des réflexions sont donc engagées pour prendre en compte ces contraintes spécifiques ;

• ensuite, un rapprochement s'effectue entre environnements de proximité et à distance, avec par exemple l'initiation de transactions de proximité à l'aide de téléphones mobiles ou en se connectant à un environnement de vente en ligne. Les banques envisagent donc naturellement de faire converger les solutions de sécurité sur les différents canaux de vente, en proposant, aux commerçants et aux porteurs, des solutions techniques adaptées à ces nouveaux modes d'initiation des transactions.

Dans ce contexte, les plus récentes innovations technologiques leur permettent de disposer de nouveaux moyens d'authentification, telles des cartes bancaires incluant de nouvelles fonctionnalités comme la génération de codes à usage unique sur un écran intégré.

2|3|2 Les commerçants mettront à disposition ces dispositifs sur plus de canaux

La même tendance est observée du côté des commerçants, qui se montrent attentifs au développement de nouveaux modes de paiement, tels les portefeuilles électroniques. Là encore, une homogénéisation du niveau de sécurité, quel que soit le moyen de paiement proposé sur le site, leur semble indispensable.

Les réponses collectées montrent un rapport coûts/bénéfices positif pour les commerçants, sans impact sur leur chiffre d'affaires. Le surcoût généré actuellement par l'authentification non rejouable à la charge des émetteurs justifie quant à lui l'approche par les risques préconisée par l'Observatoire. Ce dernier invite ainsi de nouveau les e-commerçants les plus importants à migrer vers « 3D-Secure », recommandation reprise dans le récent rapport Pauget-Constans sur l'avenir des moyens de paiement en France [5] ainsi que dans le rapport élaboré par le *SecuRe Pay* sur la sécurité des paiements sur Internet [6], présenté ci-après.

3| *SecuRe Pay*, vers l'harmonisation du niveau de sécurité à l'échelle européenne

3|1 Une organisation associant l'ensemble des acteurs chargés de superviser la sécurité des moyens de paiement

Ce forum, créé en 2011, vise à aider les surveillants et les superviseurs de fournisseurs de services de paiement à acquérir une connaissance et une compréhension communes des enjeux dans le domaine de la sécurité des paiements de détail.

SecuRe Pay regroupe ainsi les superviseurs bancaires et banques centrales de pays membres de l'Union européenne. Il définit chaque année un programme de travail et constitue à cette fin des groupes de travail qui, en fonction des sujets traités, consultent les acteurs de marché concernés.

Les groupes constitués en 2011 ont ainsi travaillé sur la protection des services bancaires en ligne et la sécurité des paiements par carte sur Internet, dans l'objectif de lutter contre la fraude, en accord avec les priorités définies au sein de l'Observatoire. Ces travaux devraient conduire à la publication d'un premier rapport en 2012 [7], dont les recommandations finales seront appliquées par les banques, les prestataires de services de paiement et par les commerçants de manière indirecte *via* leurs banques acquéreurs.

3|2 Des recommandations en adéquation avec celles émises par l'Observatoire

Le forum préconise la généralisation de l'authentification non rejouable pour les paiements par carte sur Internet, reposant sur une approche par les risques qui vise à protéger en premier lieu les transactions les plus exposées à la fraude à chaque fois que cela est possible et pertinent.

Il inclut les solutions alternatives de paiement basées sur le paiement par carte, tels les portefeuilles électroniques et prévoit l'adoption de mesures complémentaires de sécurisation applicables au processus d'enrôlement, à la sécurité des données, à l'actualisation de l'analyse des risques, etc.

4| Conclusion : une progression constante du niveau de sécurité sur Internet, sous l'action de l'ensemble des acteurs

L'enquête d'opinion menée pour la deuxième année consécutive par l'Observatoire et les statistiques transmises par les établissements bancaires et leurs prestataires techniques montrent de réelles avancées en termes de sécurisation des opérations de paiement par carte sur Internet en 2011. La progression de la notoriété des solutions déployées à cette fin traduit la hausse de leur maturité en un an.

5 Rapport publié en mars 2012, page 17 : « Garantir une sécurité maximale des paiements par Internet en généralisant l'utilisation du dispositif 3D-Secure ». L'objectif du rapport Pauget-Constans est (1) de réaliser un état des lieux des moyens de paiement utilisés en France et (2) d'identifier les évolutions ou innovations à mener afin de mieux répondre aux besoins des consommateurs et d'améliorer la sécurité tout en réduisant les coûts de ces solutions. Le rapport préconise notamment de développer les paiements sécurisés en ligne, les paiements par carte en proximité, de réduire la part du chèque et de développer de nouveaux services autour du paiement. Il encourage les administrations publiques à participer activement à sa mise en œuvre. *http://www.banque-france.fr/ccsf/fr/publications/telechar/autres/rapport_avenir_moyens_paiement.pdf*

6 Rapport publié en avril 2012, page 11 : « *Internet payment services should be initiated by strong customer authentication*. »

7 Une consultation publique sur le projet de rapport a eu lieu d'avril à juin 2012.

Les bénéfices liés à la mise en place de moyens d'authentification renforcée et de « 3D-Secure » apparaissent en outre réels et ressentis à la fois par les établissements bancaires et les commerçants (avec une baisse importante du taux de fraude constaté sur ces opérations) et par les consommateurs, qui accueillent toujours favorablement ces dispositifs. Les coûts de déploiement apparaissent quant à eux non négligeables pour les parties prenantes, bien qu'encore difficiles à évaluer.

L'Observatoire recommande aux banques et aux commerçants de poursuivre les actions engagées afin de lutter contre la hausse du taux de fraude sur les opérations à distance, dont le niveau reste élevé (cf. chapitre 2, p. 24) :

- les banques ayant désormais quasiment achevé le déploiement des solutions d'authentification renforcée, l'enjeu pour ces dernières réside dans la mise en place de plans de communication adéquats à destination des porteurs et des commerçants visant à expliciter les modalités et l'intérêt de telles solutions. Il conviendra également pour certaines de travailler à l'amélioration du taux de réussite des transactions sécurisées ;

- la généralisation de l'authentification non rejouable et donc de « 3D-Secure » auprès des commerçants, avec un déclenchement reposant sur une analyse de risques, reste une priorité pour l'Observatoire. L'adoption de « 3D-Secure » par quelques grands e-commerçants devrait constituer dans ce cadre un élément déterminant dans la fiabilisation des bases chez les émetteurs et une diffusion plus large de ce protocole auprès des e-commerçants de taille significative ;

- ces recommandations sont enfin en ligne avec les conclusions du rapport Pauget-Constans sur l'avenir des moyens de paiement en France et avec celles du rapport de *SecuRe Pay* sur la sécurisation des paiements sur Internet en Europe, lesquelles préconisent respectivement la généralisation de l'authentification non rejouable et l'authentification renforcée du porteur en fonction du risque de la transaction lors de paiement sur Internet.

Statistiques de fraude pour 2011

Depuis 2003, l'Observatoire établit des statistiques de fraude sur les cartes de paiement de type « interbancaire » et de type « privatif », sur la base de données recueillies auprès des émetteurs et des accepteurs. Ce recensement statistique suit une définition et une typologie harmonisées, établies dès la première année de fonctionnement de l'Observatoire et reprises en annexe 6 du présent rapport. Une synthèse des statistiques pour 2011 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou de retrait) et l'origine de la fraude (carte perdue ou volée, carte non parvenue, carte altérée ou contrefaite, numéro de carte usurpé). En complément, une série d'indicateurs détaillés est présentée dans l'annexe 5 de ce rapport.

Encadré 1

Statistiques de fraude : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire recueille les données de l'ensemble des émetteurs de cartes de type « interbancaire » ou « privatif ».

Les statistiques calculées par l'Observatoire portent ainsi sur :

- *485,2 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 64,7 millions de cartes de type « interbancaire » émises en France (dont 1,92 million de porte-monnaie électroniques et 3,26 millions de cartes sans contact) ;*

- *18,8 milliards d'euros de transactions réalisées (principalement en France) avec 21,0 millions de cartes de type « privatif » émises en France ;*

- *29,6 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.*

Les données recueillies proviennent :

- *de neuf émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club et Franfinance ;*

- *des 130 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et de Visa Europe France ;*

- *des émetteurs du porte-monnaie électronique Moneo.*

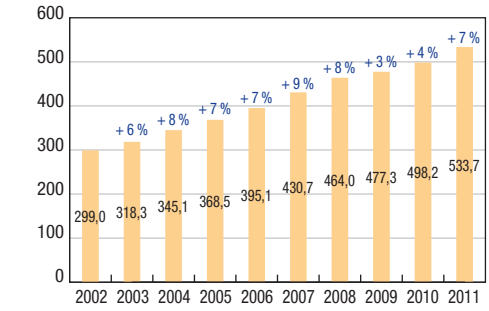
1| Vue d'ensemble

En 2011, le montant total des paiements par carte s'élève à 533,7 milliards d'euros, en croissance de 7 % par rapport à 2010. Le rythme de croissance annuelle de l'activité retrouve un niveau proche de ceux observés de 2004 à 2008, après deux années de croissance plus modérée en 2009 (+ 3 %) et 2010 (+ 4 %).

Graphique 1

Évolution du montant des transactions

(en milliards d'euros)



Source : Observatoire de la sécurité des cartes de paiement

Le montant total de la fraude est quant à lui en forte augmentation (+ 12 % par rapport à 2010) pour s'élever à 413,2 millions d'euros en 2011. Alors que la fraude à l'international est en léger recul, cette hausse sensible de la fraude s'explique au niveau national par deux tendances principales :

• une augmentation de nouveau importante, comme chaque année, de la fraude sur les paiements à distance et notamment sur le canal Internet. L'ensemble des paiements à distance, qui représente 8,4 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude ;

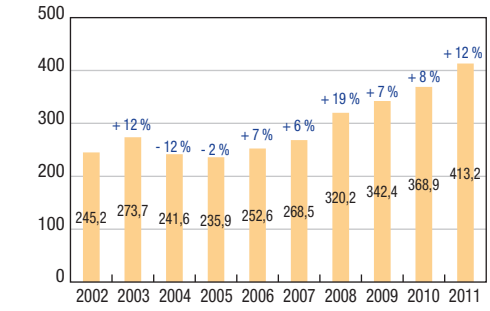
• pour la première fois depuis plusieurs années, une hausse de la fraude en paiement de proximité, accompagnée d'une poursuite de l'augmentation de la fraude sur les retraits également observée l'année dernière. Pour autant, le taux de fraude sur ce type de transaction reste près de vingt fois inférieur au taux de fraude observé sur les transactions à distance.

Compte tenu de ces évolutions, le taux de fraude sur les paiements et les retraits par carte enregistré en 2011 dans les systèmes français s'élève à 0,077 %, en légère augmentation pour la quatrième année consécutive.

Graphique 2

Évolution du montant de la fraude

(en millions d'euros)



Source : Observatoire de la sécurité des cartes de paiement

Le taux de la fraude émetteur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France s'établit en 2011 à 0,061 %, pour un montant de fraude de 306,8 millions d'euros (contre 0,057 % et 269,3 millions d'euros en 2010).

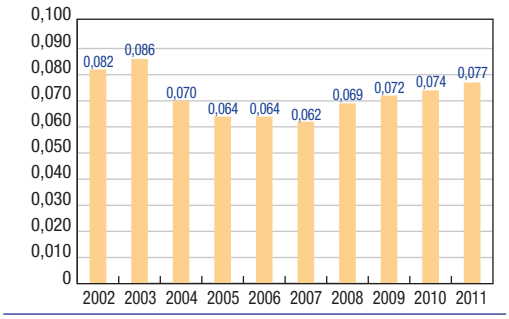
Le taux de la fraude acquéreur, c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France quelle que soit l'origine géographique de la carte, est en augmentation plus sensible. Il s'établit en 2011 à 0,063 %, pour un montant de fraude de 317,8 millions d'euros (contre 0,055 % en 2010, pour un montant de fraude de 263 millions d'euros).

Le montant moyen d'une transaction frauduleuse est également en augmentation, pour s'établir à 130 euros contre 122 euros en 2010.

Graphique 3

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement

2| Répartition de la fraude par type de carte

Tableau 1

Répartition de la fraude par type de carte

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

	2007	2008	2009	2010	2011
Cartes de type « interbancaire »	0,063 (253,6)	0,070 (304,3)	0,072 (324,3)	0,074 (351,5)	**0,077 (394,9)**
Cartes de type « privatif »	0,052 (15,0)	0,054 (16,0)	0,068 (18,2)	0,080 (17,4)	**0,083 (18,3)**
Total	0,062 (268,5)	0,069 (320,2)	0,072 (342,4)	0,074 (368,9)	**0,077 (413,2)**

Source : Observatoire de la sécurité des cartes de paiement

La progression du taux de fraude est constatée de manière équivalente sur les cartes de type « interbancaire » ou « privatif ».

Pour les cartes de type « interbancaire », les taux de fraude émetteur et acquéreur sont respectivement de 0,061 % et de 0,062 % (contre 0,057 % et 0,055 % en 2010). La valeur moyenne d'une transaction frauduleuse est de 127 euros, contre 119 euros en 2010.

Pour les cartes de type « privatif », les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,059 % et à 0,071 % (contre 0,063 % et 0,068 % en 2010). La valeur moyenne d'une transaction frauduleuse s'élève à 321 euros en 2011, contre 353 euros en 2010.

3| Répartition de la fraude par zone géographique

La répartition de la fraude par zone géographique est marquée en 2011 par la forte augmentation de la fraude sur les transactions nationales qui atteint 211,5 millions d'euros (+ 29,1 % par rapport à 2010). Ainsi, pour la première fois depuis la création de l'Observatoire en 2002, le montant de la fraude sur les transactions nationales dépasse celui de la fraude sur les transactions internationales, qui est en légère diminution à 201,7 millions d'euros (– 1,6 % par rapport à 2010).

Pour autant, au regard du montant des opérations en jeu, le taux de fraude sur les transactions internationales (0,367 %) reste près de huit fois plus élevé que le taux de fraude sur les opérations nationales (0,044 %).

Les transactions internationales représentent ainsi un peu plus de 10 % de la valeur totale des paiements par carte mais comptent pour 49 % du montant total de la fraude.

Tableau 2

Répartition de la fraude par zone géographique

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

	2007	2008	2009	2010	2011
Transactions nationales	**0,029 (114,5)**	**0,031 (130,9)**	**0,033 (144,0)**	**0,036 (163,8)**	**0,044 (211,5)**
Transactions internationales	**0,368 (154,0)**	**0,427 (189,4)**	**0,449 (198,4)**	**0,423 (205,0)**	**0,367 (201,7)**
- dont émetteur français et acquéreur étranger [a]	0,476 (85,3)	0,594 (118,3)	0,594 (121,6)	0,728 (54,9)	0,638 (51,0)
- dont émetteur français et acquéreur SEPA	–	–	–	0,331 (50,6)	0,255 (44,3)
- dont émetteur étranger [b] et acquéreur français	0,288 (68,7)	0,291 (71,0)	0,324 (76,8)	0,831 (64,5)	0,892 (81,3)
- dont émetteur SEPA et acquéreur français	–	–	–	0,195 (35,0)	0,122 (25,1)
Total	**0,062 (268,5)**	**0,069 (320,2)**	**0,072 (342,4)**	**0,074 (368,9)**	**0,077 (413,2)**

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

La fraude sur les transactions internationales réalisées avec des cartes émises en France s'élève à 95,3 millions d'euros, en diminution sensible (– 9,7 %) par rapport à 2010 (105,5 millions d'euros de fraude). On note que le taux de fraude sur les transactions effectuées hors zone SEPA avec des cartes émises en France (0,638 %), est plus de deux fois et demie supérieur à celui des transactions effectuées au sein de la zone SEPA avec ces mêmes cartes (0,255 %).

La fraude sur les transactions effectuées en France avec des cartes étrangères est, à l'inverse, en augmentation (106,4 millions d'euros en 2011 contre 99,5 millions d'euros en 2010, soit + 6,9 %). On notera cependant que la fraude sur les transactions effectuées en France avec des cartes étrangères émises au sein de la zone SEPA diminue fortement (25,1 millions d'euros en 2011 contre 35 millions d'euros en 2010, soit - 28 %) alors que la fraude sur les transactions effectuées en France avec des cartes étrangères émises en dehors de la zone SEPA augmente quant à elle fortement (81,3 millions d'euros en 2011 contre 64,5 millions d'euros en 2010, soit + 26 %).

Ainsi, le taux de fraude sur les transactions effectuées en France avec des cartes étrangères émises hors de la zone SEPA est désormais plus de sept fois supérieur à celui des transactions effectuées avec des cartes étrangères émises dans la zone SEPA (0,892 % contre 0,122 %), justifiant ainsi les efforts réalisés depuis plusieurs années en Europe pour migrer l'ensemble des cartes et des terminaux de paiements vers le standard EMV (cf. chapitre 3.3. – État d'avancement de la migration EMV).

4| Répartition de la fraude par type de transaction

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

En ce qui concerne les transactions nationales, on observe que :

- le taux de fraude sur les paiements de proximité et sur automate augmente pour s'établir à 0,015 % alors qu'il diminuait régulièrement depuis 2004. Ces paiements, qui représentent plus de 67 % du montant des transactions nationales, ne représentent néanmoins que 23 % du montant de la fraude.

Le taux de fraude sur les retraits est également en augmentation pour s'établir à 0,029 %.

Tableau 3

Répartition du taux de fraude nationale par type de transaction

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

	2007	2008	2009	2010	2011
Paiements	0,032 (95,6)	0,036 (111,7)	0,038 (123,2)	0,041 (137,3)	0,049 (177,8)
dont paiements de proximité et sur automate	0,017 (45,4)	0,015 (44,5)	0,014 (41,0)	0,012 (36,2)	0,015 (48,1)
dont paiements à distance	0,236 (50,1)	0,252 (67,2)	0,263 (82,2)	0,262 (101,1)	0,321 (129,6)
dont par courrier/téléphone	*0,201* *(23.8)*	*0,280* *(28,5)*	*0,263* *(30,3)*	*0,231* *(27,3)*	*0,259* *(25,4)*
dont sur Internet	*0,281* *(26,4)*	*0,235* *(38,8)*	*0,263* *(51,9)*	*0,276* *(73,9)*	*0,341* *(104,2)*
Retraits	0,020 (19,0)	0,018 (19,1)	0,019 (20,8)	0,024 (26,5)	0,029 (33,7)
Total	**0,029** **(114,5)**	**0,031** **(130,9)**	**0,033** **(144,0)**	**0,036** **(163,8)**	**0,044** **(211,5)**

Source : Observatoire de la sécurité des cartes de paiement

L'augmentation de la fraude sur ces transactions peut s'expliquer par un contexte économique plus difficile que les années précédentes et une augmentation des vols de carte avec code confidentiel auprès des populations les plus fragiles. Ainsi, le nombre de cartes en opposition, pour lesquelles au moins une transaction frauduleuse a été observée, est en augmentation sensible de 16 % (745 000 cartes en 2011 contre 640 500 en 2010). Parallèlement, on note une augmentation importante (+ 18 %) des piratages de distributeurs automatiques de billets qui semblent désormais une cible privilégiée pour des réseaux de fraude organisés, comme le confirme l'augmentation du nombre d'affaires traitées par les forces de l'ordre en la matière (voir encadré 4 sur les indicateurs des services de police et de gendarmerie). Face à cette tendance, l'Observatoire réitère ses conseils de prudence aux porteurs en matière de bonnes pratiques lors d'une opération de paiement chez un commerçant, sur Internet, ou encore lors d'un retrait (cf. annexe 1).

• le taux de fraude sur les paiements à distance est quant à lui en forte augmentation à 0,321 % (+ 22 %), plus de vingt fois plus élevé que le taux de fraude sur les paiements de proximité. On notera en particulier que le taux de fraude sur les paiements sur Internet continue d'augmenter pour s'établir à 0,341 %. L'augmentation est plus modérée pour les paiements à distance effectués par courrier ou par téléphone. Dans un contexte de croissance toujours soutenue du commerce électronique, les paiements à distance, qui ne représentent que 8,4 % de la valeur des transactions nationales, comptent pour 61 % du montant de la fraude (ratio stable par rapport à 2010).

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

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

On remarque que la fraude a diminué sur les paiements de proximité et sur automate réalisés à l'étranger avec des cartes françaises (28,6 millions d'euros en 2011 contre 35,0 millions d'euros en 2010). Le taux de fraude sur les paiements de proximité réalisés avec des cartes françaises hors de la zone SEPA (0,369 %) est deux fois et demie supérieur à celui des paiements de proximité effectués dans la zone SEPA (0,140 %) – où les points de vente ont pratiquement tous migré à EMV. Cependant, ce ratio a été divisé par deux entre 2010 et 2011 grâce aux efforts réalisés par les émetteurs de cartes pour lutter contre la fraude en contrefaçon de piste magnétique.

Le taux de fraude sur les paiements réalisés avec des cartes étrangères émises hors de la zone SEPA augmente (1,056 % en 2011 contre 0,982 % en 2010) et est désormais trois fois et demie supérieur (contre deux fois et demie en 2010) à celui des paiements réalisés avec des cartes étrangères émises au sein de la zone SEPA – où les émetteurs ont pratiquement tous migré leurs parcs de cartes à EMV.

Si la fraude a diminué sur les paiements à distance réalisés avec des cartes françaises (45,0 millions d'euros en 2011 contre 54,0 millions d'euros en 2010), on constate toujours un taux de fraude sur les paiements à distance particulièrement élevé (1,320 % hors zone SEPA) et beaucoup plus important que celui sur les paiements de proximité et sur automate. Le taux de fraude sur les paiements à distance réalisés avec des cartes françaises dans la zone SEPA a par contre fortement diminué (0,571 % en 2011 contre 0,944 % en 2010) et le déploiement de dispositifs d'authentification renforcée, sous l'impulsion notamment des recommandations du Forum européen sur la sécurité des moyens de paiement (*SecuRe Pay* – cf. chapitre 1) devrait permettre de confirmer cette tendance.

Enfin, on remarque une augmentation de la fraude sur les retraits, qui concerne principalement les transactions réalisées par les cartes françaises à l'étranger hors zone SEPA, où l'utilisation d'EMV n'est pas généralisée.

Encadré 2

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

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

Tableau

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

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

Secteur	Montant de fraude	Part du secteur dans la fraude
Voyage, transport	31,9	24,9
Commerce généraliste et semi-généraliste	21,4	16,7
Services aux particuliers	19,3	15,1
Téléphonie et communication	17,8	13,9
Produits techniques et culturels	10,8	8,4
Équipement de la maison, ameublement, bricolage	9,9	7,7
Approvisionnement d'un compte, vente de particulier à particulier	6,6	5,1
Services aux professionnels	3,2	2,5
Divers	2,6	2,0
Alimentation	2,2	1,7
Jeu en ligne	2,0	1,5
Assurance	0,4	0,3
Santé, Beauté, Hygiène	0,1	0,1
Total	**128,3**	**100,0**

Les secteurs Voyage/transport, Commerce généraliste et semi-généraliste, Services aux particuliers et Téléphonie et communication représentent 70 % du montant de la fraude sur Internet, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Produits techniques et culturels, Équipement de la maison, ameublement, bricolage).

On note également que le taux de fraude sur le secteur Jeu en ligne a fortement baissé en 2011 à 0,303 % contre 0,478 % en 2010 et 0,740 % en 2009, et qu'il se situe désormais en dessous du taux moyen de fraude tous secteurs confondus (cf. histogramme ci-après). Cette tendance s'explique par un déploiement progressif des dispositifs d'authentification non rejouable du porteur par les sites de jeux en ligne conformément aux recommandations de l'Observatoire et aux actions complémentaires de sensibilisation de l'Autorité de Régulation des Jeux en Ligne.

Graphique

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

(en %)

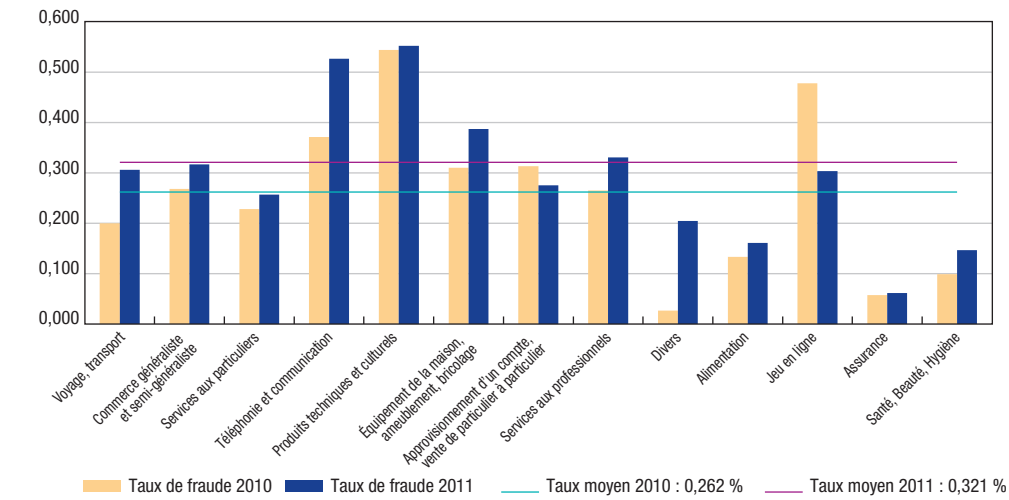


Tableau 4

Répartition du taux de fraude internationale par type de transaction

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

Émetteur français – Acquéreur étranger [a]	**2008**	**2009**	**2010**	**2011**
Paiements	0,655	0,679	0,795	0,561
	(99,3)	(105,2)	(39,8)	(30,5)
dont paiements de proximité et sur automate	0,286	0,406	0,655	0,369
	(32,0)	(44,7)	(25,8)	(16,0)
dont paiements à distance	1,698	1,350	1,310	1,320
	(67,2)	(60,5)	(14,0)	(14,5)
dont par courrier/téléphone	*1,284*	*1,016*	*1,193*	*1,011*
	(11,2)	*(9,7)*	*(3,8)*	*(3,1)*
dont sur Internet	*1,815*	*1,440*	*1,360*	*1,440*
	(56,0)	*(50,8)*	*(10,2)*	*(11,4)*
Retraits	0,399	0,331	0,596	0,800
	(19,1)	(16,5)	(15,1)	(20,5)
Total	**0,594**	**0,594**	**0,728**	**0,638**
	(118,3)	**(121,6)**	**(54,9)**	**(51,0)**
Émetteur français – Acquéreur SEPA				
Paiements	–	–	0,396	0,300
			(49,1)	(43,1)
dont paiements de proximité et sur automate	–	–	0,112	0,140
			(9,2)	(12,6)
dont paiements à distance	–	–	0,944	0,571
			(40,0)	(30,5)
dont par courrier/téléphone	–	–	*0,566*	*0,643*
			(4,0)	*(5,6)*
dont sur Internet	–	–	*1,021*	*0,557*
			(36,0)	*(24.9)*
Retraits	–	–	0,052	0,040
			(1,5)	(1,2)
Total	**–**	**–**	**0,331**	**0,255**
			(50,6)	**(44,3)**
Émetteur étranger [b] **– Acquéreur français**				
Paiements	0,339	0,397	0,982	1,056
	(65,4)	(74,1)	(63,2)	(80,7)
Retraits	0,110	0,055	0,103	0,042
	(5,6)	(2,8)	(1,4)	(0,6)
Total	**0,291**	**0,324**	**0,831**	**0,892**
	(71,0)	**(76,8)**	**(64,5)**	**(81,3)**
Émetteur SEPA – Acquéreur français				
Paiements	–	–	0,239	0,155
			(33,8)	(24,3)
Retraits	–	–	0,032	0,017
			(1,2)	(0,8)
Total	**–**	**–**	**0,195**	**0,122**
			(35,0)	**(25,1)**

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

5| Répartition de la fraude selon son origine

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

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

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

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

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

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

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

L'origine de fraude la plus importante (59,9 %) est celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance. Elle est en légère diminution (60,5 % en 2010). La fraude liée aux pertes et vols de cartes représente encore 36,1 % des paiements nationaux frauduleux, en augmentation (34,2 % en 2010) après trois années consécutives de baisse. Cette tendance vient corroborer l'augmentation des fraudes constatées en paiement de proximité ou en retrait, pour lesquelles la possession d'une carte non mise encore en opposition est requise. La contrefaçon de cartes n'est à l'origine que de 2,3 % des paiements nationaux frauduleux, en légère diminution (2,4 % en 2010).

Enfin, on observe une stabilité de la rubrique « autres », qui est généralement utilisée par les systèmes de carte de type « privatif » pour indiquer les fraudes par ouverture frauduleuse d'un compte ou d'un dossier de crédit (fausse identité) et qui est très significative pour ce type de carte (près de 40 %).

Tableau 5

Répartition de la fraude nationale selon son origine et par type de carte en 2011

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

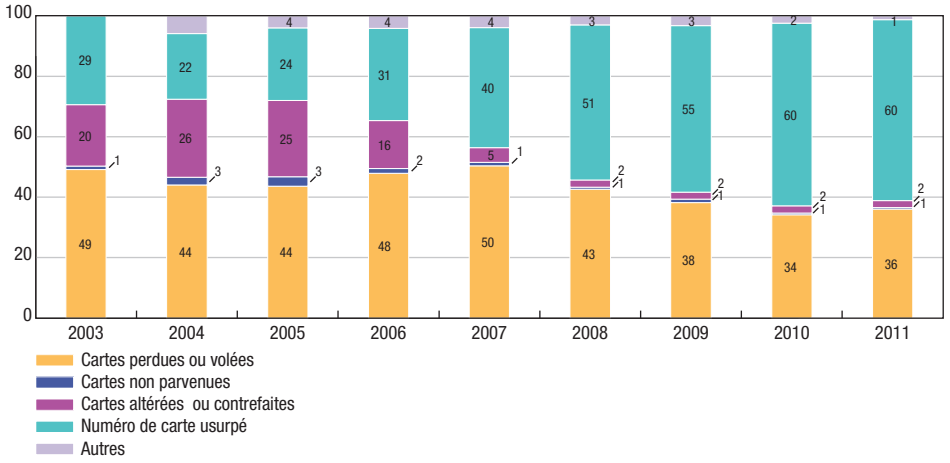
	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant	Part	Montant	Part	Montant	Part
Carte perdue ou volée	76,3	36,1	74,8	36,5	1,5	22,2
Carte non parvenue	1,1	0,5	0,5	0,2	0,6	8,9
Carte altérée ou contrefaite	4,9	2,3	4,1	2,0	0,8	12,7
Numéro usurpé	126,6	59,9	125,4	61,2	1,2	18,7
Autres	2,7	1,3	0,2	0,1	2,5	37,5
Total	211,5	100	204,9	100	6 ,6	100

Source : Observatoire de la sécurité des cartes de paiement

Graphique 4

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

(en %)



Source : Observatoire de la sécurité des cartes de paiement

Encadré 3

Indicateurs des services de police et de gendarmerie

Pour l'année 2011, les services de police et de gendarmerie enregistrent une stabilité des interpellations pour fraude à la carte bancaire, faisant état de 234 personnes interpellées contre 235 en 2010, 190 en 2009 et 154 en 2008.

Les attaques de distributeurs automatiques de billets (DAB) sont en hausse sensible avec 622 piratages de DAB en 2011 (contre 527 en 2010, 526 en 2009, 427 en 2008, 391 en 2007, 515 en 2006, 200 en 2005 et 80 en 2004). À celles-ci s'ajoutent 32 attaques de terminaux de paiement (contre 30 en 2010). Ces chiffres en hausse confirment dans les faits la tendance haussière des statistiques relevées par l'Observatoire concernant la fraude en retrait ou en paiement. Par contre, aucune attaque de distributeur automatique de carburant (DAC) n'a été constatée en 2011 (contre 6 en 2010).

Face à de tels agissements, de nombreuses enquêtes ont été diligentées sur l'ensemble du territoire national et six officines de contrefaçon de cartes bancaires étrangères ont ainsi été démantelées sur l'ensemble du territoire.

Veille technologique

1| Le mobile comme terminal de paiement

Les terminaux de paiement électroniques (TPE) évoluent régulièrement au gré des changements technologiques liés soit à la carte de paiement utilisée (migration aux standards EMV – *Europay MasterCard Visa* notamment), soit aux réseaux ou protocoles de communication supportés (utilisation des réseaux GPRS – *General Packet Radio Service*, 3G – troisième génération, WiFi, support du protocole NFC[1], etc.). Ces évolutions conduisent régulièrement à reconsidérer les implications en termes de sécurité pour le terminal de paiement. L'Observatoire s'est penché ces dernières années sur plusieurs de ces évolutions, en particulier celles concernant la migration aux standards EMV (rapport 2009, chapitre 3, p. 41), l'apparition des terminaux légers (rapport 2009, chapitre 3, p. 38) ou encore la sécurité des réseaux d'automates de paiement (rapport 2008, chapitre 3, p. 36).

Les appareils permettant à un commerçant disposant d'un point de vente physique d'accepter les paiements par carte sont aujourd'hui dédiés à ces seules opérations[2]. Ils offrent ainsi les fonctions d'affichage du paiement à effectuer, de reconnaissance et de validation des cartes (à piste ou à puce), de saisie du code PIN (*Personal Identification Number*) du porteur (dans ce dernier cas) et de transmission de l'ensemble des données de transaction sur les serveurs de l'acquéreur, de façon sécurisée.

Toutefois, les récentes évolutions technologiques permettent à des appareils, dont ce n'est pas la fonction première, de remplir en partie ou en totalité ces fonctionnalités. Par définition mobile et disposant de capacités techniques avancées, le *smartphone*[3] semble promis à jouer un rôle accru dans ce cadre. À ce jour, plusieurs solutions existent déjà sur le marché, notamment aux États-Unis avec des offres destinées aux petits commerçants souvent très mobiles (photographes, artisans, livreurs, etc.). Ces dernières permettent par exemple de réaliser des encaissements sur le lieu de la prestation ou de désengorger une file d'attente dans un grand commerce par le simple ajout de points d'acceptation de paiement. Ces offres, bien qu'aujourd'hui marginales dans l'industrie du paiement, pourraient prendre de l'ampleur car elles permettent un encaissement fluide et accessible à toute personne physique ou morale disposant d'un simple *smartphone*, sans nécessiter d'équipement dédié. Ceci explique leur développement rapide dans des environnements où le terminal de paiement traditionnel n'avait jusqu'alors pas réussi à s'implanter.

L'Observatoire a souhaité analyser le fonctionnement et la sécurité du terminal de paiement sur mobile afin d'évaluer dans quelles conditions sécuritaires cette nouvelle solution d'acceptation des paiements pouvait être mise en œuvre en France. Cette analyse comporte, dans un premier temps, une description des différentes solutions existant sur le marché en fonction de la présence ou non d'un dispositif physique connecté au mobile, puis détaille les enjeux sécuritaires qui leur sont liés.

1|1 Les différents modes d'utilisation du mobile en tant que TPE

Les encaissements par carte réalisés sur l'appareil mobile présentent des fonctionnalités différentes en fonction de la présence ou non d'un lecteur de cartes et des contrôles sécuritaires réalisés (vérification de la validité de la carte, de la signature du porteur ou de son code PIN). Dans cette partie, sont étudiées les modalités fonctionnelles d'acceptation de la carte sur le mobile en tant que terminal de paiement avec ou sans dispositif physique externe associé.

1 NFC est un protocole de communication à courte distance répandu pour les paiements de type sans contact (rapport 2009, chapitre 3, p. 27), alors que les réseaux GPRS, 3G ou WiFi sont des technologies de communication sans fil permettant au terminal de dialoguer avec les serveurs monétiques d'acquisition des transactions de paiement.

2 Les applications de gestion des programmes affinitaires sont ici considérées comme liées à la transaction. Elles ne seront toutefois pas développées par la suite.

3 Ou ordiphone : téléphone mobile doté de fonctionnalités autres que celles dédiées à la téléphonie : accès Internet, messagerie électronique, jeux, musique, etc. Même si d'autres types d'appareils mobiles, tels les ordinateurs ultra-portables ou les tablettes tactiles, permettraient fonctionnellement de réaliser les mêmes opérations, la présente étude se concentre sur les *smartphones* en raison de leur taux de pénétration élevé sur le marché. Dans cette étude, les termes téléphone, mobile ou *smartphone* seront invariablement utilisés pour désigner le même dispositif.

1|1|1 Sans dispositif physique connecté au mobile

Le principe de l'encaissement par téléphone sans lecteur de cartes consiste à reproduire une interface de terminal de paiement électronique sur une application mobile. De façon similaire à l'acceptation de paiements à distance sur Internet, le commerçant doit préalablement s'enregistrer auprès d'une banque acquéreur ou d'un établissement de paiement offrant un service d'acquisition des transactions. Pour réaliser un encaissement, le commerçant se connecte sur un site particulier ou ouvre une application (généralement protégés par un simple mot de passe), puis indique le montant de la transaction. Le porteur est alors invité à saisir son numéro de carte [4], la date de validité de celle-ci, ainsi que son cryptogramme visuel (CVx2 [5]) lorsque le réseau d'acceptation le permet [6]. La cinématique de la transaction est équivalente à celle rencontrée traditionnellement sur une page de paiement Internet. En l'absence de dispositif d'impression de facturette, l'envoi du ticket peut se faire optionnellement par courriel lorsqu'il est possible de saisir l'adresse de ce dernier sur l'application de paiement.

Cette solution se caractérise par sa praticité (du point de vue du commerçant) liée au fait de ne pas ajouter un quelconque dispositif physique pour l'acceptation d'un paiement par carte sur un téléphone. Toutefois, la saisie manuelle sur un écran tactile des seize chiffres de la carte (ainsi que des trois chiffres du cryptogramme visuel [7] le cas échéant) peut s'avérer préjudiciable à la fluidité du paiement. En outre, bien que l'achat soit réalisé dans un contexte de présence de la carte au moment du paiement, la transaction est considérée à l'identique d'une transaction à distance, ce qui ne lui assure pas le niveau de garantie d'un paiement de proximité.

Ce dispositif est déjà commercialisé en France, par exemple avec la solution m-Terminal d'Ogone proposant la saisie de l'ensemble des chiffres de la carte de paiement sur un écran tactile.

1|1|2 Couplé à un dispositif physique

Diverses solutions ont vu récemment le jour visant à associer le mobile avec un dispositif physique, du simple lecteur de cartes à la station d'accueil en passant par des procédés de chiffrement des données, afin de tenter de faire converger les fonctionnalités offertes par les mobiles et les terminaux de paiement.

Les lecteurs de cartes

En mode contact

Les marchés nord-américain et asiatique ont vu émerger diverses solutions (Square, Intuit, Swiff, Payfirma, Simply Swipe It, Payware, etc.) associant le téléphone à un lecteur de piste connecté sur celui-ci. Une fois les formalités de souscription au service réalisées [8], le commerçant doit préalablement télécharger l'application de paiement sur son téléphone puis est invité à s'identifier en renseignant son numéro de contrat ainsi que la clé d'activation qui lui a été communiquée par voie de courrier lors de son inscription. Par la suite, l'ouverture de l'application est conditionnée à la saisie d'un code secret personnalisé défini par le commerçant lors de cette première utilisation. La réalisation d'un encaissement par carte se déroule alors selon les étapes suivantes : le commerçant ouvre son application de paiement, connecte le lecteur sur le *smartphone*, saisit un montant puis procède à une lecture de la piste magnétique de la carte *via* le lecteur. Une fois cette lecture terminée et les contrôles de cohérence des données réalisés, le porteur valide son paiement en signant sur l'écran tactile du téléphone.

4 Certaines solutions permettent toutefois d'associer un identifiant au numéro de carte préenregistré, notamment dans le cas de porte-monnaie électronique en ligne.
5 MasterCard CVC2 (*Card Verification Code*) et Visa CVV2 (*Card Verification Value*).
6 Certains systèmes de paiement par carte réservent l'utilisation du CVx2 exclusivement aux environnements de vente à distance.
7 Trois chiffres pour les cartes « CB », Visa, MasterCard ; quatre chiffres pour une carte American Express
8 Identiques à celles réalisées dans le cas du terminal sans dispositif physique de lecture

Les vérifications de cohérence et l'identification de la carte peuvent également être réalisées de manière sécurisée à l'aide d'un dialogue avec la carte conforme aux standards EMV [9]. L'état d'avancement de la migration aux standards EMV en Europe (cf. chapitre 2) fait preuve d'une quasi-généralisation des cartes à puce sur ce périmètre, leur permettant de dialoguer de façon sécurisée avec les terminaux compatibles. Ainsi, certains pays européens voient se développer des solutions conformes aux standards EMV permettant de s'assurer de l'authenticité de la carte. Le paiement est ici aussi validé par la signature du porteur sur l'écran tactile du terminal mobile [10].

En mode sans contact

L'insertion d'une puce NFC dans le *smartphone* permet d'établir une communication sans contact entre l'appareil mobile et la carte (elle-même devant être équipée d'une puce NFC). Cette connexion peut ensuite être utilisée de deux façons :

• dans un mode simplifié, elle permet d'automatiser la saisie des numéros de carte dans un environnement applicatif tel que décrit en 1|1. La communication sans contact rend alors la solution plus ergonomique, puisque le porteur n'a pas à ressaisir l'ensemble des données de sa carte ;

• la technologie NFC peut également être employée entre la carte et le *smartphone* dans le cadre d'un paiement sans contact classique : le dialogue instauré entre la carte et l'appareil mobile permet alors de mettre en œuvre les processus sécuritaires applicables à cet environnement, tels les standards EMV.

Les lecteurs de cartes avec chiffrement des données

Des lecteurs de piste ou de puce plus évolués intègrent, outre le système de lecture commun aux solutions décrites ci-dessus, un module cryptographique permettant de chiffrer les données lues avant toute transmission vers le *smartphone*. Les communications sont ainsi chiffrées de bout en bout, seul l'acquéreur ou le prestataire de services gérant la solution étant en mesure de déchiffrer les données de ces cartes.

Les stations d'accueil

Des dispositifs plus évolués (telle la solution iSMP d'Ingénico) se positionnent quant à eux en véritables concurrents des terminaux de paiement traditionnels puisqu'ils intègrent à la fois un lecteur de cartes à puce, un clavier numérique dédié, ainsi qu'optionnellement la fonctionnalité d'impression de facturettes ou de lecture de codes-barres. Ces équipements s'apparentent ergonomiquement à des « stations d'accueil » pour téléphone portable. La communication entre le lecteur et le téléphone se fait généralement au travers d'une connexion mini-USB ou d'une prise propriétaire (de type Apple).

Ces terminaux permettent une sécurisation accrue de l'environnement transactionnel par la réalisation de contrôles cryptographiques liés aux données d'authentification de la carte et du porteur directement sur le périphérique associé et non plus sur le mobile. La présence d'éléments sécurisés tels que le pavé numérique dédié et le dispositif de lecture des cartes à puce entraîne logiquement un coût plus élevé de fabrication de ces terminaux. La preuve de paiement est délivrée au porteur soit par l'édition d'une facturette lorsque le dispositif externe est équipé d'un module d'impression, soit par l'envoi d'un courriel reprenant les références de la transaction.

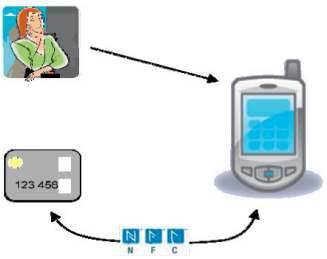
9 Organisme regroupant American Express, JCB Card, MasterCard et Visa

10 Ce dispositif ne prévoyant pas la saisie et le contrôle du PIN, il ne s'intègre toutefois pas dans les exigences requises par certains *schemes* (dont le Groupement des Cartes Bancaires « CB ») pour l'acceptation de paiements par carte en présence du porteur.

Encadré 1

Récapitulatif des différents modes d'utilisation du mobile

- *Sans dispositif physique de lecture*



(la saisie des données de carte s'effectue en mode contact ou sans contact)

- *Avec un **lecteur de cartes à piste*** *ou **à puce***

(les données sont chiffrées ou non par le dispositif physique)

- *Avec **une station d'accueil***

(l'ensemble possède des fonctions très proches de celles d'un terminal de paiement traditionnel)

1|2 Les enjeux sécuritaires liés à l'utilisation du mobile comme terminal de paiement

1|2|1 Les environnements juridique et normatif applicables à la filière d'acceptation

L'environnement juridique de l'acceptation des cartes de paiement

Le terminal de paiement électronique a pour fonction de réaliser les encaissements par carte dans les conditions définies par le réseau émetteur (par exemple le Groupement des Cartes Bancaires « CB », Visa ou MasterCard) et fixées entre l'organisme acquéreur (une banque, un établissement de paiement voire un réseau privatif) et l'accepteur (le commerçant) dans un « contrat d'acceptation ».

En l'absence de dispositions d'ordre légal ou réglementaire qualifiant les accepteurs, la possibilité offerte à une personne physique ou morale d'exercer cette fonction relève actuellement en France du domaine contractuel. L'entrée sur le marché de sociétés proposant les solutions décrites au paragraphe 1| devra donc être étudiée plus avant par les acteurs de la filière d'acquisition, afin d'évaluer l'adaptabilité du cadre contractuel en vigueur à la nature juridique des bénéficiaires potentiels de telles solutions.

Il conviendra également d'apprécier l'activité de ces acteurs au regard des dispositions de la directive sur les services de paiement [11] : si ces derniers encaissaient des fonds sur un compte ouvert à leur nom pour les reverser ensuite aux différents bénéficiaires, ce qui relève des services de paiement tels que définis au II de l'article L. 314-1 du *Code monétaire et financier,* ils devraient alors respecter les conditions d'accès à la profession et obtenir un statut d'établissement de paiement [12].

Les standards et certifications sécuritaires des terminaux

Les acteurs de la filière d'acceptation comme d'acquisition des cartes de paiement doivent se conformer à différentes règles et standards de sécurité demandés par les systèmes de paiement par carte. Pour les cartes et les terminaux, ces derniers les incluent dans leurs processus d'agrément des équipements destinés aux porteurs et aux commerçants [13].

Parmi ces règles, on note les mesures dites PCI développées par l'organisme « PCI SSC » (*Payment Card Industry Security Standard Council* [14]). Elles s'appliquent de manière mondiale à l'ensemble des acteurs de la chaîne de paiement (banques acquéreurs, commerçants, prestataires de service exploitant des plates-formes de paiement, etc.) participant aux systèmes de paiement par carte membres de PCI, à la fois pour les transactions transfrontalières, mais aussi pour les transactions nationales dans le cas de cartes co-badgées avec un système de paiement par carte national [15]. Compte tenu de ce champ d'application, ces mesures prennent, de fait, largement le caractère de standards.

Les mesures PCI ont pour objectif de lutter contre le détournement des données de carte afin d'éviter leur réutilisation frauduleuse. Plusieurs séries de règles ont été édictées par PCI SSC, dont PCI PTS (*Pin Transaction Security*), s'adressant aux fabricants de terminaux et couvrant la sécurité des dispositifs permettant la saisie du PIN lors de transactions par carte au point de vente. Les règles PA DSS (*Payment Application Data Security Standard*) visent quant à elles à sécuriser les applications destinées à stocker, traiter ou transmettre les données de carte durant les processus d'autorisation et de règlement.

L'EPC [16] a, de son côté, développé des spécifications fonctionnelles et sécuritaires définies dans son *SEPA Cards Standardisation Volume – Book of Requirements*. Le volet sécurité repose sur les règles PCI rappelées ci-dessus. Elles constituent un socle pour tout matériel (cartes ou terminaux) utilisé au sein de l'espace SEPA [17].

Par ailleurs, afin de s'assurer que les cartes et terminaux atteignent un niveau de sécurité conforme aux normes en vigueur sur le marché, l'EPC a engagé une réflexion visant à créer un cadre de certification harmonisé en Europe pour les cartes et terminaux, reposant sur une méthodologie commune d'évaluation. L'objectif est, à terme, d'obtenir la reconnaissance mutuelle des certificats délivrés par les différentes autorités de certification, et plus généralement d'encadrer le processus d'évaluation et de certification. Parmi ces autorités, on trouve notamment en ce qui concerne les terminaux :

- EMVCo [18] pour les standards EMV, lesquels comportent deux niveaux de conformité : *Level 1* (pour les aspects interopérabilité entre les cartes et les terminaux d'acceptation) et *Level 2* (relatif aux règles de sécurité à respecter une fois le contact établi entre la puce et le terminal) ;

- PCI SSC pour les différentes spécifications PCI.

11 Directive 2077/64/CE du 13 novembre 2007
12 Art. L. 522-6 du *Code monétaire et financier*
13 Voir rapport 2010, chapitre 4, p. 41
14 PCI SSC a été créé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. International (voir rapport 2009, chapitre 1, p. 9).
15 C'est notamment le cas de la majorité des cartes émises en France par les membres du Groupement des Cartes Bancaires « CB ».
16 European Payment Council, organisme représentatif de l'industrie bancaire en Europe, chargé du développement des instruments SEPA
17 Visa a également publié un guide des bonnes pratiques sur l'acceptation des paiements par mobile (*Visa best practices for mobile payment acceptance solutions* version 1.0), dont les fondements sont là encore inspirés des règles PCI.
18 EMVCo regroupe American Express, JCB Card, MasterCard et Visa.

1|2|2 Les enjeux sécuritaires liés à l'utilisation du mobile dans ce cadre

L'authentification de la carte

Le mode d'authentification de la carte dépend de la configuration matérielle utilisée.

Sans dispositif physique

Si le mobile est utilisé seul, les données de carte (PAN – *Primary Account Number*, date d'expiration, CVx2) sont saisies par le porteur sur l'application de l'accepteur. La carte est alors authentifiée par la saisie du CVx2, qui ne doit pas être stocké sur le mobile et ultérieurement sur les serveurs de l'acquéreur en application des règles PCI.

En présence d'un lecteur connecté

Quand la configuration matérielle permet d'apparenter le mobile à un terminal de paiement (par adjonction d'un lecteur de cartes ou la connexion à une station d'accueil), le niveau sécuritaire visé doit être celui caractérisant un environnement de proximité. Seule l'utilisation d'une puce permet aujourd'hui d'authentifier la carte de manière sûre par des procédés cryptographiques éprouvés, en permettant notamment de lutter contre la capture des données écrites sur les pistes magnétiques à des fins frauduleuses [19].

L'authentification du porteur

Le mode d'authentification du porteur est étroitement lié à la configuration matérielle utilisée telle que décrite au chapitre 1.

Sans dispositif physique

La transaction s'apparente ici à une transaction réalisée à distance, comme vu précédemment. En raison du taux de fraude particulièrement élevé sur ce type de transaction, il convient dès lors d'authentifier le porteur de manière renforcée, comme le préconise l'Observatoire depuis 2008.

En présence d'un lecteur connecté

Que la carte soit authentifiée à l'aide d'une piste ou d'une puce, seule la saisie du code PIN de son porteur permet d'authentifier ce dernier de manière sûre. Toutefois, l'utilisation d'un lecteur de cartes à piste seul ne permet pas de répondre aux standards de sécurité en vigueur au sein de la zone SEPA [20]. Aujourd'hui, la communication entre la carte et le terminal doit en effet permettre d'établir un canal sécurisé, protégé par des procédés cryptographiques et à même de garantir l'intégrité et la confidentialité des informations échangées dans ce cadre, dont le code PIN.

En outre, les modalités de saisie du code PIN doivent répondre à certaines règles comme vu ci-dessus (bonnes pratiques des systèmes de paiement par carte, spécifications fonctionnelles et sécuritaires définies par l'EPC, l'ensemble reposant sur le respect des mesures PCI). Seuls les terminaux disposant de claviers sécurisés peuvent en particulier prétendre à une certification PCI PTS, ce qui n'est pas le cas des mobiles, sauf à apprécier l'ensemble formé du mobile et de sa station d'accueil, cette dernière répondant elle-même à ces règles.

La protection des données de la transaction

L'enjeu réside dans la sécurisation des données de la transaction (comprenant principalement le numéro de la carte, sa date de validité, le code PIN du porteur et les éventuels certificats de transaction) entre chacun des éléments communicants : dispositif physique de lecture, téléphone mobile et serveurs d'acquisition.

Contenues sur le terminal de paiement

Certains périphériques (lecteurs de cartes à piste ou à puce) font transiter les données de la carte vers le mobile *via* sa prise *jack* [21]. Afin d'éviter les risques de compromission des données lors de cette phase, sensible à des attaques du type « homme du milieu » [22], il convient de protéger les données par des procédés cryptographiques conformes à l'état de l'art. Certains dispositifs intègrent ces

19 « *Skimming* », voir chapitre 5, rapport 2010
20 Un des prérequis du SEPA Card Framework est l'utilisation des standards EMV.
21 Prise audio analogique
22 Ce type d'attaque consiste à intercepter des données entre un émetteur et un récepteur sans que ces derniers en aient connaissance.

fonctions en étant capables de chiffrer les données dès leur lecture par des « têtes chiffrantes » comme vu précédemment.

Il convient ensuite de protéger les données sur le téléphone mobile avant leur transmission vers les serveurs d'acquisition ou les concentrateurs monétiques. Les principaux systèmes d'exploitation embarqués dans les terminaux mobiles (iOS d'Apple, Android de Google, Windows Phone, Symbian de Nokia, Bada de Samsung, etc.) ont été conçus pour le grand public en privilégiant l'accessibilité et la convivialité. De ce fait, la sécurité du système d'exploitation, déterminante dans la protection des applications de paiement, constitue un maillon faible dans le développement des applications d'encaissement mobile. Ces applications étant de surcroît téléchargeables à distance sur le téléphone mobile, l'accepteur s'expose au risque de diffusion d'une fausse application de paiement chargée en réalité de récupérer les données confidentielles du porteur.

Afin de pallier ce manque de sécurisation, des mesures complémentaires pourraient être mises en œuvre permettant de se prémunir contre les risques de compromission du terminal mobile. Cela passe par exemple par une politique de contrôle d'accès aux ressources système du mobile et la possibilité de chiffrement des données sur le mobile. D'autre part, un mécanisme de cloisonnement et de signature des applications pourrait compléter le dispositif de sécurité garantissant la qualité et l'intégrité des applications de paiement.

Ce dernier mécanisme paraît enfin d'autant plus prégnant s'agissant des applications de paiement que ces dernières ne peuvent prétendre à une certification par PCI SSC : cet organisme a en effet réalisé en juin 2011 une analyse des risques associés à l'encaissement par carte sur téléphone mobile dans le cadre d'une homologation PA-DSS. Le résultat de cette analyse conclut que les applications mobiles pouvant prétendre à une certification PA-DSS sont strictement restreintes :

- aux terminaux répondant aux standards PCI PTS (actuellement version 3.1), c'est-à-dire capables de strictement cloisonner les fonctions liées au paiement et de sécuriser la saisie du PIN, ce qui correspond aux terminaux de paiement classiques actuellement sur le marché et exclut les téléphones mobiles ;

- aux mobiles dédiés à la fonction paiement et livrés avec une application intégrée par le constructeur. La sécurité de ces environnements est donc par définition renforcée.

Actuellement, aucun *smartphone* disponible en France ne semble donc pouvoir prétendre à une certification PCI. L'utilisation de tels appareils afin de réaliser des encaissements nécessiterait, pour l'ensemble des acteurs concernés, de réévaluer le niveau des exigences sécuritaires applicables à chaque situation de paiement, dans le cadre d'une analyse de risques adaptée.

Entre le mobile et les serveurs de l'acquéreur

La problématique se posant de la même manière quel que soit le terminal fonctionnant en mobilité, la sécurité des communications entre le terminal mobile, les concentrateurs monétiques et les serveurs d'acquisition est un sujet sur lequel l'Observatoire a déjà été amené à formuler des recommandations lors de ses rapports précédents[23]. Ces recommandations demeurent d'actualité dans le cadre de l'utilisation d'un mobile comme terminal d'acceptation.

L'utilisation des réseaux ouverts basés sur le protocole Internet IP faisant intervenir de multiples opérateurs interconnectés constitue en particulier un risque de compromission des données. Pour garantir leur confidentialité et intégrité, une sécurisation de bout en bout des communications doit être mise en œuvre à l'instar de ce qui est proposé sur des réseaux privatifs de type réseau privé virtuel (VPN[24]). Cette sécurisation sur réseau ouvert accessible *via* un téléphone mobile s'effectue généralement par le protocole SSLv3[25]. Seule la mise en œuvre de ces dispositions permet de se prémunir contre le risque de modification et d'interception des données de la transaction à des fins de réutilisation frauduleuse.

23 Rapport 2008 (sécurité des réseaux d'automates de paiement) et 2009 (sécurité des terminaux de paiement légers)
24 *Virtual private network*, réseaux caractérisés par un chiffrement des données de bout en bout
25 "*Secure socket layer*" version 3. Son successeur TLS ("*Transport layer security*") versions 1 et supérieures est bien entendu également approprié.

1|3 Conclusion

Le marché des terminaux de paiement connaît de nombreuses évolutions depuis quelques mois, avec l'apparition d'offres basées sur l'utilisation d'appareils mobiles évolués, notamment les *smartphones*. Les solutions reposent sur l'utilisation de sites sécurisés ou d'applications téléchargées sur le téléphone mobile, auxquels sont parfois adjoints des lecteurs de cartes à piste ou à puce, voire des stations d'accueil.

Les *smartphones* étant, par essence, multi-applicatifs, multi-tâches et dépourvus d'éléments de sécurité, ils apparaissent de prime abord peu adaptés aux requis habituellement exigés sur les terminaux de paiement traditionnels, dédiés à cette fonction.

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

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

2| Portefeuille électronique et paiement par carte

Les paiements par carte, initialement conçus pour répondre aux besoins des différents intervenants dans le cadre de transactions de proximité, ont évolué avec le développement de la vente à distance en général et du commerce sur Internet en particulier au cours des dernières années. Cette évolution soulève de nouvelles problématiques liées aux cinématiques d'utilisation, notamment du fait :

- de son ergonomie peu ou mal adaptée au canal Internet, le porteur devant saisir manuellement les seize chiffres de sa carte, ainsi que la date de validité et le cryptogramme visuel ;

- d'une possible réticence des porteurs à communiquer leurs données de carte en raison des risques liés au détournement et à l'utilisation frauduleuse de ces données.

Dans ce contexte, des solutions de paiement qualifiées d'alternatives sont apparues afin de pallier ces problématiques. Les solutions de paiement alternatives traitées dans cette étude revêtent la forme d'un portefeuille électronique, pouvant se définir comme une solution permettant à un utilisateur de confier à un tiers, jugé de confiance, des données de paiement et des données personnelles, stockées en vue d'effectuer ultérieurement notamment des ordres de paiement.

Ces solutions permettent alors de réaliser une opération de paiement par la saisie d'identifiants, comme par exemple le numéro de téléphone portable ou le courriel de l'utilisateur, sans que ce dernier ait à ressaisir des informations sensibles (données de compte ou de carte) à chaque transaction.

Conformément au mandat de l'Observatoire, cette étude porte sur les portefeuilles électroniques permettant l'initiation d'ordres de paiement par carte, même si d'autres moyens de paiement peuvent y être intégrés. Après en avoir rappelé les caractéristiques, l'étude analyse les aspects sécuritaires de ces solutions de paiement alternatives, notamment la protection des données de la carte et l'authentification des utilisateurs, ainsi que leurs impacts sur les acteurs de la chaîne de paiement. Elle n'a toutefois pas pour objectif de décrire le cadre juridique applicable aux portefeuilles électroniques, ni l'étendue des responsabilités de chacun des acteurs.

2|1 Les portefeuilles électroniques et les risques auxquels ils sont soumis

2|1|1 Les solutions, objet de la présente étude

Les solutions considérées dans cette analyse sont les portefeuilles électroniques qui peuvent être proposés par :

- des acteurs spécialisés dans les services de paiement sur Internet (par exemple Paypal, FiaNet avec l'offre Kwixo) ;
- des acteurs traditionnels (par exemple Crédit Mutuel avec l'offre Pay2You) ;
- des opérateurs téléphoniques (avec l'offre Buyster) ;
- des systèmes de paiement par carte tels Cartes Bancaires, Visa ou MasterCard.

Ces portefeuilles électroniques sont généralement utilisables auprès d'un large réseau d'acceptation. Ils peuvent toutefois être proposés et utilisables auprès d'un unique commerçant, par exemple lorsque le portefeuille électronique a pour vocation d'enregistrer les numéros de carte auprès de ce dernier afin que ses clients n'aient plus à les ressaisir par la suite [26] lors de futurs achats (exemple Fnac, Amazon).

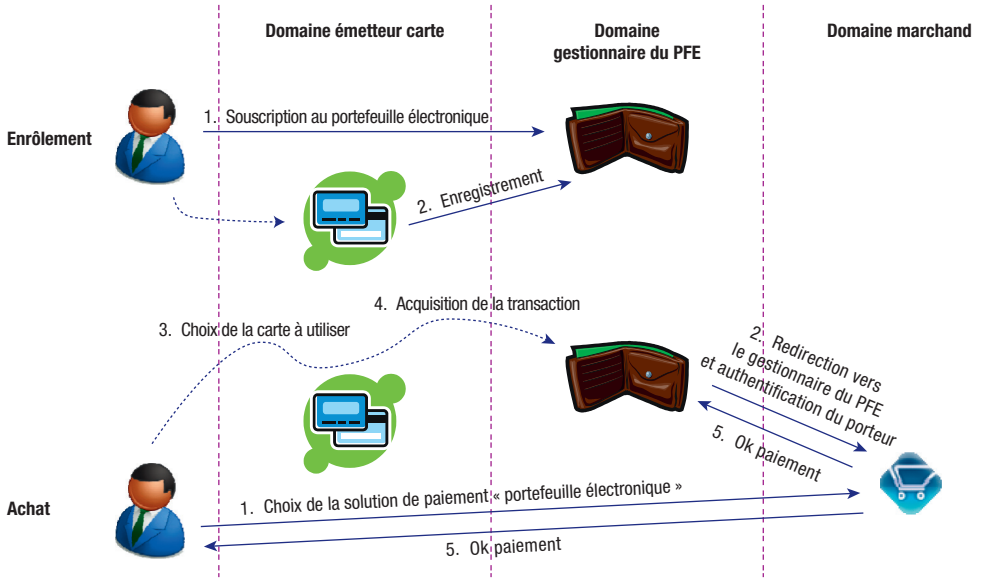
2|1|2 Les cinématiques d'utilisation

L'utilisation d'un portefeuille électronique nécessite une inscription préalable de l'utilisateur au service, celle-ci se faisant le plus souvent par Internet. Il est alors invité à saisir :

- ses données personnelles : adresse, numéro de téléphone, courriel, etc. ;
- ses données de carte : numéro et validité d'une ou plusieurs cartes de paiement [27].

Encadré 2

Cinématique d'utilisation du portefeuille électronique (PFE)



26 Service généralement qualifié de « paiement en un clic »
27 Ou le RIB de l'utilisateur si les services sont étendus au virement/prélèvement, ces deux derniers moyens de paiement ne sont pas traités ici.

Une fois ces données enregistrées, l'utilisateur se voit attribuer des identifiants d'accès qui sont constitués par un code utilisateur [28] (généralement son numéro de téléphone ou courriel) et un mot de passe. Ces identifiants seront par la suite utilisés pour réaliser des opérations de paiement au bénéfice des marchands acceptant la solution de paiement considérée.

Le portefeuille électronique peut permettre d'effectuer des transferts de personne à personne. Ces opérations étant initiées de la même manière que les paiements réalisés auprès des marchands, les cinématiques et mesures de sécurité à mettre en œuvre sont similaires.

Le portefeuille électronique peut enfin permettre l'alimentation d'un compte de monnaie électronique [29]. Cette possibilité permet au prestataire de services de paiement de maintenir dans ses livres les flux liés aux opérations de paiement de ses utilisateurs. Les gestionnaires de tels comptes doivent alors généralement disposer d'un statut d'établissement de crédit ou d'établissement de monnaie électronique.

2|1|3 Les risques pesant sur les solutions de paiement alternatives

Ces solutions sont exposées à différents risques, liés à la conservation de données sensibles (données de compte ou de carte) et à la réutilisation de ces données à l'insu de leur titulaire légitime.

Compromission des données de carte suite à une attaque des serveurs du portefeuille électronique

Les fournisseurs de solutions de portefeuille électronique doivent par nature stocker des données enregistrées par les utilisateurs. Ces données comportent des informations d'identité ainsi que de paiement, notamment les numéros de cartes de paiement des utilisateurs. La concentration de ces informations sensibles représente une cible pour les réseaux de fraudeurs cherchant à obtenir de grandes quantités de données. Par le passé, de tels fournisseurs [30] ont été victimes de vols de données.

Enregistrement de données de carte fraudées dans un portefeuille électronique

Si le niveau de sécurité à l'enrôlement n'est pas suffisamment élevé, des personnes malveillantes pourront ouvrir en toute légitimité des portefeuilles électroniques afin d'y enregistrer des cartes dont les données ont été préalablement compromises.

Utilisation frauduleuse du portefeuille électronique

L'usurpation des identifiants d'accès à un portefeuille électronique permet d'accéder aux moyens de paiement enregistrés dans celui-ci. Le niveau de protection du portefeuille électronique doit par conséquent être suffisamment élevé pour se prémunir des tentatives de fraude visant à l'utiliser à l'insu de son titulaire légitime.

2|2 Les enjeux sécuritaires des solutions de paiement alternatives et leurs impacts sur les acteurs

2|2|1 Les mesures sécuritaires

Les risques exposés ci-dessus justifient la mise en œuvre de mesures sécuritaires par les fournisseurs de portefeuilles électroniques. Ces mesures concernent tant la protection des données sensibles que la vérification de l'identité du porteur, lors de l'enregistrement de sa carte de paiement ou de l'utilisation de son portefeuille électronique.

Liées à la protection des données sensibles

L'enregistrement et la conservation des données liées à la carte de paiement sont notamment soumises à des règles sécuritaires édictées par l'organisme PCI-SSC [31]. Ces règles sont définies au sein des mesures dites « PCI-DSS » [32], qui visent à protéger

28 Ou « *login* »
29 Ce compte est généralement qualifié de « porte-monnaie électronique ».
30 On citera par exemple Sony, lequel se serait vu dérober plus de deux millions de données de carte en avril 2011 sur son Playstation Network.
31 Ce consortium (*Payment Card Industry Security Standard Council*) regroupe ses systèmes fondateurs (American Express, Discover financial Services, JCB International, MasterCard Worldwide et Visa Inc. International).
32 PCI - *Data Security Standard*, voir chapitre 1, rapport 2009

les données transmises au travers des systèmes d'information de la chaîne d'acquisition ou stockées dans ces systèmes. Ces mesures devraient donc être respectées dès lors qu'un prestataire conserve des données de carte sur ses serveurs. La conformité aux règles PCI est évaluée au travers d'un processus de certification obtenu auprès d'organismes agréés par PCI-SSC.

En France, conformément à la loi n° 78-17 dite loi « informatique et libertés », ces traitements doivent en outre faire l'objet d'une déclaration préalable auprès de la CNIL [33] qui vérifiera notamment les conditions d'information des personnes et les conséquences liées à la mise en œuvre de ces traitements.

Enfin, selon l'acteur impliqué dans la solution de paiement mise en place, la répartition des responsabilités de chacun est à considérer attentivement. Elles peuvent en effet relever du commerçant, de son prestataire technique ou de l'acquéreur, les relations entre ceux-ci devant être formalisées de façon à clarifier leurs responsabilités respectives.

Liées à l'enregistrement de la carte

Les fraudeurs ciblent leurs attaques sur les moyens de paiement dont le niveau de protection est le plus faible. La fraude peut notamment se reporter vers les sites acceptant les paiements par portefeuille électronique, dans le cas où ce dernier permettrait d'enregistrer des données de cartes compromises par des personnes malveillantes, au sein de portefeuilles ouverts en toute légitimité.

Il convient dès lors de s'assurer que le porteur de la carte est bien celui qu'il prétend être au moment de l'enregistrement des données de carte dans le portefeuille électronique et que le détenteur du portefeuille est bien le titulaire légitime des moyens de paiement qu'il entend enregistrer dans ce dernier. Ceci doit conduire les gestionnaires de portefeuilles électroniques à mettre en œuvre diverses solutions afin de garantir leur intégrité au moment de l'enregistrement et de lutter contre le risque identifié d'utilisation frauduleuse du portefeuille électronique (cf. *supra*).

L'Observatoire recommande ainsi le recours par le gestionnaire de portefeuille électronique à l'authentification renforcée du porteur par l'émetteur de la carte, au moyen de solutions dites « non rejouables » [34], lesquelles s'appuient sur l'utilisation de protocoles de sécurité, tels « 3D-Secure » ou toute solution équivalente.

On notera en outre que les gestionnaires de portefeuille électronique ont parfois mis en place des mesures de sécurité complémentaires permettant de limiter les risques d'utilisation frauduleuse du portefeuille au cours des premiers mois d'activité :

- certains invitent leurs clients à réaliser une transaction par carte pour un faible montant, choisi de façon aléatoire, montant qui devra être ensuite confirmé par le porteur afin de s'assurer que ce dernier a bien accès aux relevés des transactions pour la carte considérée. Cette solution présente toutefois l'inconvénient pour le porteur de devoir initier une transaction sans en connaître le montant ;

- d'autres observent le fonctionnement du portefeuille électronique sur une période prédéfinie avant de lever certains seuils définis à l'ouverture.

Liées à l'utilisation frauduleuse du portefeuille électronique

En cas d'usurpation des ses identifiants (cf. *supra*), le détenteur doit être protégé contre une utilisation frauduleuse des moyens de paiement enregistrés dans son portefeuille électronique.

33 Commission nationale de l'informatique et des libertés. voir *http://www.cnil.fr/*
34 Cf. rapport 2010, chapitre 3, p. 39

L'Observatoire recommande la mise en œuvre par le gestionnaire du portefeuille électronique :

• d'une analyse de risques visant à déterminer si l'opération de paiement est réalisée dans des conditions inhabituelles pouvant entraîner le blocage de l'opération. Par construction, cette analyse est à associer à l'usage des portefeuilles électroniques sous sa responsabilité [35] ;

• du déclenchement d'une authentification non rejouable, systématiquement ou en fonction de l'analyse de risque précédente. Idéalement, cette authentification est effectuée par recours à l'émetteur de la carte présente dans le portefeuille électronique, ou *a minima* grâce à un moyen d'authentification (numéro de téléphone portable par exemple) dont le gestionnaire de portefeuille électronique garantit la sécurité [36].

2|2|2 Impacts sur les acteurs de la chaîne du paiement

En France [37], les règles habituelles de gestion de moyen de paiement définies dans le *Code monétaire et financier* s'appliquent aux opérations de paiement effectuées grâce aux solutions de portefeuille électronique, notamment en termes :

• de consentement à l'exécution d'une opération de paiement ;

• d'irrévocabilité des ordres de paiement ;

• de délai d'exécution des opérations de paiement en dates de valeur ;

• de remboursement d'une opération mal exécutée ou non autorisée.

Le détenteur d'un portefeuille électronique peut y enregistrer des cartes de paiement émises par un établissement différent du gestionnaire de ce portefeuille. En cas d'opération frauduleuse réalisée dans ce cadre, le porteur se retrouve lié à des obligations contractuelles :

• liées au contrat porteur conclu avec l'établissement émetteur de la carte, auquel il doit ainsi déclarer toute utilisation non autorisée de son moyen de paiement ;

• liées aux conditions générales d'utilisation fournies par le gestionnaire de portefeuille électronique, précisant également de lui signaler l'utilisation frauduleuse de son moyen de paiement.

La responsabilité du gestionnaire de portefeuille électronique peut être engagée en cas d'opération frauduleuse dès lors que le point de compromission est situé dans son périmètre. Par ailleurs, il conviendra d'établir clairement la démarche à suivre par l'utilisateur pour contester une opération, auprès de l'établissement émetteur de sa carte de paiement et/ou du gestionnaire de portefeuille électronique.

L'Observatoire recommande en outre aux gestionnaires de portefeuilles électroniques de veiller à la conformité et à la transparence contractuelle vis-à-vis des utilisateurs quant à l'enregistrement et à l'utilisation de moyens de paiement au sein de leur solution.

Enfin, l'Observatoire recommande aux gestionnaires de portefeuilles électroniques et aux émetteurs de mettre en place les dispositifs techniques et organisationnels permettant d'assurer la traçabilité des opérations réalisées à partir d'un portefeuille électronique. Il conviendrait notamment de permettre au porteur de pouvoir identifier le bénéficiaire de ces opérations.

35 Exemple : montant anormal, profil de risque élevé, compte non vérifié, etc.
36 On pensera notamment à la protection de l'enregistrement et de tout changement ou mise à jour de ce moyen d'authentification.
37 Pour les opérations extracommunautaires, se reporter au rapport 2009, annexe A, p. 59

2|3 Conclusion

L'émergence des portefeuilles électroniques contribue à la diversification des offres de paiement en apportant aux utilisateurs des moyens adaptés à leurs usages. La multiplication de ces offres ne doit cependant pas se faire au détriment de la sécurité des moyens de paiement, au risque de compromettre d'une part la confiance dans les instruments de paiement actuels, et d'autre part de voir la fraude se reporter vers des solutions qui seraient moins sécurisées.

L'Observatoire recommande ainsi la mise en œuvre :

- de la protection des données sensibles (dont celles liées aux cartes de paiement) par l'ensemble des acteurs impliqués ;

- du recours par le gestionnaire du portefeuille électronique à un mécanisme d'authentification non rejouable du porteur par l'émetteur au moment de l'enregistrement de la carte dans le portefeuille ;

- d'analyses de risque par le gestionnaire de portefeuilles électroniques conduisant au déclenchement d'une authentification non rejouable pour les paiements considérés comme risqués.

Enfin, le développement des portefeuilles électroniques doit s'effectuer dans des conditions de transparence en matière contractuelle. La mise à disposition de moyens de paiement, particulièrement dans un contexte de convergence des usages entre le paiement à distance et de proximité, appelle en effet à la mise en place de règles claires quant à la gestion des instruments et opérations de paiement, ainsi qu'à la définition et au partage des responsabilités entre les utilisateurs, les marchands et les gestionnaires de telles solutions.

3| État d'avancement de la migration EMV

La mise en œuvre en Europe des spécifications EMV (« Europay, MasterCard, Visa ») pour carte à puce représente un enjeu majeur dans la lutte contre la fraude transfrontalière. Elle concerne non seulement les cartes elles-mêmes, mais aussi leurs dispositifs d'acceptation (terminaux, automates de paiement et de retrait) qu'il convient de migrer aux nouvelles spécifications pour pouvoir bénéficier d'un niveau de protection égal partout en Europe. Comme il le fait depuis sept ans de façon à mesurer l'avancement de la migration EMV, l'Observatoire a de nouveau recueilli auprès du Groupement des Cartes Bancaires « CB » et de l'EPC des statistiques relatives à cette migration en France et en Europe. Ces chiffres montrent que la migration est quasiment achevée partout en Europe, mais en léger retard sur l'engagement des banques européennes au sein de l'EPC d'avoir achevé cette migration à fin décembre 2010.

3|1 État de la migration en France

En France, la migration aux standards EMV est quasiment terminée. Fin mars 2012, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes « CB », 99,5 % des terminaux et automates et 100 % des distributeurs automatiques de billets étaient conformes aux spécifications EMV. Le 0,5 % restant de terminaux et automates peu utilisés, sera migré lors de leur remplacement normal.

3|2 État de la migration en Europe

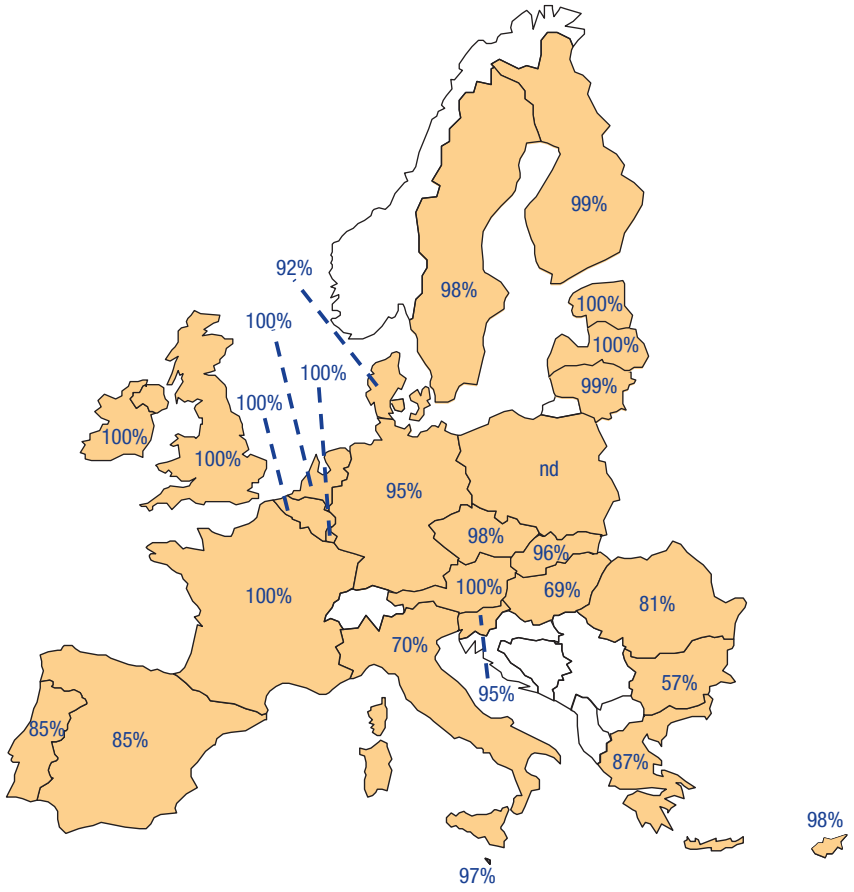
Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2012, 87,8 % des cartes interbancaires circulant au sein des 27 États membres de l'Union européenne sont désormais conformes à la spécification EMV. Le déploiement continue de progresser (+ 2,2 points par rapport à mars 2011), après une forte augmentation l'année précédente (+15,8 points) marquée par un rattrapage de certains pays moins avancés. Pays par pays, la situation reste contrastée (cf. encadré 3). Alors que la mise en conformité aux règles d'interopérabilité de SEPA a commencé depuis début 2008, certains pays sont toujours notablement en retrait par rapport aux

autres. On note néanmoins que les cartes conformes au standard sont désormais majoritaires au sein de tous les pays de l'Union [38].

Le déploiement des cartes EMV reste toujours sensiblement plus élevé dans les pays du Nord de l'Europe.

Encadré 3

Déploiement des cartes EMV en Europe



Source : European Payments Council – mars 2012

38 Excepté la Pologne, pour laquelle l'EPC ne dispose pas de données récentes.

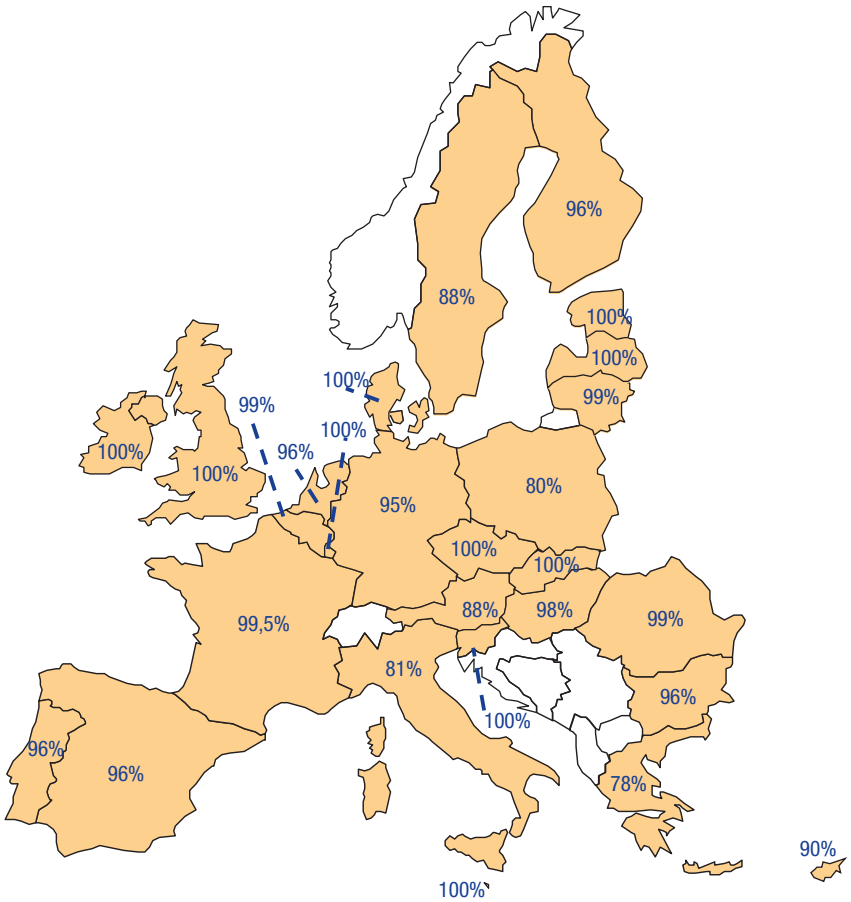
Concernant l'acquisition, la migration vers EMV progresse plus lentement que les années précédentes, tout en étant désormais à un niveau élevé : à fin mars 2012, 94,5 % des terminaux de paiement (cf. encadré 4) et 96,7 % des distributeurs automatiques de billets (cf. encadré 5) sont conformes à EMV (soit une progression de 2,5 points pour les terminaux de paiement et de 0,1 point pour les distributeurs automatiques de billets par rapport à mars 2011). On ne constate désormais plus de différences notables entre les pays du Sud de l'Europe, où la migration avait été la plus rapide, et les pays du Nord.

Les pays en fin de migration peuvent toujours rencontrer des difficultés à remplacer une dernière frange de systèmes d'acceptation, qui sont peu ou très ponctuellement utilisés.

La migration des distributeurs de billets est pratiquement achevée dans la plupart des pays [39].

Encadré 4

Déploiement des terminaux et automates EMV en Europe

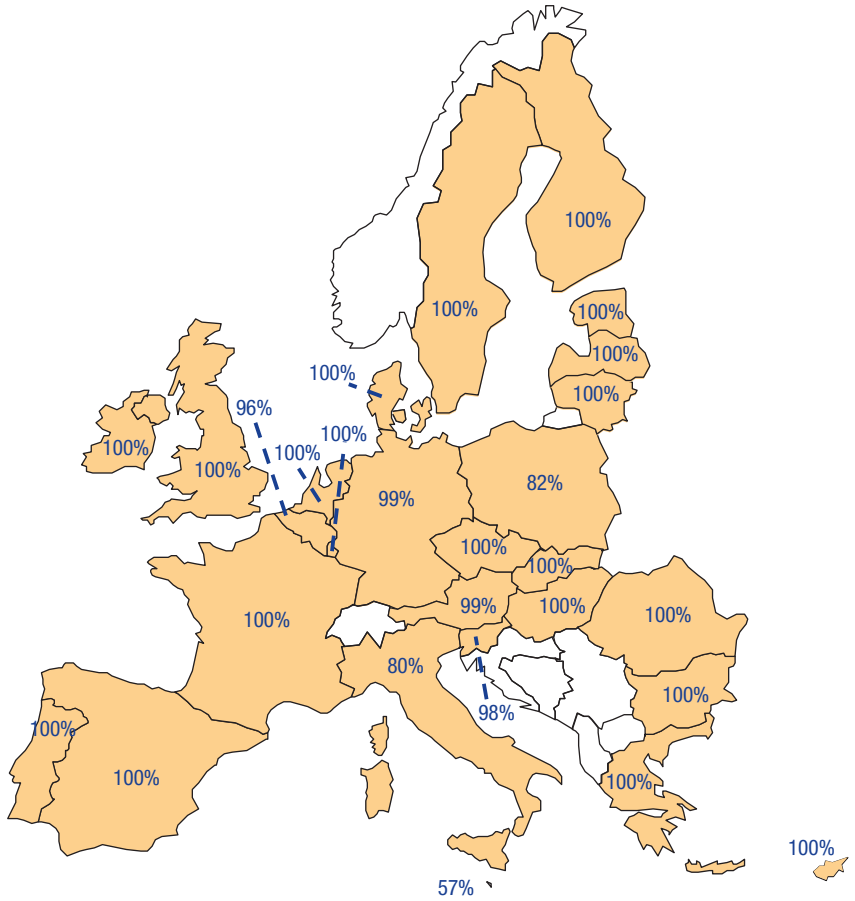


Source : European Payments Council – mars 2012

39 À noter : l'EPC ne dispose pas de données actualisées pour l'Italie. Les chiffres communiqués sont donc sujets à caution.

Encadré 5

Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2012

La coopération internationale en matière de lutte contre la fraude

Au titre de ses missions, l'Observatoire est notamment chargé d'établir des statistiques en matière de fraude et d'émettre des recommandations aux acteurs de la chaîne de paiement afin d'endiguer ce phénomène. Par la nature européenne, voire mondiale, du marché de la carte de paiement, la portée de ces recommandations dépasse aujourd'hui le seul cadre national et l'action de l'Observatoire s'inscrit dans un contexte d'harmonisation des mesures de sécurité sur la scène internationale.

À la hauteur des enjeux financiers et de la sophistication des techniques employées, la lutte contre la fraude dans le domaine des cartes de paiement est aujourd'hui une priorité, en France comme à l'international. Dans le cadre de son rapport 2011, l'Observatoire a ainsi souhaité réaliser un état des lieux des acteurs prenant part à la lutte contre la fraude sur le territoire et présenter les circuits de coopération existants à l'international.

Cette étude a été conduite sur la base d'informations collectées auprès de représentants des administrations concernées, d'organismes spécialisés nationaux, européens et internationaux et du secteur bancaire.

1| La lutte contre la fraude : des objectifs multiples mais complémentaires

Le panorama dressé par l'Observatoire révèle un nombre important d'intervenants impliqués dans la lutte contre la fraude, dont les approches sont différentes en fonction de leur positionnement dans la chaîne de paiement, mais qui permettent de couvrir l'ensemble des problématiques que sont la lutte préventive contre la fraude, l'expertise technique des composants, le démantèlement des réseaux en cas de fraude avérée et le maintien de la confiance dans le moyen de paiement par carte pour les autorités de supervision et de surveillance.

1|1 L'objectif des établissements de crédit : limiter l'impact financier de la fraude

Les émetteurs et acquéreurs de cartes de paiement subissent généralement des coûts financiers lors de fraudes et ont à ce titre intégré ce risque dans leurs politiques de sécurité.

Deux sujets sont jugés prioritaires pour eux à ce jour et bénéficient d'une attention particulière : le risque lié à l'utilisation de cartes altérées ou contrefaites et celui d'usurpation et de réutilisation, notamment sur Internet, de numéros de cartes usurpés.

Émetteurs et acquéreurs prennent donc une part active dans le développement d'innovations technologiques contribuant à lutter contre ces fraudes. Ainsi, la migration aux standards EMV [1] dans le premier cas et le déploiement de l'authentification non rejouable [2] dans le second, sont des projets d'envergure s'inscrivant dans cette démarche.

En complément de ces évolutions, ces acteurs ont également développé des outils de *scoring* des transactions, alimentés par les flux quotidiens d'autorisation ou de collecte des opérations de paiement par carte afin de surveiller l'évolution des tendances en matière de fraude. Constamment améliorés et adaptés, ces outils leur permettent d'être réactifs en cas d'anomalie. Ils reposent toutefois sur l'historique des transactions dont dispose l'établissement considéré, lequel ne peut avoir qu'une vue parcellaire du marché de la carte, en France comme à l'étranger. Dans ce contexte, le rôle des systèmes de paiement par carte, aussi bien nationaux qu'internationaux, est primordial puisqu'ils permettent d'avoir une vision plus large sur la fraude.

Enfin, ce dispositif est complété par la fourniture de services de surveillance et de réponse en cas

1 La migration aux standards EMV a fait l'objet d'une étude dans le rapport 2010, chapitre 1, p. 11.
2 Cf. rapport 2010, chapitre 3, p. 33 et rapport 2011, chapitre 1, p. 13

d'incident, assurés par des organismes labellisés dénommés CSIRT [3] et CERT [4]. Elles apportent une expertise technique pointue, notamment aux établissements bancaires, sur les menaces pesant sur les réseaux (Internet), ou encore sur les logiciels utilisés dans les systèmes d'information des entreprises. Certains établissements bancaires disposent également en interne de telles compétences.

1|2 Le besoin d'assurer la sécurité technique des composants

La sécurité des cartes de paiement repose sur le haut niveau de technicité de leurs composants [5]. Ces derniers doivent donc faire l'objet d'expertises régulières afin de s'assurer qu'ils sont maintenus à l'état de l'art et aptes à résister aux éventuelles attaques de plus en plus sophistiquées perpétrées par les fraudeurs.

En France, il existe pour ce faire des schémas indépendants de certification et d'évaluation sécuritaires des cartes de paiement et terminaux d'acceptation utilisés par les systèmes de paiement par carte. Ces derniers les intègrent dans leur processus d'agrément des composants autorisés à opérer sur leur réseau. On distingue ainsi, pour le système de paiement Cartes Bancaires (ci-après « CB »), un schéma de certification sécuritaire pour les cartes, sous l'égide de l'ANSSI [6], et un second schéma dédié aux terminaux, aux mains de l'entité *PayCert*.

Ces deux schémas s'appuient en France sur un nombre restreint de laboratoires d'expertise agréés, dont l'ANSSI et *PayCert* s'assurent régulièrement du haut niveau de compétence. Ainsi, pour les cartes, les composants sont testés au sein de Centres d'Évaluation de la Sécurité des Technologies de l'Information (CESTI), au nombre de trois sur le territoire : Leti, Serma, et Thales. Le laboratoire Elitt a quant à lui développé une compétence dans l'évaluation des terminaux d'acceptation. Une fois certifiés, les produits sont régulièrement évalués pendant leur durée de vie, afin de s'assurer de leur résistance aux nouvelles attaques.

1|3 Enquêter et démanteler les réseaux

La carte de paiement étant un moyen de paiement largement accepté en France, son usage illicite dans des cas de blanchiment d'argent, de financement du terrorisme et plus généralement les fraudes qui peuvent lui être attachées demandent à la fois la mise en place de dispositifs d'alerte au niveau national, ainsi que la présence sur le territoire de structures organisées aux compétences techniques fortes.

Rattaché au ministère de l'Economie, des Finances et du Commerce extérieur, Tracfin est ainsi chargé de lutter contre les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme. Il reçoit à cette fin des informations de la part des établissements financiers lui signalant des opérations atypiques, appelées déclarations de soupçons. Tracfin peut alors transmettre ces informations au parquet, si ces soupçons sont confirmés par ses propres investigations.

Les forces de l'ordre se sont quant à elles structurées en France à différents niveaux, conduisant la police et la gendarmerie nationale à mettre en place un certain nombre d'organismes spécialisés :

• au sein de la direction centrale de la police judiciaire, la sous-direction de la lutte contre la criminalité organisée et la délinquance financière (SDLCODF) est chargée du recueil du renseignement, de l'analyse stratégique et des relations avec les administrations concernant, entre autre, la délinquance spécialisée. À ce titre, cette sous-direction est constituée d'offices centraux parmi lesquels certains ont un rôle actif dans la lutte contre la fraude aux moyens de paiement,

3 *Computer Security Incident Response Team*
4 *Computer Emergency Response Team*
5 Il s'agit des circuits intégrés et des applications de paiement contenus dans les cartes. Pour les terminaux d'acceptation, ces composants intègrent notamment les systèmes d'exploitation.
6 Agence nationale de la sécurité des systèmes d'information. L'ANSSI assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Une de ses missions est d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. Cette agence est compétente pour apporter son expertise et son assistance technique aux administrations et aux entreprises critiques en raison des produits et services qu'elles fournissent. Elle peut à ce titre être sollicitée en cas d'apparition de nouvelles typologies de fraude.

comme l'ORCGDF [7] et l'OCLCTIC [8] sous lequel est placée la brigade centrale pour la répression des contrefaçons des cartes de paiement [9] ;

• au sein de la gendarmerie nationale, le service technique de recherches judiciaires et de documentation est constitué notamment de la division financière et de la division de lutte contre la cybercriminalité en charge de centraliser et d'exploiter les informations judiciaires relatives aux crimes et délits. Ces deux divisions sont fortement impliquées dans la lutte contre la fraude en ce qui concerne les cartes de paiement ;

• ces services spécialisés sont complétés par des services d'expertises techniques : le service central de l'informatique et des traces technologiques au sein de la police nationale et la division criminalistique ingénierie et numérique au sein de l'institut de recherche criminelle de la gendarmerie nationale, qui réalisent des investigations techniques de haut niveau.

Cette organisation est relayée sur le terrain, tant au niveau de la police que de la gendarmerie, par des enquêteurs (connus sous les termes NTECH [10] et ICC [11]) spécifiquement formés aux infractions liées aux nouvelles technologies.

1|4 L'objectif des autorités de supervision et de surveillance : maintenir la confiance dans l'instrument de paiement et les prestataires agréés

En France, l'exercice de la mission de surveillance des moyens de paiement scripturaux revient à la Banque de France en vertu des dispositions du *Code monétaire et financier* (article L. 141-4 et suivants).

Le premier objectif de la Banque de France est ainsi de maintenir la confiance dans l'utilisation des instruments de paiement, dont la carte, en contribuant à la diffusion de bonnes pratiques en matière de sécurité, adressées à l'ensemble des acteurs concernés et de façon homogène sur le territoire.

Pour cela, la Banque de France procède à des analyses de risque pour chaque instrument et établit des référentiels de sécurité. Au travers de contrôles menés sur pièces ou sur place, elle s'assure de la conformité des acteurs et de leurs prestataires techniques avec ces référentiels. Le cas échéant, elle peut recommander aux assujettis la mise en œuvre de mesures de sécurité destinées à prévenir les fraudes. En ce qui concerne le domaine de la carte de paiement, la Banque de France a ainsi évalué l'ensemble des systèmes de paiement par carte nationaux actifs sur son territoire en 2008-2009. Elle a également fait plusieurs recommandations d'importance aux acteurs de la chaîne de paiement, dont le déploiement de l'authentification non rejouable pour sécuriser les sites de banques en ligne et les paiements par carte en ligne en 2008 et le renforcement de la sécurité des cartes à puce EMV du système Cartes Bancaires en 2006 (passage à la technologie DDA – « *Dynamic Data Authentication* » – afin de lutter plus efficacement contre la contrefaçon de cartes de paiement).

Par ailleurs les prestataires agréés sont soumis au contrôle de l'Autorité de contrôle prudentiel, notamment pour ce qui concerne le risque opérationnel généré par la fourniture et la gestion des instruments de paiement (articles L612-1 et 612-2 du *Code monétaire et financier*).

2| Un besoin de coopération entre ces acteurs

Les établissements bancaires (ou plus globalement tout prestataire de service de paiement), les forces de l'ordre, les organismes de certification et laboratoires d'expertise technique ou encore les autorités bancaires sont ainsi amenés à prendre une part active dans la lutte contre la fraude au niveau national, européen et international. Afin que cette lutte soit la plus efficace possible, les acteurs ont éprouvé le besoin de mettre en place des structures de coopération.

7 Office central pour la répression de la grande délinquance financière
8 Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
9 BCRCCP
10 Enquêteur en technologies numériques
11 Investigateur en cybercriminalité

2|1 Les acteurs bancaires coopèrent à de nombreux niveaux

Les établissements bancaires sont regroupés en France au sein de la Fédération bancaire française (FBF). Cette dernière représente la communauté bancaire française au sein de la Fédération bancaire européenne (FBE), elle-même défendant les positions européennes lors des réunions de l'International Banking Federation (IbFed). Cette organisation pyramidale autorise un échange d'informations entre établissements financiers au niveau international et leur permet de définir des positions communes, également en matière de sécurité.

La coopération entre établissements bancaires au niveau européen s'effectue, quant à elle, principalement grâce à la mise en œuvre de SEPA [12]. Dans ce cadre, les établissements bancaires ont ainsi créé en 2003 le Conseil européen des paiements (« *European Payment Council* » ou EPC), structure d'échange et de coordination de la profession. L'EPC s'est organisé en groupes de travail dédiés à chaque type d'instrument de paiement traitant notamment des problématiques de sécurité et de lutte contre la fraude, le cas échéant de manière transversale. En fonction des thématiques, des organisations externes au secteur bancaire, comme Europol, peuvent être invitées afin d'enrichir les échanges.

Au niveau international, les établissements bancaires peuvent être amenés à échanger sur la fraude dans le cadre de travaux de normalisation, au sein de l'ISO notamment. Ce dernier a par exemple créé un comité technique à cet effet [13].

S'agissant plus spécifiquement des opérations par carte, le secteur bancaire s'est organisé dès 1984 en France autour d'un groupement d'intérêt économique, le GIE Cartes Bancaires, autorité de gouvernance du système de paiement par carte « CB » et pôle opérationnel et d'expertise technique du système. La naissance de ce GIE a donc de fait conduit à la naissance de l'interbancarité en France autour de la carte de paiement.

L'ensemble des transactions de paiement par carte était jusqu'à présent réalisé par l'intermédiaire d'un unique réseau d'autorisation interbancaire, d'abord géré par le GIE Cartes Bancaires puis filialisé en 2009 [14], conférant à ce dernier une position centrale dans la lutte opérationnelle contre la fraude.

Le GIE Cartes Bancaires a ainsi mis en place des outils permettant l'identification de transactions potentiellement frauduleuses et la détection de points de compromission. Il collabore, par sa position stratégique, étroitement avec les forces de l'ordre afin d'apporter des éléments de preuve notamment dans les enquêtes. Les réseaux internationaux Visa, MasterCard ou encore Amex, ont développé des outils similaires qui bénéficient à leurs membres.

Quelle que soit l'organisation retenue par les acteurs de marché, il est essentiel que la coopération en matière de lutte contre la fraude soit organisée de manière efficace, notamment en assurant le partage d'informations entre acteurs. Cela devra être notamment le cas lors de la disparition annoncée des passerelles techniques entre le système « CB » et les systèmes internationaux Visa et MasterCard, pour les transactions transfrontalières initiées en France.

2|2 La coopération technique : une marge de progrès à l'international

2|2|1 Un nombre limité d'organismes de coopération technique

Au sein de l'Europe, la coopération technique est portée essentiellement par les agences gouvernementales responsables de la sécurité des systèmes d'information. En effet, les structures existantes dans ce domaine au niveau européen ont des responsabilités limitées :

• l'ENISA [15] assiste les États membres dans la mise en place de structures et de cadres adaptés pour la prise en compte de la sécurité des systèmes d'information et de la cybersécurité. L'ENISA

12 L'objectif de SEPA est de créer un marché des paiements intégré européen et ainsi d'harmoniser les paiements de détail en euros afin qu'ils soient effectués dans les mêmes conditions de sécurité, d'efficacité et de coût.

13 TC 247 – « Mesures de prévention et de contrôle de la fraude », chargé de la normalisation dans le domaine de la détection, de la prévention et du contrôle de la fraude liée à l'identité, de la fraude financière, de la fraude relative aux produits et d'autres formes de fraude sociale et économique

14 Il s'agit du réseau e-rsb, désormais géré par la filiale Ser2S – Société d'Exploitation de Réseaux et de Services Sécurisés.

15 European Network and Information Security Agency, composée notamment d'experts dans le domaine de l'information et des communications, de représentants de l'industrie et de chercheurs en réseaux et sécurité de l'information

produit notamment des guides techniques pouvant être utilisés comme référentiels ;

• le CERT-EU est le CERT des institutions européennes, actuellement en préfiguration et qui joue un rôle opérationnel au profit de ces seules institutions, dans le domaine de la cybersécurité.

À l'international, des structures ont également été mises en place afin de permettre l'échange d'information entre les acteurs sur des problématiques précises comme les compromissions des automates ou des terminaux de paiement. L'association EAST [16] illustre cette mise en commun de moyens par des acteurs de marché, dans l'objectif de promouvoir et d'harmoniser de bonnes pratiques en matière de lutte contre la fraude sur les distributeurs automatiques de billets.

2|2|2 La certification : illustration d'un réel besoin d'harmonisation sur la scène internationale

La coopération technique s'opère efficacement dans le cadre de la certification [17] des matériels, afin de prévenir tout risque de fraude mais également de faciliter les démarches des fournisseurs de solutions. On peut toutefois noter que des efforts restent à faire, notamment au niveau européen.

Il convient tout d'abord de distinguer deux initiatives au périmètre distinct :

• les schémas de certification nationaux, sous l'égide d'agences gouvernementales telles que l'ANSSI et ses homologues à l'étranger, ont très vite partagé des processus d'évaluation et de certification ouverts ainsi qu'un cadre méthodologique s'appuyant sur une norme ISO internationale [18], plus connue sous le nom de « Critères Communs ». Afin de parvenir à une reconnaissance mutuelle des certifications délivrées, ainsi que des évaluations opérées par les laboratoires accrédités au sein de ces schémas, des accords de reconnaissance ont été mis en œuvre entre les États membres de l'Union européenne sous le nom de SOG-IS (*Senior Official Group – Information Security*), mais également au-delà, sous le nom de CCRA (*Common Criteria Recognition Agreement*).

Dans le domaine des composants carte, ce dispositif est aujourd'hui opérationnel et reconnu par les réseaux Visa et MasterCard.

• les systèmes de paiement par carte internationaux (Visa, MasterCard, Amex notamment) ont par ailleurs rapidement collaboré au sein de structures *ad hoc* dans le domaine de la carte (EMV [19] Co) et également dans celui de la protection des données sensibles liées aux transactions (PCI SSC [20]). Si les certifications EMV sont avant tout fonctionnelles et ne visent pas à tester la robustesse des composants des cartes en termes de sécurité, les standards PCI quant à eux sont dédiés à la chaîne d'acceptation du paiement par carte et s'accompagnent d'une évaluation par un laboratoire compétent puis d'une certification délivrée par l'organisme PCI SSC.

À ce jour, ce sont donc ces derniers qui prévalent en matière de certification des terminaux d'acceptation.

Si ces deux initiatives apparaissent différentes, elles convergent cependant de plus en plus en raison d'évolutions observées ces dernières années :

• certains groupes de travail dans le cadre des Critères Communs abordent la certification des terminaux et associent les acteurs principaux de PCI (Visa, MasterCard, American Express), aux côtés des agences gouvernementales, de la majorité des systèmes de paiement nationaux, dont le Groupement des Cartes Bancaires (CB), et aussi de nombreux fournisseurs et fabricants de solutions.

Les schémas de certification nationaux et PCI SSC bénéficient ainsi d'une expertise partagée en matière d'attaques et de mesures de sécurité concernant les terminaux.

• en raison de la présence de nombreux systèmes de paiement nationaux s'ajoutant aux réseaux

16 *European ATM Security Team*, organisation à but non lucratif, regroupant à l'échelon européen des systèmes de paiement par carte (en France le GIE Cartes Bancaires), des processeurs et établissements bancaires
17 Cf. l'étude dédiée au sujet de la certification en France et en Europe réalisée au sein du rapport 2008 de l'Observatoire, chapitre 4, p.47
18 Il s'agit de la norme ISO 15408 "*Information technology, security techniques, evaluation criteria for IT security*".
19 « *Europay MasterCard Visa* », cf. rapport 2010, chapitre 1, p. 19
20 *Payment Card Industry Security Standard Council*, cf. rapport 2009, chapitre 1, p. 9

internationaux, le besoin de simplifier les démarches hétérogènes de certification des cartes et des terminaux est dorénavant très présent au niveau européen. Si l'EPC s'oriente vers la méthodologie Critères Communs dans le domaine de la carte, les travaux visant à rapprocher les Critères Communs et PCI sont toujours en cours en ce qui concerne la certification des terminaux d'acceptation.

L'EPC rencontre également des difficultés à créer un organe de gouvernance [21] à même d'organiser la reconnaissance mutuelle des certificats, fonctionnels et sécuritaires, délivrés aux fabricants de cartes, de terminaux et potentiellement d'autres composants d'un système de paiement par carte. Ce projet est soutenu depuis son origine par les autorités de régulation bancaires dans l'objectif d'harmoniser le niveau de sécurité des composants à l'échelle européenne.

2|3 Une coopération en matière de répression qui bénéficie de structures bien établies

2|3|1 Des instances de coopération clairement définies au niveau national, européen et international

En France, de nombreux services de police et de gendarmerie sont amenés à enquêter sur des dossiers dans lesquels des cartes de paiement ont été utilisées illégitimement afin de commettre des infractions. On peut distinguer deux niveaux de coopération pour soutenir l'action de ces services sur le terrain :

• en matière de répression, ce sont les offices centraux qui sont en charge de la mise en œuvre de la coopération policière et judiciaire. S'agissant des cartes de paiement, l'OCLCTIC anime et coordonne la mise en œuvre opérationnelle de la lutte contre les auteurs de ces infractions au niveau national. À ce titre, l'OCLCTIC coordonne les services de police et unités de gendarmerie et entretient également des relations avec les autres administrations (Douanes, Impôts, etc.), le secteur bancaire, les associations spécialisées dans la protection des consommateurs, ainsi que les écoles et universités, notamment en matière de recherche. Ces offices sont également les points de contacts pour la coopération internationale. Ils collaborent avec les services spécialisés étrangers et sont les interlocuteurs privilégiés en matière d'échange avec les organismes Europol et Interpol ;

• en matière de partage d'information au niveau national, un service interministériel hébergé au sein de la Direction centrale de la police judiciaire, le SIRASCO [22], effectue des missions de renseignement et d'analyse stratégique sur la criminalité organisée. Ce service coopère avec Tracfin en matière financière, mais également avec l'ensemble des offices centraux potentiellement concernés, dont l'OCLCTIC.

À l'échelle européenne, a été créé en 1995 un organisme de coopération appelé Europol [23], devenu agence européenne en 2010 [24]. Europol dispose de plusieurs atouts pour les États membres :

• son rôle est de contribuer à soutenir les forces de l'ordre en Europe par le biais d'échanges et d'analyses de renseignement en matière de criminalité. Aux côtés des actions de lutte contre le terrorisme et les trafics de tout genre, la lutte contre l'usage frauduleux des cartes de paiement fait partie des sujets abordés par Europol ;

• à ce titre, l'agence a mis en place un fichier visant à collecter toute information sur les cas de fraude liés à la carte, et plus particulièrement en matière de contrefaçon, afin notamment d'identifier d'éventuels réseaux structurés agissant dans plusieurs pays. Ces échanges de données sont facilités par la mise en place d'un système d'information sécurisé dédié, intitulé SIENA, permettant de collecter des informations provenant des États membres. Ces données permettent d'une part de réaliser des analyses opérationnelles visant à mettre en évidence des liens marquants dans les enquêtes transfrontalières et d'autre part d'identifier les priorités en matière de lutte contre la criminalité. Des actions coordonnées entre États sont ainsi plus aisément rendues possibles.

21 Le *Sepa Card Certification Management Body* (SCCMB)
22 Service d'Information, de Renseignement et d'Analyse Stratégique sur la Criminalité Organisée
23 *European Union Law Enforcement Organisation*
24 Par là-même, son mandat et ses moyens s'en sont retrouvés renforcés.

Enfin, à l'international, une organisation policière existe depuis 1923, l'Organisation internationale de police criminelle, plus connue sous le nom d'Interpol. Tout comme Europol, Interpol a une vocation coopérative forte pour ses 188 membres :

• la mission principale d'Interpol est de fournir aux États une plate-forme d'échange et d'analyse du renseignement en matière criminelle et de mettre en évidence des liens entre les actes répertoriés. Les fraudes aux cartes de paiement sont plus spécifiquement traitées au sein du groupe de travail en charge de la lutte contre la cybercriminalité ;

• pour mener à bien sa mission, Interpol dispose également d'un système d'information centralisé, baptisé I-24/7, accessible à ses membres dans un environnement sécurisé. Afin de compléter ce dispositif, un service d'appui opérationnel permettant de dépêcher sur place des équipes spécialisées en cas d'infraction grave a été mis en place. Enfin, un centre de formation dans ses domaines de compétences est proposé à ses membres.

2|3|2 Des réseaux et structures *ad hoc* complètent ce dispositif pour renforcer son efficacité

À la fois sur le plan très opérationnel de la lutte contre la criminalité, mais également afin d'améliorer la richesse des informations collectées par des organismes comme Europol ou Interpol, des réseaux et structures supplémentaires bénéficiant entre autres à la lutte contre la fraude à la carte de paiement ont été mis en place :

• de manière opérationnelle, sous l'impulsion du G8 et suite aux attentats du 11 septembre 2001 aux États-Unis, un réseau commun de 58 pays (G8 H24) a été instauré dans l'objectif de mettre en relation directe des services d'investigation pour répondre aux demandes urgentes de gel de données numériques et ainsi éviter la disparition d'éléments de preuve ;

• l'Organisation des Nations unies a quant à elle créé une équipe spéciale de lutte contre le terrorisme, organe de liaison et d'échange dont l'objet est d'assister les États dans la mise en œuvre des normes internationales en la matière. Cette structure regroupe diverses entités dépendantes des Nations unies et est en lien avec Interpol, notamment pour lutter contre la fraude aux moyens de paiement en tant que vecteur de financement du terrorisme ;

• en Europe, la Convention européenne d'entraide judiciaire [25] prévoit la possibilité de créer des équipes communes d'enquêtes entre États membres. Ainsi, les autorités judiciaires et services d'enquêtes de chaque pays signataire peuvent échanger des renseignements précis, mener des opérations d'investigation conjointes sur les territoires et coordonner l'exercice des poursuites pénales entre pays impliqués dans une même affaire. De même, l'Office de lutte anti-fraude, qui a notamment pour mission de protéger les intérêts financiers de l'Union européenne contre la fraude, la corruption et toute autre activité illégale, est amené à financer des programmes visant à lutter contre la fraude aux moyens de paiement, la carte de paiement y tenant une place importante étant donné son usage très répandu en Europe.

2|4 Une coopération entre autorités de régulation bancaires qui se met en place à l'échelle européenne mais qui manque encore d'un relai au niveau international

En matière de lutte contre la fraude, si la coopération au sein d'un même secteur est essentielle, elle se doit également d'avoir lieu de manière transversale afin de gagner en efficacité. En ce qui concerne les cartes de paiement, ce sont en majorité les instances de régulation bancaires qui peuvent jouer un rôle dans l'organisation de cette coopération.

2|4|1 L'Observatoire de la sécurité des cartes de paiement, un modèle de coopération

En France, l'Observatoire de la sécurité des cartes de paiement occupe une place de choix. Il regroupe des représentants de l'État, le surveillant et le superviseur bancaires, les administrations, les émetteurs de cartes de paiement, les systèmes de paiement par carte, les

25 Article 13 de la Convention européenne d'entraide judiciaire du 29 mai 2000, complété par la décision cadre du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres

consommateurs et les commerçants. L'Observatoire assure ainsi une grande représentativité des acteurs présents sur le marché de la carte et permet d'échanger sur l'ensemble des sujets d'intérêt commun.

Grâce à la mise en place d'un outil de suivi statistique de l'évolution de la fraude et d'une veille active autour des nouvelles technologies, l'Observatoire a ainsi grandement contribué depuis sa création en 2002 au déploiement et au suivi des dispositifs de sécurité dont bénéficient les cartes de paiement en France, et par là même au maintien du haut niveau de confiance attaché à cet instrument.

Ses travaux ont par ailleurs nourri la réflexion de nombreux acteurs au niveau européen, et son fonctionnement a inspiré la création du Forum européen sur la sécurité des moyens de paiement de détail (« *European Forum on the Security of Retail Payments* » - *SecuRe Pay*).

2|4|2 Les autorités bancaires, actives au niveau européen sous l'impulsion de la BCE

La surveillance des banques centrales : une activité exercée en coopération en Europe

Les banques centrales nationales ont en Europe un rôle déterminant à jouer en ce qui concerne le développement de moyens de paiement scripturaux efficaces et sûrs, rôle que leur confèrent les textes européens [26] et le cas échéant les cadres juridiques nationaux.

Le moyen de paiement carte est le premier instrument scriptural à bénéficier de cette surveillance commune des banques centrales. L'ensemble des systèmes de paiement par carte actifs en Europe, qu'ils soient d'envergure nationale ou internationale, y sont donc soumis. Des évaluations de ces systèmes ont été entreprises dès 2008, selon un référentiel commun [27]. Le résultat consolidé de ces évaluations sera publié au sein d'un rapport reprenant les principaux enseignements tirés. Le volet sécurité y tiendra fort logiquement une place importante.

Partie intégrante de cette surveillance, une collecte annuelle de statistiques en matière de fraude sur les paiements par carte est désormais organisée au niveau européen par la BCE et les banques centrales nationales auprès de l'ensemble des systèmes de paiement par carte actifs, dans une approche similaire à celle de l'Observatoire. À cet effet, un premier rapport sera rendu public en 2012 par la BCE, confirmant les tendances observées au niveau français : une fraude en paiements de proximité maîtrisée mais une préoccupation forte sur les paiements à distance.

Un besoin de coopération entre autorités de régulation bancaires

Aucune structure en Europe ne réunissait encore récemment banquiers centraux et superviseurs afin d'avoir une approche harmonisée des autorités bancaires en matière de sécurité des moyens de paiement. La création en février 2011 du Forum *SecuRe Pay*, auquel participent la Banque de France et l'Autorité de contrôle prudentiel, répond pleinement à ce besoin. Les premières recommandations issues des travaux de ce forum seront publiées fin 2012 [28] et concerneront, à côté de la sécurisation des services bancaires en ligne, celle des paiements par carte en ligne, deux sujets identifiés comme prioritaires par les autorités participant à ce forum.

Cependant, à ce jour, aucune structure équivalente n'existe à l'échelle internationale de manière permanente. On notera que la nécessité d'harmoniser les mesures de sécurité dont bénéficient les moyens de paiement, dont la carte, a récemment été soulignée dans un rapport du Comité en charge des paiements et systèmes de règlement (« *Committee on Payment and Settlement Systems* » – CPSS) de la Banque des règlements internationaux [29].

26 L'article 127 du Traité de Lisbonne sur le fonctionnement de l'Union européenne dispose en effet qu'elles ont notamment pour mission fondamentale de promouvoir le bon fonctionnement des systèmes de paiement. L'article 22 des statuts du Système européen des banques centrales indique qu'elles doivent assurer l'efficacité et la solidité des systèmes de compensation et de paiement.

27 « *Eurosystem oversight framework for card payment schemes – standards* », janvier 2008, *http://www.ecb.int/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf*

28 Une consultation publique sur la version provisoire de ces recommandations a eu lieu du 20 avril au 20 juin 2012, cf. *http://www.ecb.europa.eu/press/pr/date/2012/html/pr120420.en.html*

29 « Innovations in retail payments », disponible à cette adresse : *http://www.bis.org/publ/cpss102.htm*

3| Conclusion et axes d'amélioration

L'ensemble des acteurs du monde de la carte de paiement a un intérêt fort à ce que la lutte contre la fraude soit la plus efficace possible. Quoique poursuivant des objectifs différents (par exemple : maintien de la confiance dans l'instrument de paiement pour les autorités de régulation, démantèlement de réseaux et trafics pour les forces de l'ordre), les acteurs se sont ainsi organisés et structurés dans leurs domaines respectifs avec des résultats tangibles :

• définition de standards en matière de sécurité, utilisation d'outils dédiés à la lutte contre la fraude (banques, EPC) ;

• définition de processus de certification des équipements (systèmes de paiement par carte, agences gouvernementales) ;

• mise en place de structures de renseignement et de répression pour les cas concrets de fraude (forces de l'ordre) ;

• définition de cadres de surveillance (autorités de régulation bancaires).

Afin de renforcer ces dispositifs de lutte contre la fraude, une coopération entre ces acteurs et les différentes structures créées existe, à la fois au niveau national, européen ou international.

Cette coopération porte ses fruits, mais des axes d'amélioration sont possibles :

• les acteurs de marché (banques, systèmes de paiement par carte) bénéficient de structures privilégiées où le sujet de la fraude sur les paiements par carte est abordé. Toutefois, les systèmes de paiement par carte se doivent de rester vigilants en ce qui concerne l'échange opérationnel de données de fraude aidant à la détection de points de compromission, au-delà de préoccupations d'ordre concurrentiel. Les intérêts commerciaux en jeu ne doivent pas en effet affecter la sécurité des opérations par carte ;

• en matière de certification et d'évaluation des composants, processus essentiels permettant de garantir un haut niveau de sécurité des équipements, les acteurs ont la volonté d'adopter en Europe une approche harmonisée pour les cartes de paiement. Toutefois, il reste encore à finaliser une telle approche, notamment sur ses aspects de gouvernance, en ce qui concerne les terminaux d'acceptation ;

• enfin, du côté des autorités de régulation bancaires, des progrès sensibles ont récemment été réalisés au niveau européen (définition d'un cadre de surveillance des systèmes de paiement par carte par les banques centrales européennes en 2008, création du Forum *SecuRe Pay* en 2011, inspiré du modèle de l'Observatoire), mais un besoin d'harmonisation des mesures et donc de coopération des autorités apparaît à l'international, comme le souligne un récent rapport du CPSS sur les innovations dans le domaine des moyens de paiement de détail.

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 :

Sauf en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un proche le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir), il faut déposer une réclamation auprès de l'établissement émetteur de la carte, dès que possible et dans un délai fixé par la loi, de 13 mois à compter de la date de débit de l'opération contestée. Dans ces conditions, votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être immédiatement remboursées sans frais. Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l'opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir dépasser 120 jours.

Bien entendu, en cas d'agissement frauduleux de votre part, les dispositions protectrices de la loi ne trouveront pas à s'appliquer et vous resterez tenu des sommes débitées avant comme après l'opposition ainsi que des éventuels autres frais engendrés par ces opérations (par exemple, en cas d'insuffisance de provision).

Protection du titulaire d'une carte en cas de paiement non autorisé

L'ordonnance de transposition de la directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 1er novembre 2009, a modifié les règles relatives à la responsabilité du titulaire d'une carte de paiement.

La charge de la preuve incombe au prestataire de services de paiement. Ainsi, lorsqu'un client nie avoir autorisé une opération, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée, comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre. La loi encadre désormais strictement les conventions de preuve puisqu'elle prévoit que l'utilisation de l'instrument telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait par négligence grave aux obligations lui incombant en la matière.

Il convient toutefois de distinguer si l'opération de paiement contestée est effectuée ou non sur le territoire de la République française ou au sein de l'Espace économique européen afin de déterminer l'étendue de la responsabilité du titulaire de la carte.

Opérations nationales ou intracommunautaires

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

Concernant les opérations non autorisées, c'est-à-dire en pratique les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, le titulaire de la carte devra contester, auprès de son prestataire dans un délai de 13 mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son prestataire devra alors rembourser immédiatement l'opération non autorisée au titulaire de la carte et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Une indemnisation complémentaire pourra aussi éventuellement être versée. Nonobstant l'extension du délai maximal de contestation à 13 mois, le porteur devra, lorsqu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer sans tarder son prestataire de services de paiement.

Une dérogation à ces règles de remboursement est cependant prévue pour les opérations de paiement réalisées en utilisant un dispositif de sécurité personnalisé, par exemple la frappe d'un code secret.

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

Avant information aux fins de blocage de la carte

Avant « opposition » [2], le payeur pourra supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de la carte si l'opération est effectuée avec l'utilisation du dispositif personnalisé de sécurité. En revanche, si l'opération est effectuée sans l'utilisation du dispositif personnalisé de sécurité, le titulaire de la carte ne voit pas sa responsabilité engagée.

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

En revanche, le titulaire de la carte supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à ses obligations de sécurité, d'utilisation ou de blocage de sa carte, convenues avec son prestataire de services de paiement.

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

Après information aux fins de blocage de la carte

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

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

L'information aux fins de blocage peut être effectuée auprès du prestataire de services de paiement ou auprès d'une entité que ce dernier aura indiquée à son client, suivant les cas, dans le contrat de services de paiement ou dans la convention de compte de dépôt.

Lorsque le titulaire de la carte a informé son prestataire de services de paiement de la perte, du vol, du détournement ou de la contrefaçon de sa carte, ce dernier lui fournit sur demande et pendant 18 mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

Opérations extra-européennes

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

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

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

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

Par ailleurs, le délai maximal de contestation de l'opération est ramené à 70 jours et conventionnellement étendu à 120 jours. En revanche, le remboursement immédiat de l'opération non autorisée est étendu.

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

Missions et organisation de l'Observatoire

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

Cartes concernées

L'ancien article L. 132-1 du *Code monétaire et financier,* dans sa rédaction antérieure au 1er novembre 2009 [1], définissait une carte de paiement comme toute carte émise par un établissement de crédit permettant à son titulaire de retirer ou de transférer des fonds. L'ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, ayant maintenu le périmètre de compétence de l'Observatoire, il a été décidé de continuer de s'appuyer sur cette définition en l'étendant aux prestataires de services de paiement qui sont, aux termes du I de l'article L. 521-1 du *Code monétaire et financier*, les établissements de crédit 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. Il s'agit, d'une part, des cartes monoprestataires émises par une seule entreprise et acceptées en paiement d'un bien ou d'un service déterminé par elle-même ou par des accepteurs ayant noué avec elle un accord de franchise commerciale [3] et, d'autre part, des cartes multiprestataires, qui ne sont acceptées, pour l'acquisition de biens ou de services, que dans les locaux de l'émetteur de la carte ou, dans le cadre d'un accord commercial avec ce dernier, dans un réseau limité de personnes ou pour un éventail limité de biens ou de services [4].

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

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

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

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

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

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

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

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

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

• les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai (supérieur à quarante jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

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

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

• les porte-monnaie électroniques sont des cartes sur lesquelles sont stockées des unités de monnaie électronique. Aux termes de l'article 1 du règlement CRBF n° 2002-13, « une unité de monnaie électronique constitue un titre de créance incorporé dans un instrument électronique et accepté comme moyen de paiement, au sens de l'article L. 311-3 du *Code monétaire et financier*, par des tiers autres que l'émetteur. La monnaie électronique est émise contre la remise de fonds. Elle ne peut être émise pour une valeur supérieure à celle des fonds reçus en contrepartie ».

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

Attributions

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

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

• il est chargé d'établir des statistiques en matière de fraude. À cette fin, les émetteurs de cartes de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents types de cartes de paiement ;

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

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

met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

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

Composition

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

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel 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 sont nommés pour trois ans. Leur mandat est renouvelable.

Le président est désigné parmi ces membres par le ministre chargé de l'Économie, des Finances et du Commerce extérieur. Son mandat est de trois ans, renouvelable. Monsieur Christian Noyer, gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément à l'article R. 142-23 et suivants du *Code monétaire et financier*, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures

proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté en 2003 un règlement intérieur qui précise les conditions de son fonctionnement.

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, des Finances et du Commerce extérieur 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, des Finances et du Commerce extérieur le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail permanents chargés, l'un d'harmoniser et d'établir des statistiques en matière de fraude, l'autre d'assurer une veille technologique relative aux cartes de paiement. En 2010, l'Observatoire a décidé la création d'un groupe de travail dédié à la problématique du déploiement de la technologie « 3D-Secure ».

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

Liste nominative des membres de l'Observatoire

En application de l'article R. 142-22 du *Code monétaire et financier*, les membres de l'Observatoire autres que les parlementaires, ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel sont nommés pour trois ans par arrêté du ministre chargé de l'Économie, des Finances et du Commerce extérieur. Le dernier arrêté de nomination date du 29 juin 2009.

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD
Député
Nicole BRICQ
Sénatrice remplacée à la fin de son mandat par
Michèle ANDRÉ
Sénatrice

Représentant du secrétaire général de l'Autorité de contrôle prudentiel

Philippe RICHARD
Olivier PRATO
Secrétariat général

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

- Le directeur central de la sécurité des systèmes d'information ou son représentant :
  Patrick PAILLOUX

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

- Le haut fonctionnaire de défense ou son représentant :
  Stéphane MARTIN
  Jacques THOMAS

- Le directeur général du Trésor ou son représentant :
  Laurent PERDIOLAT
  Magali CESANA

Sur proposition du ministre chargé de la consommation :

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

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Régis PIERRE
  Jérôme SIMON

Sur proposition du ministre de l'Intérieur :

- Le chef de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ou son représentant :
  Valérie MALDONADO
  Thierry MEZENGUEL

Sur proposition du ministre de l'Intérieur :

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

Sur proposition du ministre délégué de l'Industrie :

- Le directeur général des entreprises ou son représentant :
  Mireille CAMPANA

Représentants des émetteurs de cartes de paiement

Yves BLAVET
Directeur des Instruments de Paiement
Société Générale
Jean-Marc BORNET
Administrateur
Groupement des Cartes Bancaires
Jean-François DUMAS
Vice-président
American Express France
Bernard DUTREUIL (jusqu'au 20 novembre 2011)
remplacé par **Willy DUBOST**
(depuis le 21 novembre 2011)
Directeur Systèmes et Moyens de paiement
Fédération bancaire française
Bernard GOURAUD
Directeur des technologies
Banque Populaire – Caisse d'Épargne
François LANGLOIS
Directeur des Relations institutionnelles
BNP Paribas Personal Finance
Frédéric MAZURIER
Directeur administratif et financier
Carrefour Banque
Gérard NEBOUY
Directeur général
Visa Europe France
Emmanuel PETIT
Président directeur général
MasterCard France
Narinda YOU
Directeur
Stratégie et pilotage interbancaire
Crédit Agricole SA

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

Régis CREPY
Confédération nationale – Associations familiales catholiques (CNAFC)
Valérie GERVAIS
Secrétaire général
Association FO Consommateurs (AFOC)
Christian HUARD (jusqu'au 20 novembre 2011)
remplacé par **Ariane POMMERY**
(depuis le 21 novembre 2011)
Secrétaire général
Association de défense d'éducation et d'information du consommateur (ADEIC)
Jean-Pierre JANIS
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Représentants des organisations professionnelles de commerçants

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

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL
Executive Vice-President
Gemalto
David NACCACHE
Professeur
École normale supérieure
Sophie NERBONNE
Directeur adjoint à la direction des affaires juridiques, internationales et de l'expertise
Commission nationale de l'informatique et des libertés (CNIL)

Dossier statistique

Le dossier statistique qui suit a été réalisé à partir des données concernant l'exercice 2011, 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, ainsi que de MasterCard et de Visa Europe France pour les données internationales ;
- neuf émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref et Sofinco), Cofidis, Cofinoga, Diners Club et Franfinance ;
- les émetteurs du porte-monnaie électronique Moneo.

Total des cartes en circulation en 2011 : 85,8 millions
- dont 64,7 millions de cartes de type « interbancaire » (« CB », MasterCard et Moneo) ;
- et 21,0 millions de cartes de type « privatif ».

Cartes mises en opposition [1] en 2011 : environ 745 000

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 2011 – Émission

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	6 904,07	308,46	125,39	8,17	28,89	3,04
Paiements à distance hors Internet	119,73	9,64	12,06	0,88	2,94	0,31
Paiements à distance sur Internet	380,48	29,62	94,09	4,24	9,75	0,70
Retraits	1 507,83	114,58	27,52	3,03	17,99	2,57
Total	**8 912,10**	**462,30**	**259,06**	**16,32**	**59,59**	**6,62**
Cartes de type « privatif »						
Paiements de proximité et sur automate	133,34	14,89	5,05	0,84	6,79	1,30
Paiements à distance hors Internet	3,11	0,18	nd	nd	nd	nd
Paiements à distance sur Internet	6,72	0,95	2,61	0,22	0,48	0,09
Retraits	4,27	0,38	nd	nd	nd	nd
Total	**147,43**	**16,39**	**7,67**	**1,06**	**7,27**	**1,39**
Total général	**9 059,53**	**478,69**	**266,73**	**17,38**	**66,86**	**8,01**

Source : Observatoire de la sécurité des cartes de paiement

Tableau 2

Le marché des cartes de paiement en France en 2011 – Acquisition

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Cartes de type « interbancaire »						
Paiements de proximité et sur automate	6 904,07	308,46	144,94	10,57	35,21	4,68
Paiements à distance hors Internet	119,73	9,64	6,19	1,40	2,13	0,82
Paiements à distance sur Internet	380,48	29,62	16,75	2,09	3,34	0,48
Retraits	1 507,83	114,58	28,47	4,89	7,03	1,47
Total	**8 385,27**	**462,30**	**196,35**	**18,94**	**47,71**	**7,44**
Cartes de type « privatif »						
Paiements de proximité et sur automate	133,34	14,89	4,99	1,49	4,55	1,58
Paiements à distance hors Internet	3,11	0,18	nd	nd	nd	nd
Paiements à distance sur Internet	6,72	0,95	0,41	0,08	0,41	0,09
Retraits	4,27	0,38	nd	nd	nd	nd
Total	**147,43**	**16,39**	**5,41**	**1,57**	**4,96**	**1,67**
Total général	**9 059,53**	**478,69**	**201,76**	**20,51**	**52,67**	**9,11**

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 2011 – Émission

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	517,1	45 147,2	112,5	11 075,4	85,5	14 521,3
Cartes perdues ou volées	451,3	41 724,7	41,0	3 785,1	18,2	3 442,5
Cartes non parvenues	11,8	367,2	0,7	40,6	0,1	7,1
Cartes altérées ou contrefaites	47,4	2 929,1	23,1	2 987,1	48,2	8 294,9
Numéro de carte usurpé	1,0	63,1	45,4	4 067,5	17,2	2 481,8
Autres	5,6	63,2	2,3	195,1	1,8	294,9
Paiements à distance hors Internet	384,5	25 159,8	60,1	5 644,3	24,3	3 117,7
Cartes perdues ou volées	2,2	153,4	15,6	1 593,6	7,3	994,3
Cartes non parvenues	0,0	1,3	0,2	2,4	0,1	2,4
Cartes altérées ou contrefaites	0,0	1,1	12,7	1 062,4	5,8	702,8
Numéro de carte usurpé	382,2	25 003,1	30,9	2 944,1	10,9	1 399,8
Autres	0,0	0,8	0,6	41,9	0,2	18,4
Paiements à distance sur Internet	795,8	101 203,7	321,3	24 112,5	85,3	10 671,3
Cartes perdues ou volées	6,8	880,8	88,4	6 733,9	32,3	3 055,7
Cartes non parvenues	0,0	1,0	0,3	22,0	0,1	9,2
Cartes altérées ou contrefaites	0,1	17,3	71,4	4 763,8	31,8	2 942,8
Numéro de carte usurpé	788,9	100 302,2	159,0	12 240,6	49,0	4 602,2
Autres	0,0	2,4	2,2	352,2	0,3	61,3
Retraits	119,8	33 382,2	5,7	1 199,6	121,7	20 525,8
Cartes perdues ou volées	112,4	32 042,7	3,7	808,7	7,0	1 089,5
Cartes non parvenues	0,5	111,9	0,0	3,9	0,1	6,4
Cartes altérées ou contrefaites	6,1	1 115,4	1,8	345,7	110,7	18 714,3
Numéro de carte usurpé	0,0	2,5	0,1	6,7	0,6	92,3
Autres	0,7	109,7	0,2	34,7	3,3	623,3
Total	**1 817,2**	**204 892,9**	**499,6**	**42 031,8**	**344,9**	**48 836,1**

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 2011 – Acquisition

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	517,1	45 147,2	146,8	21 641,0	306,1	76 015,1
Cartes perdues ou volées	451,3	41 724,7	48,2	2 324,9	40,8	11 030,3
Cartes non parvenues	11,8	367,2	3,1	117,6	0,5	163,3
Cartes altérées ou contrefaites	47,4	2 929,1	12,2	2 746,5	94,6	23 704,3
Numéro de carte usurpé	1,0	63,1	78,5	16 223,6	167,8	40 570,2
Autres	5,6	63,2	4,9	228,4	2,3	547,0
Paiements à distance hors Internet	384,5	25 159,8	nd	nd	nd	nd
Cartes perdues ou volées	2,2	153,4	nd	nd	nd	nd
Cartes non parvenues	0,0	1,3	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,0	1,1	nd	nd	nd	nd
Numéro de carte usurpé	382,2	25 003,1	nd	nd	nd	nd
Autres	0,0	0,8	nd	nd	nd	nd
Paiements à distance sur Internet	795,8	101 203,7	nd	nd	nd	nd
Cartes perdues ou volées	6,8	880,8	nd	nd	nd	nd
Cartes non parvenues	0,0	1,0	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,1	17,3	nd	nd	nd	nd
Numéro de carte usurpé	788,9	100 302,2	nd	nd	nd	nd
Autres	0,0	2,4	nd	nd	nd	nd
Retraits	119,8	33 382,2	2,9	822,3	2,3	611,4
Cartes perdues ou volées	112,4	32 042,7	2,5	705,4	1,2	332,2
Cartes non parvenues	0,5	111,9	0,1	31,3	0,0	3,4
Cartes altérées ou contrefaites	6,1	1 115,4	0,2	55,1	1,0	250,5
Numéro de carte usurpé	0,0	2,5	0,0	10,1	0,1	22,4
Autres	0,7	109,7	0,1	20,4	0,0	2,9
Total	**1 817,2**	**204 892,9**	**149,7**	**22 463,4**	**308,4**	**76 626,5**

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 2011 – Émission

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	6,22	2 990,27	5,29	1 511,70	5,68	1 470,43
Cartes perdues ou volées	2,24	407,28	1,90	159,72	0,33	143,06
Cartes non parvenues	0,56	211,84	0,21	171,71	0,06	23,10
Cartes altérées ou contrefaites	1,34	299,94	1,54	602,55	4,45	940,35
Numéro de carte usurpé	0,66	107,04	1,58	542,12	0,81	360,74
Autres	1,43	1 964,16	0,06	35,60	0,03	3,18
Paiements à distance hors Internet	0,30	239,25	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,17	11,04	nd	nd	nd	nd
Autres	0,13	128,21	nd	nd	nd	nd
Paiements à distance sur Internet	10,07	3 011,32	6,58	744,10	2,82	741,61
Cartes perdues ou volées	2,10	805,71	1,75	26,54	0,16	66,70
Cartes non parvenues	0,71	310,93	0,03	2,57	0,01	9,15
Cartes altérées ou contrefaites	2,66	535,42	1,23	71,40	0,98	280,87
Numéro de carte usurpé	3,69	1 008,55	3,48	624,32	1,65	378,87
Autres	0,90	350,70	0,09	19,26	0,02	6,13
Retraits	1,95	359,19	nd	nd	nd	nd
Cartes perdues ou volées	1,55	249,36	nd	nd	nd	nd
Cartes non parvenues	0,26	66,45	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	9,34	nd	nd	nd	nd
Autres	0,12	34,05	nd	nd	nd	nd
Total	**18,54**	**6 600,02**	**11,87**	**2 255,79**	**8,50**	**2 212,03**

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 2011 – Acquisition

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume	**Valeur**	**Volume**	**Valeur**	**Volume**	**Valeur**
Paiements de proximité et sur automate	6,22	2 990,27	1,15	493,00	2,96	962,28
Cartes perdues ou volées	2,24	407,28	0,06	11,90	0,11	49,61
Cartes non parvenues	0,56	211,84	0,00	0,02	0,00	0,00
Cartes altérées ou contrefaites	1,34	299,94	0,69	149,26	1,93	321,74
Numéro de carte usurpé	0,66	107,04	0,40	314,04	0,86	580,00
Autres	1,43	1 964,16	0,00	17,79	0,06	10,94
Paiements à distance hors Internet	0,30	239,25	nd	nd	nd	nd
Cartes perdues ou volées	0,00	0,00	nd	nd	nd	nd
Cartes non parvenues	0,00	0,00	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,17	11,04	nd	nd	nd	nd
Autres	0,13	128,21	nd	nd	nd	nd
Paiements à distance sur Internet	10,07	3 011,32	4,70	2 126,15	9,41	3 685,65
Cartes perdues ou volées	2,10	805,71	0,40	77,92	0,78	340,94
Cartes non parvenues	0,71	310,93	0,01	0,12	0,04	0,55
Cartes altérées ou contrefaites	2,66	535,42	1,14	507,24	3,39	1 438,16
Numéro de carte usurpé	3,69	1 008,55	3,14	1 464,02	5,11	1 885,07
Autres	0,90	350,70	0,02	76,34	0,09	20,83
Retraits	1,95	359,19	nd	nd	nd	nd
Cartes perdues ou volées	1,55	249,36	nd	nd	nd	nd
Cartes non parvenues	0,26	66,45	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,02	9,34	nd	nd	nd	nd
Autres	0,12	34,05	nd	nd	nd	nd
Total	**18,54**	**6 600,02**	**5,85**	**2 619,16**	**12,37**	**4 647,93**

Source : Observatoire de la sécurité des cartes de paiement

Définition et typologie de la fraude relative aux cartes de paiement

Définition de la fraude

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

• ayant pour conséquence un préjudice pour le banquier teneur de compte qu'il s'agisse du banquier du porteur de la carte ou de celui de l'accepteur (commerçant, administration… pour son propre compte ou au sein d'un système de paiement [1]), le porteur, l'accepteur, l'émetteur, un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ;

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

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

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

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

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

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

Typologie de la fraude

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

Les origines de fraude :

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

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

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

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

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

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

Les techniques de fraude :

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

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

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

3 Personal Account Number

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

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

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

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

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

Les types de paiement :

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

La répartition du préjudice entre :

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

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

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

Le *rapport de l'Observatoire de la sécurité des cartes de paiement* est en libre téléchargement sur le site internet de l'Observatoire (*www.observatoire-cartes.fr*).

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

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

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

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

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

Secrétariat de rédaction
Marcia Toma

Réalisation
Direction de la Communication
de la Banque de France

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

Version papier
Observatoire de la sécurité des cartes de paiement
011-2324
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