2010 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 2010
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Monsieur le Ministre de l'Économie, des Finances et de l'Industrie
Monsieur le Président du Sénat
Monsieur le Président de l'Assemblée nationale

par

Monsieur Christian Noyer,

Gouverneur de la Banque de France,
Président de l'Observatoire de la sécurité des cartes de paiement

SOMMAIRE

AVANT-PROPOS

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 chargé de l'économie, des finances et de l'industrie et transmis au Parlement. Il comprend cette année :

- une étude sur les coûts de migration aux standards EMV (1ère partie) ;
- une présentation des statistiques de fraude pour 2010 (2ème partie) ;
- un état des lieux de la sécurisation des paiements par carte sur Internet (3ème partie) ;
- une synthèse des travaux conduits en matière de veille technologique (4ème partie), avec deux sujets traités : la sécurité des cartes prépayées et les avancées récentes en matière de standardisation européenne ;
- une étude portant sur les enjeux sécuritaires liés aux évolutions des systèmes de paiement par carte en France et en Europe (5ème partie) ;
- enfin, en annexe et suite à la transposition en novembre 2009 de la directive européenne sur les services de paiement, un rappel des nouvelles règles de protection du titulaire d'une carte de paiement en cas de paiement non autorisé.

[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.

SYNTHÈSE

Le huitième rapport annuel d'activité de l'Observatoire de la sécurité des cartes de paiement, relatif à l'exercice 2010, comprend cette année cinq parties dont les principales conclusions sont reprises ci-après.

1ère partie : étude sur les coûts de migration aux standards EMV

L'Observatoire a souhaité cette année intégrer à son rapport un volet relatif aux différents coûts de la sécurité. Sa première étude dans ce domaine porte sur les coûts de migration aux standards EMV. Les coûts liés à cette migration, qui s'est déroulée entre 2001 et 2008, sont estimés par les acteurs interrogés à un total de 394 millions d'euros pour les banques et de 340 millions d'euros pour les commerçants. En plus de ces coûts d'investissement, les dépenses récurrentes annuelles, variables selon les établissements, sont évaluées en moyenne à 41 millions d'euros pour les banques et 12 millions d'euros pour les commerçants. Achevée en France, cette migration se poursuit au niveau international et fait l'objet d'un suivi régulier par l'Observatoire au plan européen. Les nombreuses mesures mises en place pour accroître la sécurité ont dans leur ensemble permis une baisse importante des taux de fraude constatés. Les standards EMV seront par ailleurs amenés à évoluer, afin de prendre en compte de nouvelles menaces ou de s'adapter à de nouvelles cinématiques de paiement, tel le paiement sans contact, ou de nouvelles habitudes de consommation, comme l'usage de cartes multi-applicatives.

2ème partie : statistiques de fraude pour l'année 2010

Le taux de fraude s'établit pour l'année 2010 à 0,074 %, correspondant à un montant de 368,9 millions d'euros (contre 0,072 % et 342,4 millions d'euros en 2009), ce qui recouvre des évolutions divergentes :

- la fraude sur les paiements nationaux réalisés aux points de vente et sur automates continue de décroître et se situe à un niveau très faible (0,012 %, pour un montant de 36,2 millions d'euros) ;
- en contrepartie, la fraude en valeur nominale continue d'augmenter sur les paiements à distance (par Internet, téléphone ou courrier) :
  - pour les paiements nationaux effectués à distance, le taux de fraude est de 0,262 % et le montant de la fraude de 101,1 millions d'euros (contre 0,263 % et 82,2 millions d'euros en 2009) dans un contexte de croissance soutenue des paiements à distance (+ 23,8 % en 2010). Ces derniers, qui représentent 8,6 % de la valeur des transactions nationales, comptent désormais pour 62 % du montant de la fraude ;
  - la fraude sur les paiements à distance enregistrée pour des cartes françaises chez des commerçants étrangers est en recul mais demeure élevée avec un taux de fraude de 1,018 %, pour un montant de 54,0 millions d'euros.

Par ailleurs et pour la première fois cette année, 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 supérieurs aux taux relevés en Europe pour des cartes émises en France, et des cartes étrangères émises hors Europe fraudées près de quatre 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.

3ème partie : sécurisation des paiements par carte sur internet

Le déploiement par les banques de solutions de sécurisation auprès de leurs porteurs est aujourd'hui généralisé, conformément aux recommandations de la Banque de France. L'Observatoire se félicite de la migration de plusieurs grands e-commerçants comme Air France, Orange Boutique et Voyages-SNCF vers des dispositifs d'authentification non rejouable des paiements par carte. Il salue la création, sous l'égide de la Banque Centrale Européenne, du forum européen sur la sécurité des moyens de paiement, qui devra notamment permettre d'assurer la sécurisation des paiements par carte sur Internet à l'échelle européenne. Enfin, l'Observatoire a conduit une étude dont il ressort que l'expérience des cyberacheteurs au regard des dispositifs de sécurisation est globalement positive, 96 % d'entre eux estimant que les dispositifs d'authentification non rejouable présentés renforcent la sécurité des paiements par carte sur Internet. Un accompagnement des utilisateurs pour l'appropriation de ces nouveaux dispositifs par tous reste néanmoins nécessaire.

4ème partie : travaux de veille technologique autour de la sécurité des cartes prépayées et de la standardisation européenne dans le domaine de la carte

L'Observatoire a étudié le marché des cartes prépayées rechargeables dont la valeur est stockée sur les serveurs de l'émetteur. Encore anecdotique en France, la distribution de ces cartes est en pleine croissance et pourrait être amplifiée par la mise en œuvre au niveau européen du nouveau statut d'émetteur de monnaie électronique introduit par la Directive 2009/110/CE. Ces cartes pouvant être acquises et utilisées de façon anonyme, elles sont vulnérables à la contrefaçon et doivent donc prévoir des dispositifs de sécurité adéquats (présence d'une puce notamment). L'Observatoire estime en outre que l'utilisation potentielle de ces cartes à des fins de transferts de fonds entre particuliers nécessite la mise en place de dispositifs de surveillance adaptés, éventuellement précisés dans des dispositions légales à définir.

Par ailleurs, l'Observatoire a dressé cette année un panorama de la standardisation dans le domaine de la carte en Europe, en notant des avancées significatives sur les efforts d'harmonisation entrepris depuis plusieurs années sur les aspects techniques.

5ème partie : enjeux sécuritaires en France et en Europe

La lutte contre le « *skimming* » (vol de données aux distributeurs et terminaux de paiement) et la protection des transactions à distance par carte représentent des enjeux particulièrement importants, au regard de leur impact en termes de fraude. Alors que plusieurs initiatives visant à créer un nouveau système de paiement par carte européen ont été annoncées, il convient de s'assurer que ces enjeux sont bien pris en compte par l'ensemble des acteurs, et les mesures adéquates adoptées de manière coordonnée.

1 LES COÛTS DE MIGRATION AUX STANDARDS EMV

Au titre de sa mission de suivi des politiques de sécurité mises en œuvre par les émetteurs, les acquéreurs et les accepteurs, l'Observatoire a souhaité, dans le cadre de son rapport 2010, étudier les modalités de migration aux standards EMV (« Europay Mastercard Visa »), laquelle a débuté dès 2002 en France et fait l'objet chaque année d'un suivi spécifique (voir p. 66 du présent rapport).

Il s'agit ici de revenir sur les dispositions prises par chacun des acteurs, individuellement ou de façon concertée, visant à migrer les cartes et matériels au format EMV, ainsi que de mesurer l'impact de cette migration, tant en termes organisationnels que techniques et financiers.

L'Observatoire a conduit son étude sur la base d'informations recueillies auprès de représentants des établissements émetteurs, des commerçants ainsi que des systèmes de paiement par carte ayant été impliqués dans la migration aux standards EMV[2].

1 1 La migration aux standards EMV

Les raisons de la migration aux standards EMV

Dès 1992, en France, l'ensemble des cartes en circulation bénéficiait de la présence d'une puce, le format appliqué répondant au nom de B0'. Ce type de carte a permis d'éradiquer un premier type de fraude, basé sur la lecture, la copie puis la reproduction des données présentes sur la piste.

Ces cartes à puce de première génération sont toutefois apparues potentiellement vulnérables à des attaques visant à compromettre les clés cryptographiques protégeant les communications entre la carte et le terminal. Un nouveau type de fraude est en outre apparu à la fin de cette décennie, consistant à falsifier des cartes utilisables pour réaliser des transactions en mode déconnecté (« off-line »), quel que soit le code PIN entré. Ces cartes sont couramment appelées des « YesCards ».

La communauté bancaire française a donc décidé de migrer progressivement l'ensemble des cartes et terminaux de paiement au format EMV[3] dès l'année 2001, la migration devant initialement s'étendre jusqu'en 2003. Dans les faits, il aura fallu attendre 2004 pour voir la plupart des matériels compatibles avec les nouvelles spécifications, et 2008 afin d'obtenir des taux de migration proches de 100 %.

La migration aux standards EMV s'est en fait déroulée en deux phases : dans un premier temps (2002-2005), les cartes et matériels d'acceptation ont migré au format EMV SDA (*Static Data Authentication*), renforçant les procédés cryptographiques par rapport à B0' ; dans un second temps (2005-2008), ces matériels ont progressivement intégré le format EMV DDA (*Dynamic Data Authentication*). L'ensemble des cartes actives sur le territoire français intègre désormais

2 BNP Paribas, BPCE, Crédit Agricole SA, Crédit Mutuel-CIC, Société Générale, La Banque Postale, LCL, GIE Cartes Bancaires, Mastercard, American Express, Mercatel.

3 Les standards EMV font l'objet d'une description en annexe de cette fiche.

cette fonctionnalité, permettant une authentification dynamique de la carte en mode déconnecté. Il n'est donc théoriquement plus possible de fabriquer une « YesCard », la carte disposant de son propre système cryptographique afin de chiffrer ses données d'identification.

Les modalités de migration aux standards EMV

La migration aux standards EMV a nécessité la mise en œuvre de processus tant organisationnels que techniques de la part des trois catégories d'acteurs impliqués : les systèmes de paiement par carte, les banques, agissant en tant qu'émetteur ou acquéreur, et les commerçants.

Les aspects organisationnels

Selon les acteurs interrogés, les processus mis en œuvre afin de permettre la migration aux standards EMV ont été le plus souvent internalisés. Ils ont conduit à la constitution d'équipes dédiées aux différentes étapes de la chaîne de traitement.

Les systèmes de paiement par carte et les banques ont tout d'abord été conduits à mettre en place des « équipes projet » chargées de la migration. Ces équipes ont été constituées en amont de la période effective de mise en œuvre technique (voir ci-dessous), ont participé aux différentes phases du cycle de vie du projet (tests, pilotes, déploiement) et sont généralement restées en place après la date de migration effective afin d'assurer un support technique et un accompagnement au changement de l'ensemble des équipes internes :

– les équipes techniques ont en effet dû intégrer les spécificités des standards EMV, en matière cryptographique et de gestion des autorisations sur les serveurs de l'émetteur notamment. La gestion des incidents a également été considérée par les acteurs interrogés comme un élément impactant, en termes humain et financier, durant la phase de déploiement ;

– les équipes formant les « back-offices » en charge des traitements des transactions de carte ont également dû être formées.

Les banques interrogées ont enfin mis en place des plans de communication à destination des porteurs et commerçants, visant à justifier les motivations ayant conduit au remplacement accéléré du parc de terminaux, de DAB et de cartes, afin de maintenir un niveau de confiance élevé sur l'ensemble de la filière.

De leur côté, les commerçants, notamment les grands groupes disposant de leur propre système monétique, ont eux aussi structuré leur approche organisationnelle en constituant des équipes projet à même d'examiner l'ensemble des impacts de la migration aux standards EMV sur leur chaîne de paiement aux points de vente.

Les aspects techniques

Au-delà des aspects organisationnels internes, la migration aux standards EMV a nécessité entre 2002 et 2004 de nombreux investissements liés à la mise à niveau d'une part des matériels et logiciels intervenant dans la filière d'acquisition, d'autre part des cartes en ce qui concerne la filière d'émission.

Les terminaux de paiement et DAB ont en effet vu leurs caractéristiques profondément évoluer afin d'intégrer les cinématiques de communication propres aux cartes EMV. Dans le but de

tester ces matériels et de procéder aux évaluations de conformité requises, les systèmes de paiement par carte ont donc dans un premier temps mis à niveau leurs outils matériels et logiciels.

Les banques, qui restent dans la majorité des cas propriétaires des équipements mis à la disposition des commerçants et qui sont donc chargées de leur mise à jour, ont ensuite fait évoluer leurs équipements. La migration aux standards EMV a ainsi conduit à un renouvellement accéléré du parc de terminaux de paiement et de DAB sur le territoire.

Les commerçants disposant de leurs propres matériels ont adopté la même démarche, avec un renouvellement des terminaux, des concentrateurs monétiques[4] et une mise à jour des serveurs centraux reliés aux serveurs d'acquisition de leurs établissements bancaires acquéreurs.

En ce qui concerne la filière d'émission, les banques interrogées ont indiqué que les dépenses d'investissements liées aux cartes étaient dues non seulement au renouvellement du parc, de façon similaire à celui des terminaux de paiement, mais également à l'intégration d'un surcoût lié directement à leur évolution technologique. Ainsi, l'évolution des puces conformes aux standards EMV et les mises à niveau des logiciels utilisés dans le processus de personnalisation ont naturellement conduit à une anticipation et à une augmentation des dépenses programmées liées au cycle de vie normal des cartes. De nouveaux équipements ont également dû être déployés en interne ou par les prestataires en charge de la personnalisation, tels les HSM[5], en raison des nouvelles fonctionnalités cryptographiques intégrées aux cartes.

Enfin, les banques ont adapté leurs systèmes afin d'y intégrer les données propres au format EMV. Ceci concerne tant les serveurs d'autorisation que d'acquisition, tous deux reliés aux réseaux d'échanges interbancaires, que les systèmes internes utilisés à des fins de suivi et d'analyse des transactions.

1|2 Les aspects financiers

Les investissements initiaux

Les acteurs interrogés ont tout d'abord souligné l'importance des coûts précédemment engagés afin de migrer leurs systèmes et matériels au format B0', qui requérait l'usage d'une puce sur la carte de paiement. La migration aux standards EMV a donc été ressentie en France de façon moins forte que dans les pays cumulant l'adoption de la puce et de ces spécifications au sein d'un même processus de migration. En outre, la migration s'est inscrite dans le cadre d'une réflexion plus globale de mise à niveau des systèmes d'information afin d'intégrer les problématiques liées au passage à l'an 2000 et à l'euro, qui ont mobilisé la quasi-totalité des équipes techniques.

Les données rapportées par les acteurs interrogés peuvent ainsi inclure des investissements et dépenses récurrentes à caractère plus large que la seule migration aux standards EMV.

4 Voir rapport 2007, ch. 1, p. 9.

5 Hardware Security Module : équipement cryptographique permettant de protéger les secrets les plus critiques (clés de chiffrement, d'authentification) et de prendre en charge certains processus liés à la génération et la gestion de secrets.

Les tendances suivantes ont toutefois pu être mises en évidence :

– le total des investissements déclarés par les banques interrogées, qui gèrent à elles seules 97 % du parc de matériel déployé sur le territoire s'élève à 383 M€. Par extrapolation au regard du parc de matériel concerné, les dépenses d'investissement à l'échelle nationale peuvent donc être estimées à 394 M€ ;

– les commerçants ont quant à eux estimé le coût total de leurs investissements, lesquels intègrent notamment les dépenses engagées par les grands commerçants comme vu précédemment (concentrateurs monétiques, terminaux intégrés, distributeurs automatiques de carburants…), à un montant global de 340 M€, soit un niveau proche de celui des banques.

Seul un système de paiement par carte ayant déclaré des données chiffrées lors de cette enquête, aucune estimation globale n'est possible pour cette catégorie d'acteur. Pour autant, il est admis que les dépenses engagées par les systèmes de paiement par carte restent négligeables comparées à celles des commerçants et des banques.

Les coûts récurrents suite à la migration

Au-delà des dépenses initiales liées au projet de migration, la mise en conformité aux standards EMV engendre également des coûts récurrents.

La réorganisation interne des acteurs interrogés, comme vu précédemment, a eu un impact à plus long terme en raison du redimensionnement des équipes, de leur montée en compétence sur le sujet ou de la nécessaire mise en place d'équipes de recherche et développement sur le domaine considéré. Ces dépenses, comme celles liées à la mise en place de plans de communication ou de programmes spécifiques d'audit et d'inspection, correspondent à une augmentation des sommes allouées, à caractère pérenne, sur des postes de dépenses préexistants.

Les dépenses engagées visant au renouvellement des matériels dans le cadre de leur cycle de vie ont également augmenté mécaniquement en raison de leur évolution technologique. A titre d'exemple, un surcoût affectant les dépenses de fabrication et de personnalisation des cartes est venu s'ajouter et s'élève à 1,5 % par an depuis 2007. Les composants électroniques y représentent une part non négligeable[6]. En outre, de nouveaux types de dépenses sont apparus. On peut par exemple citer les dépenses liées au renouvellement des clés cryptographiques gérées au sein des HSM (voir ci-dessus).

Selon les résultats de l'enquête, les coûts récurrents peuvent ainsi être estimés entre 9 et 13 % des dépenses d'investissement[7], soit une moyenne annuelle de 41 M€ à l'échelle nationale. Les représentants des commerçants ont indiqué pour leur part des coûts annuels de l'ordre de 12 M€.

6 Source AFPC, 03/2011. Les composants électroniques contribuent à hauteur de 1/5ème de l'augmentation.

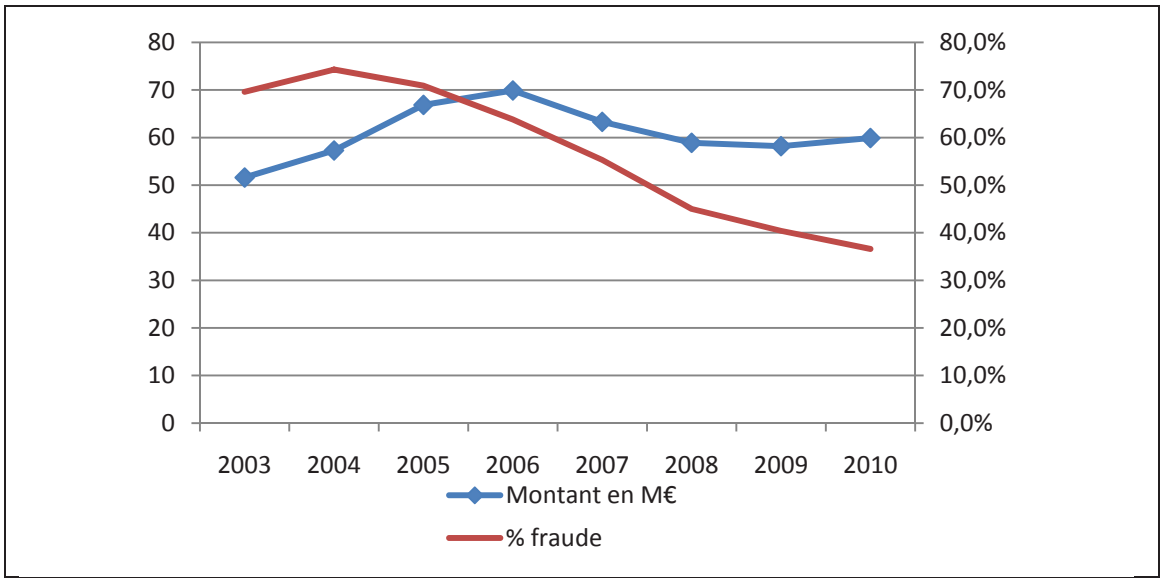
7 Fourchette constatée après élimination des extrêmes.

1|3 Les effets constatés et attendus de la migration

L'impact de la migration sur la fraude : un objectif atteint

Les standards EMV ont été développés en France afin d'apporter une réponse à l'augmentation croissante de la fraude liée aux cartes contrefaites, en renforçant la sécurité du processus cryptographique jusqu'en 2005, puis en intégrant des crypto-processeurs dans les cartes elles-mêmes à partir de cette date.

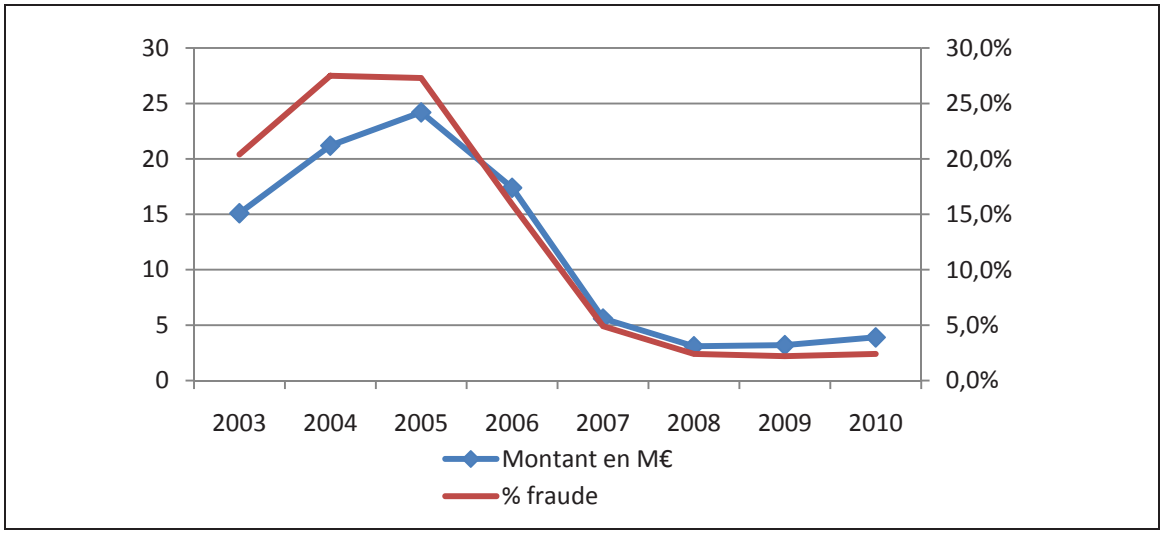
Le tableau suivant montre l'évolution de la fraude en contrefaçon et en perte/vol entre les années 2003 et 2010 (en montant et pourcentage du total de la fraude).



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 1 – **L'évolution de la fraude en contrefaçon et en perte/vol**

On observe une diminution régulière du montant fraudé à partir de 2004, qui provient essentiellement de la seule fraude en contrefaçon comme le montre le tableau ci-dessous :



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 2 – **L'évolution de la fraude en contrefaçon**

On observe ainsi une baisse du montant de la fraude de 20 M€ sur une base annuelle. Ce montant est toutefois sous-estimé si l'on considère que la tendance haussière en montant observée entre 2003 et 2005 se serait probablement poursuivie sans l'application des standards EMV. Il est toutefois difficile d'en évaluer l'ampleur.

Ces données confirment les tendances communiquées par les acteurs interrogés, lesquels ont ressenti une forte baisse du taux de fraude lié à la contrefaçon des cartes dès 2006. La migration aux standards EMV a ainsi permis de lutter efficacement contre le type de fraude décrit en 1 | 1 (« YesCards »), lequel a été éradiqué sur le territoire français. Les standards EMV permettent en outre d'optimiser les processus de gestion du risque mis en œuvre par les émetteurs, en autorisant la délocalisation de certains contrôles au point de vente.

Les spécifications EMV doivent toutefois être adoptées au niveau international pour être totalement efficaces. Les banques interrogées ont en effet constaté le report de la fraude en contrefaçon sur les transactions effectuées à l'étranger, ce qui contribue au maintien d'un niveau résiduel pour ce type de fraude. L'Observatoire suit ainsi depuis plusieurs années l'état d'avancement de la migration en Europe, laquelle progresse régulièrement dans chacun des pays, bien que ceux-ci affichent encore des taux de migration très différents pour les cartes et terminaux.

En outre, l'Eurosystème a recommandé, à partir de 2012, l'émission en Europe de cartes à puce ne comportant plus de piste, témoignant de l'avancée de la migration au niveau international et donnant une nouvelle impulsion afin d'achever cette migration au plus tôt. Le Conseil Européen des Paiements[8] a adopté une approche similaire.

Plus globalement, la sécurisation des transactions de proximité atteinte grâce à l'application des standards EMV a déplacé progressivement la fraude sur les paiement à distance, qui représentent désormais la majeure partie de la fraude globale, et qui font par ailleurs l'objet de recommandations sécuritaires de l'Observatoire depuis plusieurs années.

Les autres bénéfices réalisés ou attendus

Au-delà de l'effet direct sur le taux de fraude constaté pour les transactions de proximité comme vu ci-dessus, l'application des standards EMV a permis à l'ensemble des acteurs concernés de bénéficier d'autres avantages, non chiffrables.

Les commerçants bénéficient, à leur niveau, du transfert de responsabilité sur la banque émettrice en cas de fraude. Ceci est directement lié à la matérialisation du consentement du porteur par la saisie de son code PIN lors d'une transaction de proximité.

L'application de ces spécifications permet ensuite de standardiser l'ensemble des processus mis en œuvre et ainsi de bénéficier d'économies d'échelle non négligeables. L'« écosystème cartes » bénéficiait déjà d'une telle uniformisation liée à l'application du format B0' sur un plan national, mais les standards EMV ont permis d'asseoir cet avantage et de l'étendre au niveau international pour des acteurs eux-mêmes présents sur de nombreux marchés.

Le niveau de confiance dans ce moyen de paiement s'est également renforcé suite à l'application de ces standards et aux actions de communication engagées par chacun des acteurs interrogés (voir ci-dessus).

8 *European Payment Council* (EPC), organisme représentatif de l'industrie bancaire en Europe, chargé du développement du projet SEPA.

Enfin, certaines actions ont pu être menées par les systèmes de paiement par carte avec des représentants de secteurs particuliers (grands commerces, pétroliers…) afin de les inciter à migrer rapidement aux standards EMV, contribuant ainsi à élever le niveau de sécurité de l'ensemble de la filière d'acceptation. C'est par exemple le cas concernant l'acquisition de terminaux de paiement.

Les évolutions prévues liées aux standards EMV

Les acteurs interrogés ont recensé deux grandes catégories d'évolutions liées à l'application des standards EMV au cours des prochaines années :

– tout d'abord, les standards EMV eux-mêmes continueront d'évoluer afin de prendre en compte les technologies émergentes dans le domaine de la carte et d'améliorer la sécurité des transactions.

  Les standards EMV intègrent ainsi désormais un recueil spécifique aux transactions sans contact[9], prévoyant une adaptation des standards EMV à ce type particulier de transactions lors d'achats de proximité.

  Concernant la sécurité, la prochaine phase attendue est la migration au format CDA (*Combined Data Authentication*), qui permet de s'assurer que la carte prenant part au processus d'autorisation est bien celle ayant été authentifiée durant la phase d'initiation de la transaction. La mise en œuvre des standards EMV CDA conduira à une nouvelle mise à niveau des cartes et terminaux de paiement, lesquels sont actuellement en majorité encore incompatibles avec ce format ;

– enfin, l'application des standards permet de faire cohabiter sur une même puce plusieurs applications, en garantissant un niveau de sécurité élevé pour chacune d'entre elles (et en premier lieu pour les applications de paiement). Si cette fonctionnalité n'est pas ou peu exploitée aujourd'hui, elle autorise à l'avenir le développement de programmes de fidélité ou de garanties gérés à l'aide d'applications intégrées aux cartes de paiement des porteurs, réduisant les risques de perte liés à la détention d'un grand nombre de cartes et facilitant les relations commerciales entre l'émetteur, le partenaire (commerçant) et le porteur.

1|4 Conclusion

La migration aux standards EMV a mobilisé, de façon coordonnée, l'ensemble des acteurs interrogés sur une période de trois ans à partir de 2001, voire plus si l'on tient compte de la migration résiduelle de matériels isolés jusqu'en 2008. Elle a nécessité la mobilisation de moyens importants, tant humains que financiers, sur l'ensemble de la chaîne de traitement.

Ainsi, l'Observatoire a pu estimer que les coûts liés à la migration aux standards EMV entre 2001 et 2008, sur la base des données transmises par les acteurs interrogés, ont été supportés quasiment à parts égales entre les banques (394 M€) et les commerçants (340 M€). Les dépenses relevant des systèmes de paiement par carte apparaissent négligeables, mais les réponses reçues ne permettent pas de se prononcer plus avant. Les dépenses récurrentes annuelles, variables selon les établissements, ont quant à elles été estimées à 41 M€ pour les banques et 12 M€ pour les commerçants.

9 EMV Contactless Specifications for Payment Systems.

Il apparaît toutefois difficile de rapprocher les coûts des économies réalisées par les acteurs suite à la migration, pour trois raisons :

– tout d'abord, ceux-ci englobent potentiellement des postes de dépenses liés à d'autres projets majeurs concomitants, ayant mobilisé des moyens communs ;

– ensuite, si l'application des standards EMV a eu indéniablement un impact fort sur le taux de fraude lié à la contrefaçon, représentant à ce jour une réelle avancée sécuritaire dans le domaine de la carte, il apparaît délicat de préjuger de l'évolution de ce taux en l'absence de migration ;

– enfin, les acteurs concernés ont bénéficié d'autres avantages liés à l'application des standards EMV, lesquels ne peuvent être chiffrés, tels le transfert de responsabilité pour les commerçants, la standardisation à une échelle internationale et le maintien d'un niveau de confiance élevé dans la carte.

Cette migration est aujourd'hui achevée en France mais se poursuit au niveau international, ce qui fait l'objet d'un suivi régulier par l'Observatoire au plan européen. Seule une telle généralisation est en effet de nature à faire bénéficier aux acteurs de l'ensemble des effets attendus, la fraude s'étant reportée sur les pays les moins avancés au fil des années.

Les standards EMV seront par ailleurs amenés à évoluer, afin de prendre en compte de nouvelles menaces ou de s'adapter à de nouvelles cinématiques de paiement, tel le paiement sans contact, ou de nouvelles habitudes de consommation, comme l'usage de cartes multi-applicatives. Les coûts récurrents liés directement à l'évolution de ces standards seront donc conjugués dans les prochaines années à de nouvelles dépenses d'investissement visant à répondre à ces besoins.

Annexe

Les standards EMV

Les standards EMV sont développés par EMVCo, regroupant les réseaux VISA, MASTERCARD, JCB et AMERICAN EXPRESS. Ils permettent l'interopérabilité internationale des transactions de paiement et de retrait par cartes de type « interbancaire » à puce dans un contexte multi-applicatif[10]. Les standards EMV visent à la fois à permettre le développement de nouveaux services et à améliorer la sécurité des transactions.

La dernière version des standards EMV (4.2), publiée en juin 2008, a été complétée de spécifications dites CPA (« Common Payment Application »)[11], CPS (« Card Personalization Specification »)[12] et Contactless[13], permettant de couvrir les différentes technologies applicables aux transactions de proximité.

Les standards EMV s'appuient sur des normes ISO ou interbancaires[14] afin de permettre une offre ouverte et concurrentielle de la part des fournisseurs de cartes et de terminaux. Ils définissent l'ensemble des fonctionnalités et des procédures nécessaires au dialogue entre une carte et un terminal pour effectuer des transactions de paiement et de retrait. Ils précisent notamment les caractéristiques physiques, électriques et d'étanchéité entre applications que doivent respecter la carte et le terminal, les traitements à effectuer de part et d'autre, ainsi que les échanges de données entre la carte et le terminal pendant tout le déroulement de la transaction.

Concernant la sécurité des transactions, les standards EMV apportent 4 types d'améliorations :

– l'apport sécuritaire majeur est le renforcement important de la protection contre la fraude par contrefaçon de la piste magnétique, grâce à l'utilisation de la puce de la carte pour toutes les transactions de paiement et de retrait réalisées sur un terminal ou un automate conformes aux standards EMV ;

– le deuxième apport sécuritaire réside dans l'amélioration de la protection contre l'utilisation frauduleuse des cartes perdues ou volées, grâce à la généralisation (au niveau international) de l'usage du code confidentiel pour authentifier le porteur sur les terminaux EMV, que la transaction se déroule avec ou sans demande d'autorisation ;

– le troisième apport sécuritaire est l'amélioration de la gestion du risque porteur par l'émetteur (par exemple, pour déclencher une demande d'autorisation en fonction non seulement des caractéristiques de la transaction en cours, mais également des transactions précédentes enregistrées sur la carte). L'émetteur a en outre à sa disposition plusieurs méthodes d'authentification du porteur ; il a la possibilité de définir un ordre de priorité dans l'emploi de ces méthodes d'authentification en fonction des possibilités offertes par le terminal et du montant de la transaction ;

– le dernier apport sécuritaire réside dans l'enrichissement des services cryptographiques disponibles au niveau de la carte et du terminal pour valider la transaction, et dans le renforcement de la robustesse des mécanismes cryptographiques associés[15]. En France, l'une des différences majeures par rapport aux services cryptographiques disponibles sur les cartes de type B0' est la possibilité de réaliser une authentification dynamique « off-line » de la carte baptisée DDA (« Dynamic Data Authentication »). Les standards EMV prévoient en outre un second mécanisme, baptisé CDA (« Combined Data Authentication »), permettant une authentification « off-line » de la carte par le terminal à l'initiation de la transaction et durant la phase d'autorisation.

10 Plusieurs applications différentes (paiements domestiques, paiements internationaux, porte-monnaie électronique, programme de fidélisation, etc.) peuvent ainsi être présentes sur la même carte.

11 Description de spécifications fonctionnelles a minima devant être remplies par une application pour lui permettre d'être conforme à la norme EMV.

12 Spécifications liées au processus de personnalisation des cartes.

13 Déclinaison des normes EMV aux modes de paiement sans contact.

14 Telle que la norme intersectorielle ISO 7816 relative aux cartes à microprocesseur.

15 Les services cryptographiques définis par les standards EMV couvrent l'authentification « off-line » de la carte par le terminal, l'authentification du porteur, l'authentification « on-line » de la carte par l'émetteur lors d'une demande d'autorisation, l'authentification de l'émetteur par la carte lors de la réponse à une demande d'autorisation, la certification en intégrité et en authenticité de la transaction lors de sa finalisation et l'envoi de scripts sécurisés en intégrité et/ou confidentialité à la carte par l'émetteur en fin de transaction.

2 | STATISTIQUES DE FRAUDE POUR 2010

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 E du présent rapport. Une synthèse des statistiques pour 2010 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[16], transactions de proximité ou à distance, transactions de paiement ou 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 D 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 :

– 453,4 milliards d'euros de transactions réalisées en France et à l'étranger au moyen de 64,1 millions de cartes de type « interbancaire » émises en France (dont 1,74 million de porte-monnaie électroniques) ;

– 19,1 milliards d'euros de transactions réalisées (principalement en France) avec 24,4 millions de cartes de type « privatif » émises en France ;

– 25,7 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 ;

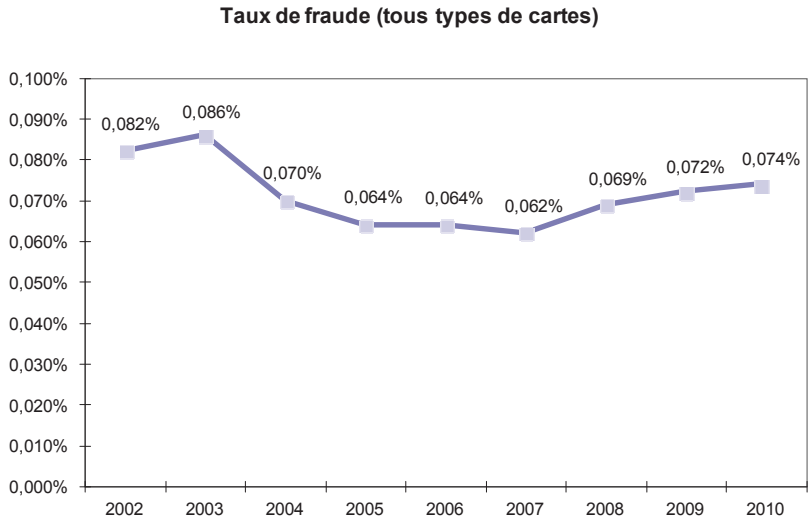
– des 130 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et de Visa Europe France ;

– des émetteurs du porte-monnaie électronique Moneo.

[16] Pour la première fois cette année, l'Observatoire est en mesure de distinguer parmi les transactions internationales celles qui sont réalisées au sein de la zone SEPA de celles qui le sont hors de la zone SEPA.

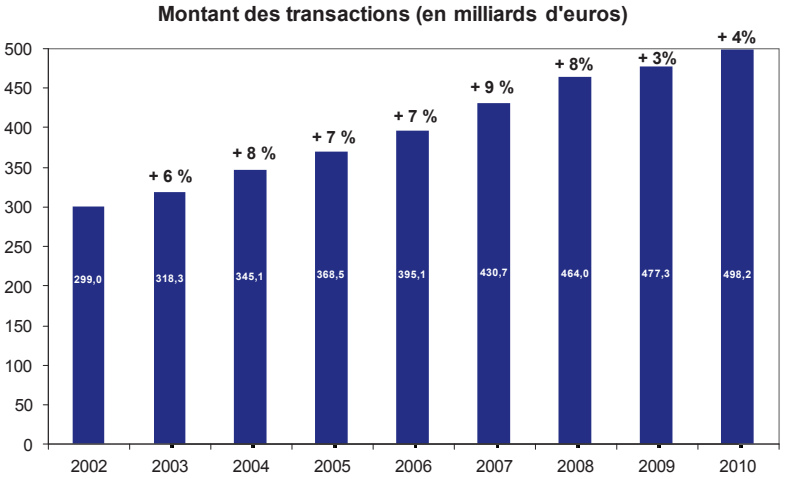
2|1 Vue d'ensemble

Le taux de fraude sur les paiements et les retraits par carte enregistré en 2010 dans les systèmes français est de 0,074 %, en légère augmentation comparé aux années précédentes. Le montant moyen d'une transaction frauduleuse est en baisse, à 122 euros contre 136 euros en 2009.



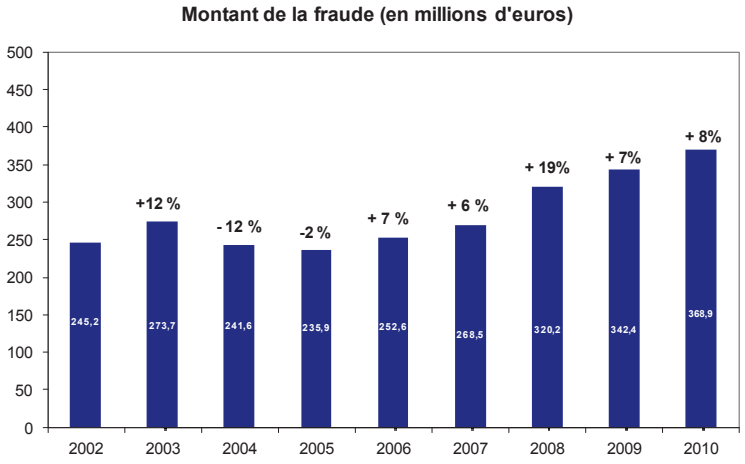
Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 3 – **Évolution du taux de fraude pour tous types de cartes**



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 4 – **Évolution du montant des transactions**



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 5 – **Évolution du montant de la fraude**

On observe une baisse du 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. Il s'établit en 2010 à 0,057 %, pour un montant de fraude de 269,3 millions d'euros (contre 0,059 % et 265,6 millions d'euros en 2009).

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 sensible. Il s'établit en 2010 à 0,055 %, pour un montant de fraude de 263 millions d'euros (contre 0,048 % en 2009, pour un montant de fraude de 220,8 millions d'euros).

L'annexe D du présent rapport regroupe des tableaux détaillés des volumes et valeurs de transaction et des volumes et valeurs de fraude, par type de carte, zone géographique, type de transaction et origine de fraude.

2|2 Répartition de la fraude par type de carte

Taux de fraude
(Montant de la fraude en millions d'euros)

	2006	2007	2008	2009	2010
Cartes de type « interbancaire »	0,065 % (237,0)	0,063 % (253,6)	0,070 % (304,3)	0,072 % (324,3)	**0,074 %** (351,5)
Cartes de type « privatif »	0,052 % (15,6)	0,052 % (15,0)	0,054 % (16,0)	0,068 % (18,2)	**0,080 %** (17,4)
Total	0,064 % (252,6)	0,062 % (268,5)	0,069 % (320,2)	0,072 % (342,4)	**0,074 %** (368,9)

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 6 – **Répartition de la fraude par type de carte**

Les taux de fraude sont en augmentation pour les deux types de cartes. Cette augmentation est plus forte pour les cartes de type « privatif » dont le taux de fraude dépasse celui des cartes de type « interbancaire » pour la première fois depuis 2006.

Pour les cartes de type « interbancaire », les taux de fraude émetteur et acquéreur sont respectivement de 0,057 % et de 0,055 % (contre 0,059 % et 0,048 % en 2009). La valeur moyenne d'une transaction frauduleuse est de 119 euros, contre 132 euros en 2009.

Pour les cartes de type « privatif », les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,063 % et à 0,068 % (contre 0,053 % et 0,059 % en 2009). La valeur moyenne d'une transaction frauduleuse s'élève à 353 euros en 2010, contre 324 euros en 2009.

2|3 Répartition de la fraude par zone géographique

	Taux de fraude (Montant de la fraude en millions d'euros)				
	2006	**2007**	**2008**	**2009**	**2010**
Transactions nationales	**0,031 % (109,6)**	**0,029 % (114,5)**	**0,031 % (130,9)**	**0,033 % (144,0)**	**0,036 % (163,8)**
Transactions internationales	**0,362 % (143,0)**	**0,368 % (154,0)**	**0,427 % (189,4)**	**0,449 % (198,4)**	**0,423 % (205,0)**
Dont émetteur français et acquéreur étranger[17]	0,453 % (76,4)	0,476 % (85,3)	0,594 % (118,3)	0,594 % (121,6)	0,728 % (54,9)
Dont émetteur français et acquéreur SEPA	-	-	-	-	0,331 % (50,6)
Dont émetteur étranger[18] **et acquéreur français**	0,295 % (66,5)	0,288 % (68,7)	0,291 % (71,0)	0,324 % (76,8)	0,831 % (64,5)
Dont émetteur SEPA et acquéreur français	-	-	-	-	0,195 % (35,0)
Total	**0,064 % (252,6)**	**0,062 % (268,5)**	**0,069 % (320,2)**	**0,072 % (342,4)**	**0,074 % (368,9)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 7 – **Répartition de la fraude par zone géographique**

La répartition de la fraude par zone géographique demeure marquée par un déséquilibre entre les transactions nationales et internationales : 56 % de la fraude portent sur les transactions internationales, alors que ce type de transaction compte à peine pour 10 % de la valeur des transactions par carte enregistrées dans les systèmes français.

Dans un contexte de croissance du montant des transactions nationales (+ 3,8 %), le taux de fraude de celles-ci est en légère hausse, mais demeure à un niveau très faible, à 0,036 % en 2010, contre 0,033 % en 2009.

Le montant de la fraude sur les transactions internationales augmente également en 2010. Mais, du fait d'une augmentation plus importante du montant des transactions, le taux de fraude est en baisse et revient à un niveau équivalent à celui de 2008. Cette baisse marque un changement de tendance après plusieurs années de hausse régulière. Dans le détail, le taux de fraude liée aux transactions effectuées à l'étranger avec des cartes émises en France est en baisse mais reste toujours très élevé à 0,462 % (contre 0,594 % en 2009), pour un montant de fraude de 105,5 millions d'euros (contre 121,6 millions d'euros en 2009). Le taux de fraude liée aux transactions effectuées en France avec des cartes émises à l'étranger est par contre en

17 A partir de 2010 : acquéreur hors SEPA uniquement.

18 A partir de 2010 : émetteur hors SEPA uniquement.

hausse et s'établit à 0,387 %, pour un montant de fraude de 99,5 millions d'euros (contre 0,324 % en 2009, pour un montant de fraude de 76,8 millions d'euros).

Il est possible cette année, pour la première fois, de comparer le taux de fraude des transactions internationales réalisées au sein de la zone SEPA avec celui des transactions réalisées hors de la zone SEPA. On note ainsi que le taux de fraude sur les transactions effectuées hors zone SEPA, avec des cartes émises en France, est plus de deux fois supérieur à celui des transactions effectuées au sein de la zone SEPA (0,728 % contre 0,331 %) et que le taux de fraude sur les transactions effectuées en France avec des cartes étrangères émises hors de la zone SEPA, est plus de quatre fois supérieur à celui des transactions effectuées avec des cartes étrangères émises dans la zone SEPA (0,831 % contre 0,195 %).

Ces bons résultats relatifs pour les transactions effectuées au sein de la zone SEPA sont certainement le bénéfice direct des efforts réalisés en Europe pour migrer les cartes et les terminaux de paiements vers le standard EMV (voir chapitre 4 | 3 – État d'avancement de la migration EMV).

Encadré 2 – Répartition du préjudice de la fraude

Depuis 2007, l'Observatoire fournissait, pour l'ensemble des systèmes de type « privatif » et de type « interbancaire », des indicateurs de la répartition du préjudice de la fraude entre le porteur, le commerçant et leurs banques. Cette année, les données fournies par les émetteurs et les accepteurs n'étant plus suffisamment significatives d'un point de vue statistique, l'Observatoire n'est pas en mesure de fournir ces indicateurs.

2 | 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 nationales des données internationales.

Transactions nationales

	Taux de fraude (Montant de la fraude en millions d'euros)				
Transactions nationales	**2006**	**2007**	**2008**	**2009**	**2010**
Paiements	**0,035 % (92,3)**	**0,032 % (95,6)**	**0,036 % (111,7)**	**0,038 % (123,2)**	**0,041 % (137,3)**
- dont paiements de proximité et sur automate	0,024 % (59,1)	0,017 % (45,4)	0,015 % (44,5)	0,014 % (41,0)	0,012 % (36,2)
- dont paiements à distance	0,199 % (33,2)	0,236 % (50,1)	0,252 % (67,2)	0,263 % (82,2)	0,262 % (101,1)
- dont par courrier / téléphone	0,194 % (19,8)	0,201 % (23,8)	0,280 % (28,5)	0,263 % (30,3)	0,231 % (27,3)
- dont sur Internet	0,208 % (13,4)	0,281 % (26,4)	0,235 % (38,8)	0,263 % (51,9)	0,276% (73,9)
Retraits	**0,019 % (17,4)**	**0,020 % (19,0)**	**0,018 % (19,1)**	**0,019 % (20,8)**	**0,024 % (26,5)**
Total	**0,031 % (109,6)**	**0,029 % (114,5)**	**0,031 % (130,9)**	**0,033 % (144,0)**	**0,036 % (163,8)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 8 – **Répartition de la fraude nationale par type de transaction**

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

– le taux de fraude sur les paiements de proximité et sur automate continue de diminuer et s'établit à 0,012 %. Les paiements de proximité et sur automate comptent pour 67 % du montant des transactions nationales, et pour seulement 22 % du montant de la fraude ;

– le taux de fraude sur les paiements à distance est stable en 2010 à 0,262 % mais il reflète deux tendances contraires : le taux de fraude sur les paiements par courrier et par téléphone est en baisse alors que le taux de fraude sur les paiements Internet continue d'augmenter pour se rapprocher de son maximum historique[19] de 2007. Les paiements à distance, qui représentent 8,6 % de la valeur des transactions nationales, comptent ainsi désormais pour 62 % du montant de la fraude (contre 57 % en 2009), dans un contexte de croissance toujours soutenue du volume et de la valeur de ces paiements (+ 23,8 % entre 2009 et 2010 en valeur). Le niveau très élevé de la fraude sur ce canal de paiement conduit l'Observatoire à renouveler son encouragement pour la mise en œuvre de mesures permettant de lutter contre cette tendance. Le rapport 2008 de l'Observatoire avait souligné l'importance de généraliser progressivement l'authentification du porteur pour tout acte de paiement et de renforcer les méthodes d'authentification utilisées. Des progrès ont été réalisés en ce sens (cf. chapitre 3), mais il apparaît crucial que les efforts engagés par l'ensemble des acteurs se poursuivent afin d'infléchir cette tendance ;

– le taux de fraude sur les retraits est en augmentation sensible mais reste inférieur à son maximum historique de 2004 (0,027 %). Les retraits représentent 25 % du montant des transactions nationales et comptent pour 16 % du montant de la fraude.

[19] L'Observatoire mesure le taux de fraude des paiements sur Internet depuis 2006.

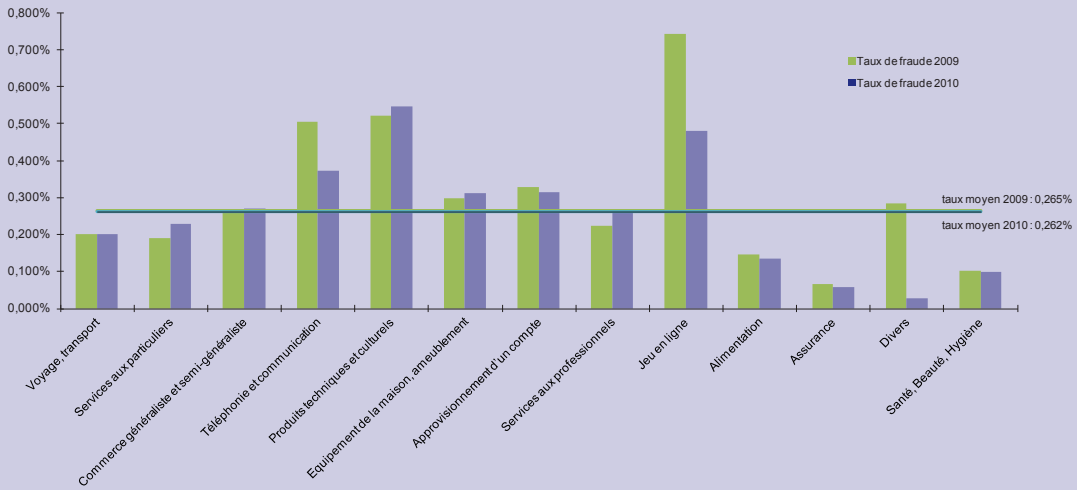
Encadré 3 – Fraude nationale en vente à distance selon le secteur d'activité

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.

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

Ventilation de la fraude sur les paiements à distance par secteur d'activité pour les transactions nationales

Les secteurs Voyage/transport, Services aux particuliers, Commerce généraliste et semi-généraliste et Téléphonie et communication représentent 69 % de la fraude, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Produits techniques et culturels, Jeu en ligne – le taux de fraude sur ce secteur ayant toutefois fortement baissé à 0,478 % contre 0,740 % en 2009) (cf. histogramme ci-après). Néanmoins, l'Observatoire remarque qu'au sein d'un même secteur, le taux de fraude varie sensiblement d'un commerçant à l'autre selon les mesures de sécurité déployées.



Taux de fraude sur les paiements à distance par secteur d'activité pour les transactions nationales

Source : Observatoire de la sécurité des cartes de paiement

Transactions internationales

	Taux de fraude (Montant de la fraude en millions d'euros)			
Émetteur français – Acquéreur étranger[20]	**2007**	**2008**	**2009**	**2010**
Paiements	**0,483 % (65,2)**	**0,655 % (99,3)**	**0,679 % (105,2)**	**0,795 % (39,8)**
- dont paiements de proximité et sur automate	0,299 % (30,0)	0,286 % (32,0)	0,406 % (44,7)	0,655 % (25,8)
- dont paiements à distance	1,024 % (35,1)	1,698 % (67,2)	1,350 % (60,5)	1,310 % (14,0)
- dont par courrier / téléphone	0,790 % (7,6)	1,284 % (11,2)	1,016 % (9,7)	1,193 % (3,8)
- dont sur Internet	1,117 % (27,4)	1,815 % (56,0)	1,440 % (50,8)	1,360 % (10,2)
Retraits	**0,455 % (20,0)**	**0,399 % (19,1)**	**0,331 % (16,5)**	**0,596 % (15,1)**
Total	**0,476 % (85,3)**	**0,594 % (118,3)**	**0,594 % (121,6)**	**0,728 % (54,9)**
Émetteur français – Acquéreur SEPA	**2007**	**2008**	**2009**	**2010**
Paiements	**–**	**–**	**–**	**0,396 % (49,1)**
- dont paiements de proximité et sur automate	**–**	**–**	**–**	0,112 % (9,2)
- dont paiements à distance	**–**	**–**	**–**	0,944 % (40 ,0)
- dont par courrier / téléphone	**–**	**–**	**–**	0,566 % (4,0)
- dont sur Internet	**–**	**–**	**–**	1,021 % (36,0)
Retraits	**–**	**–**	**–**	**0,052 % (1,5)**
Total	**–**	**–**	**–**	**0,331 % (50,6)**
Émetteur étranger[21] – Acquéreur français	**2007**	**2008**	**2009**	**2010**
Paiements	**0,334 % (62,8)**	**0,339 % (65,4)**	**0,397 % (74,1)**	**0,982 % (63,2)**
Retraits	**0,117 % (5,9)**	**0,110 % (5,6)**	**0,055 % (2,8)**	**0,103 % (1,4)**
Total	**0,288 % (68,7)**	**0,291 % (71,0)**	**0,324 % (76,8)**	**0,831 % (64,5)**
Émetteur SEPA – Acquéreur français	**2007**	**2008**	**2009**	**2010**
Paiements	**–**	**–**	**–**	**0,239 % (33,8)**
Retraits	**–**	**–**	**–**	**0,032 % (1,2)**
Total	**–**	**–**	**–**	**0,195 % (35,0)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 9 – **Répartition de la fraude internationale par type de transaction**

20 A partir de 2010 : acquéreur hors SEPA uniquement.

21 A partir de 2010 : émetteur hors SEPA uniquement.

En ce qui concerne les transactions internationales, l'Observatoire ne dispose d'une décomposition fine 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 (35,0 millions d'euros en 2010 contre 44,7 millions d'euros en 2009). Le taux de fraude sur les paiements de proximité réalisés par des cartes françaises dans la zone SEPA - où les points de vente ont pratiquement tous migrés à EMV - est presque six fois inférieur à celui des paiements de proximité effectués hors zone SEPA (0,112 % contre 0,655 %).

La fraude a légèrement diminué sur les paiements à distance (54,0 millions d'euros en 2010 contre 60,5 millions d'euros en 2009, soit un taux de 1,018 %). Néanmoins, on constate toujours un taux de fraude sur les paiements à distance particulièrement élevé (0,944 % dans la zone SEPA et 1,310 % hors zone SEPA, contre 1,350 % en 2009 pour l'étranger dans son ensemble) et beaucoup plus important que celui sur les paiements de proximité et sur automate. Le déploiement de dispositifs d'authentification renforcée devrait permettre de continuer à réduire la fraude sur les paiements à distance.

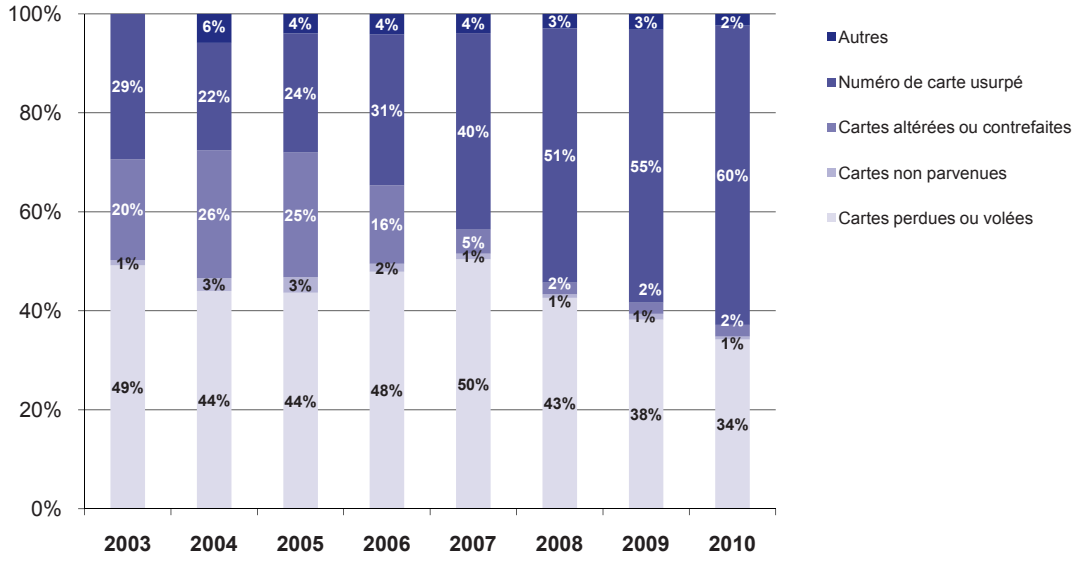
Enfin, on remarque une stabilisation de la fraude sur les retraits, après la forte baisse observée en 2009, qu'il s'agisse de transactions réalisées par des cartes françaises à l'étranger ou par des cartes étrangères en France.

2|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 à l'insu de son titulaire légitime, 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 indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements).



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 10 – **Répartition de la fraude selon son origine (transactions nationales, en valeur)**

En augmentation depuis 2005, l'origine de fraude la plus importante (60,5 %, contre 55,1 % en 2009) est celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance. La fraude liée aux pertes et vols de cartes représente encore 34,2 % des paiements nationaux frauduleux. La contrefaçon de cartes n'est à l'origine que de 2,4 % des paiements nationaux frauduleux.

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 50 %). Il faut toutefois noter que plusieurs émetteurs de cartes privatives ont déclaré cette année une forte hausse de la fraude par ouverture frauduleuse de compte, suite à la mise en place d'outils permettant de mieux détecter celle-ci (une partie de cette fraude étant auparavant non détectée et comptabilisée comme des impayés) et par conséquent de mieux la prévenir.

2010	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privatif »	
	Montant (millions d'euros)	Part	Montant (millions d'euros)	Part	Montant (millions d'euros)	Part
Carte perdue ou volée	56,0	34,2 %	54,7	35,1 %	1,3	16,6 %
Carte non parvenue	1,0	0,6 %	0,5	0,3 %	0,5	6,4 %
Carte altérée ou contrefaite	3,9	2,4 %	3,1	2,0 %	0,8	9,8 %
Numéro usurpé	99,0	60,5 %	97,5	62,6 %	1,6	19,4 %
Autres	3,9	2,4 %	-	-	3,9	47,9 %
Total	**163,8**	**100 %**	**155,7**	**100 %**	**8,1**	**100 %**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 11 – **Répartition de la fraude nationale selon son origine et par type de carte**

Encadré 4 – Indicateurs des services de police et de gendarmerie

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

Les attaques de distributeurs automatiques de billets (DAB) sont stables avec 527 piratages de DAB en 2010 (contre 526 en 2009[22], 427 en 2008, 391 en 2007, 515 en 2006, 200 en 2005 et 80 en 2004). A celles-ci s'ajoutent 6 attaques de distributeurs automatiques de carburant (DAC) (contre une seule en 2009) et 30 attaques de terminaux de paiement (contre 49 en 2009).

Face à de tels agissements, de nombreuses enquêtes ont été diligentées sur l'ensemble du territoire national. On peut distinguer parmi celles-ci :

– le démantèlement d'une équipe spécialisée dans la captation de données de carte, la contrefaçon et l'utilisation de cartes dans des commerces complices en France. Le préjudice établi s'élève à plus de 1 100 000 euros, les tentatives de fraude portant sur 4 600 000 euros ;

– l'interpellation d'une équipe spécialisée dans l'utilisation de cartes contrefaites d'origine chinoise. Les perquisitions ont permis de saisir 3 000 cartes contrefaites ainsi que du matériel utilisé pour la fraude. Le préjudice est estimé à plus de 430 000 euros ;

– le démantèlement d'un réseau chinois spécialisé dans la contrefaçon de cartes bancaires et l'achat de produits à forte valeur ajoutée. Huit personnes ont été interpellées et les perquisitions ont permis de saisir 1 000 cartes contrefaites. Le préjudice est estimé à plus de 380 000 euros ;

– l'interpellation d'une équipe roumaine de 13 personnes spécialisée dans la fraude à la carte bancaire par achat de paris sportifs en ligne. Le montant total du préjudice n'est pas encore évalué.

[22] Les données 2009 ont été consolidées et elles diffèrent par conséquent de celles publiées dans le rapport annuel 2009 de l'Observatoire (411 DAB et 18 TPE attaqués).

3 | ÉTAT DES LIEUX DE LA SÉCURISATION DES PAIEMENTS PAR CARTE SUR INTERNET

Afin de lutter contre la progression constante de la fraude sur les paiements à distance, qui représente en 2010 101,1 M€ (pour un taux de fraude de 0,262%), l'Observatoire a recommandé dans son rapport 2008 (chapitre 3.1) la généralisation progressive de l'authentification non rejouable du porteur pour les paiements sur Internet à chaque fois que cela était possible et pertinent, afin de permettre au commerçant d'être assuré de l'authenticité de la carte et du porteur, ainsi que du consentement de celui-ci.

Le présent chapitre vise dans un premier temps à présenter un état des lieux de la mise en œuvre de cette recommandation puis, dans un second temps, à restituer les résultats d'une étude menée auprès d'un panel de 1 000 cyberacheteurs afin de recueillir leur expérience relative à l'utilisation de dispositifs d'authentification non rejouable lors de paiements par carte sur Internet.

3|1 État des lieux de la sécurisation des paiements par carte sur Internet

Comme décrit dans le rapport annuel 2008 de l'Observatoire, l'authentification non rejouable des paiements par carte sur Internet nécessite d'une part, l'équipement du porteur en solutions techniques (code à usage unique généré par une calculette ou envoyé par SMS, lecteur autonome de carte EMV, etc.), dont le choix revient aux émetteurs de cartes, et d'autre part, le déploiement par le commerçant et sa banque acquéreur d'une architecture de mise en œuvre de l'authentification, comme par exemple le protocole « 3D-Secure » promu par plusieurs systèmes de paiement par carte.

L'équipement des porteurs de carte en solutions techniques d'authentification non rejouable a été généralisé en 2010

Conformément aux recommandations émises par l'Observatoire et reprises par le Gouverneur de la Banque de France, les banques émettant des cartes de paiement interbancaires ont, dans la grande majorité, achevé le déploiement des dispositifs d'authentification non rejouable auprès de leurs porteurs en juin 2010.

En ce qui concerne les solutions techniques déployées, le dispositif d'authentification par SMS est largement majoritaire, même si 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[23].

Si l'équipement des porteurs a donc été achevé en 2010, ces derniers n'ont pas encore pleinement appréhendé les modalités d'activation et de fonctionnement de ces nouveaux outils.

[23] On se reportera au rapport 2009 de l'Observatoire, chapitre 4 (p.51-52), pour une description plus complète de ces dispositifs d'authentification, ainsi que ci-dessous.

Ainsi, le taux d'activation[24] de ces dispositifs par les porteurs varie, en fonction de l'émetteur, entre 30 % et 85 % de la population totale des acheteurs en ligne. Cette situation contrastée s'explique notamment par la complexité plus ou moins élevée du processus d'activation proposé par l'émetteur. Un accompagnement des utilisateurs vers ces nouveaux dispositifs par tous les acteurs concernés reste ainsi nécessaire, comme le prouve par ailleurs les résultats de l'étude menée par l'Observatoire et présentés ci-après.

Le déploiement par les e-commerçants des dispositifs d'authentification reste limité mais devrait être plus visible en 2011

A ce jour, environ la moitié des commerçants en ligne est équipée d'architectures techniques, telles que « 3D-Secure », permettant l'authentification du porteur de carte lors du paiement. Pour autant, ces derniers ne représentent qu'environ 10 % des transactions par carte sur Internet en nombre et 15 % en valeur.

Constatant la désaffection des grands e-commerçants français au regard de ces dispositifs de sécurisation, l'Observatoire a mis en place en 2010 un groupe de travail spécifique en charge d'identifier les freins au déploiement de ces solutions en France.

Il ressort de ces travaux que les banques et les commerçants considèrent que cette technologie n'est pas à ce jour assez mature pour être généralisée, et qu'une démarche de mise en œuvre progressive et proportionnée, basée sur une approche par les risques, est à privilégier afin de lutter efficacement contre la fraude sans pénaliser le développement du commerce en ligne en France.

Des travaux ont par ailleurs été engagés avec l'ensemble des acteurs afin d'améliorer le taux de succès des transactions réalisées avec une authentification non rejouable et de mener des actions de communication auprès de l'ensemble des acteurs, notamment les consommateurs, afin de les sensibiliser à la sécurisation des paiements en ligne.

Dans ce contexte, on peut noter que plusieurs grands e-commerçants comme Air France et Orange Boutique ont déjà adopté le dispositif « 3D-Secure » et que Voyages-SNCF envisage son adoption pour une partie de ses transactions dès juillet 2011, ce qui devrait permettre une augmentation significative du taux de transactions par carte en ligne sécurisées par de l'authentification non rejouable.

On notera également qu'à cet horizon une offre proposée par l'établissement de paiement « Buyster » agréé en France, devrait également voir le jour et permettre la sécurisation par de l'authentification non rejouable[25].

Sur le plan européen, les recommandations émises par l'Observatoire dans son rapport 2008 ont été relayées par l'Eurosystème dans son 7ème rapport d'étape sur SEPA[26]. A ce titre, un forum européen sur la sécurité des moyens de paiement, réunissant les surveillants et superviseurs nationaux ainsi que des acteurs de marché le cas échéant, a été créé sous l'égide de la BCE (« Forum on SECUrity on REtail PAYments - SecuRe Pay ») et doit, parmi ses

[24] 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.

[25] Sauf lorsque l'utilisateur réalise l'opération depuis un téléphone mobile connecté en 3G.

[26] http://www.ecb.int/pub/pdf/other/singleeuropaymentsarea201010en.pdf : "market participants are encouraged to implement state-of-the-art measures for improving information security and preventing payment fraud. For remote payments, market participants are encouraged to introduce state-of-the-art authentication and migrate to it by the end of 2012. For "card-not-present" payments, secure payment protocols (e.g. "3D-secure" or virtual cards) should be used."

missions prioritaires, émettre des recommandations afin de sécuriser les paiements par carte sur Internet à l'échelle européenne.

3|2 L'expérience des cyberacheteurs français au regard des dispositifs d'authentification non rejouable

Dans la continuité des sondages effectués dans ses rapports précédents, l'Observatoire a souhaité cette année approfondir sa connaissance du ressenti des cyberacheteurs ayant été confrontés aux dispositifs d'authentification non rejouable lors d'un paiement par carte sur Internet.

Dans cette perspective, l'Observatoire a fait procéder à une étude quantitative menée par l'institut de sondage Harris Interactive. Cette étude a été réalisée par la mise en ligne sur Internet d'un questionnaire auprès d'un échantillon représentatif de 1 000 personnes âgées de 16 ans et plus résidant en France métropolitaine, contactées par Internet du 15 au 25 février 2011. Six dispositifs d'authentification ont été ainsi testés :

- la saisie de la date de naissance au moment d'effectuer un paiement ;
- le fait de devoir répondre à une question convenue au préalable avec la banque du porteur ;
- la saisie d'un code d'authentification envoyé par la banque par SMS sur le téléphone portable du porteur, ce code n'étant valable que pour un seul paiement ;
- la saisie d'un code d'authentification généré par un mini-lecteur de carte fourni par la banque du porteur. Sur ce lecteur, en insérant la carte de paiement et en tapant le code PIN associé, un code d'authentification valable pour un seul paiement est généré ;
- la saisie d'un code d'authentification généré par un dispositif électronique (« token ») fourni par la banque, ce code n'étant valable que pour un seul paiement ;
- l'utilisation d'une carte matricielle et d'un second code reçu par e-mail ou SMS, ce code n'étant valable que pour un seul paiement.

Les principaux résultats de cette étude sont résumés ci-après.

Les paiements par carte bancaire en ligne suscitent aujourd'hui peu d'inquiétude chez les cyberacheteurs

Seulement 23 % des cyberacheteurs interrogés déclarent éprouver de l'inquiétude lorsqu'ils effectuent un achat sur Internet avec leur carte bancaire, 3 % étant très inquiets et 20 % plutôt inquiets. A l'inverse, 77 % ne ressentent plutôt pas (55 %) ou pas du tout (22 %) d'inquiétude. Pour la majorité des personnes qui réalisent effectivement des achats sur Internet, cette démarche n'est donc pas associée à une prise de risque inconsidérée. Toutefois, pour une partie non négligeable d'entre eux, une légère appréhension peut subsister. Dans le détail, on constate que les femmes (29 %), les cyberacheteurs appartenant aux catégories populaires (28 %), ainsi que ceux dont les achats en ligne sont très occasionnels (moins de trois fois par an : 46 %), sont plus susceptibles de se sentir inquiets.

En revanche, **les personnes ayant déjà utilisé au moins un système d'authentification se montrent moins inquiètes que la moyenne** : elles ne sont que 19 % tous systèmes

confondus, et même 17 % en cas d'utilisation d'un système d'authentification forte[27], à se dire inquiètes contre 28 % des personnes n'ayant jamais utilisé le moindre dispositif d'authentification.

Une importante majorité de cyberacheteurs a connaissance de l'existence de dispositifs supplémentaires pour sécuriser les achats en ligne

Près de 8 cyberacheteurs sur 10 (79 %) indiquent avoir déjà entendu parler de dispositifs supplémentaires pour sécuriser les achats sur Internet. 58 % déclarent même « voir bien ce dont il s'agit », quand 21 % en ont une idée plus floue. La notoriété de ces dispositifs, dont l'existence est pourtant encore relativement récente, apparaît donc d'ores et déjà bien établie au sein de la population des cyberacheteurs.

La notoriété de ces dispositifs est plus élevée chez les cyberacheteurs de sexe masculin (83 %) et ceux appartenant aux catégories supérieures (84 %). A l'inverse, elle est un peu moins forte parmi les femmes (76 %), les catégories populaires (75 %) et surtout les cyberacheteurs les plus jeunes (69 % des 16-24 ans).

Logiquement, plus les personnes interrogées achètent en ligne, plus elles sont susceptibles d'avoir entendu parler des nouveaux dispositifs de sécurisation des achats en ligne et de savoir en quoi cela consiste. Ainsi, le taux de notoriété passe de 62 % parmi les cyberacheteurs très occasionnels à 86 % chez ceux qui effectuent au moins un achat par mois.

Pour autant, seuls 4 cyberacheteurs sur 10 (39 %) répondent par l'affirmative à la question « Avez-vous reçu une information de la part de votre / vos établissement(s) bancaire(s) concernant des dispositifs supplémentaires pour sécuriser les achats sur Internet ? ». Cette proportion monte à 54 % parmi ceux qui ont déjà fait face à un tel dispositif, et même 64 % en cas de confrontation à un dispositif d'authentification forte. En revanche, elle reste inférieure à 50 % parmi les cyberacheteurs fréquents (44 % lorsque l'individu réalise plusieurs achats en ligne par mois, 43 % lorsqu'il en effectue en moyenne un par mois) et descend même à 27 % parmi les cyberacheteurs âgés de 16 à 24 ans. Ceux qui déclarent avoir reçu une information l'ont jugée claire pour les aider à sécuriser leurs achats sur Internet à hauteur de 84 % (33 % très claire et 51 % plutôt claire). Seuls 15 % déplorent à l'inverse son relatif manque de clarté.

Des dispositifs jugés faciles à utiliser mais qui engendrent des difficultés lors de la première utilisation

Des dispositifs jugés très majoritairement faciles à utiliser

Seuls 8 % des utilisateurs déclarent trouver au moins un des dispositifs difficile à utiliser, 10 % lorsque l'on se concentre sur les dispositifs d'authentification forte. Ce sont les mini-lecteurs de carte et les cartes matricielles qui sont perçus comme les moins faciles à utiliser, mais la proportion de personnes qui déplorent une difficulté d'utilisation reste très faible (11 % dans les deux cas). Seuls 7 % des personnes qui ont déjà été confrontées à la saisie d'un code unique par SMS jugent ce dispositif difficile à utiliser. Concernant les trois

[27] Sont considérés comme systèmes d'authentification forte ceux nécessitant la saisie d'un code non-rejouable, à savoir le code envoyé par SMS, la carte matricielle associée à un code envoyé par un autre canal, le token ainsi que le mini-lecteur de cartes.

derniers dispositifs, les difficultés perçues sont très faibles (proportion inférieure ou égale à 5 %). On n'observe pas de catégorie d'utilisateurs qui serait particulièrement déstabilisée.

Près d'un utilisateur sur cinq a néanmoins rencontré des difficultés lors de sa première utilisation d'un dispositif d'authentification forte

36 % des utilisateurs d'un mini-lecteur de carte font état de difficultés lors de la première utilisation, 16 % des utilisateurs d'une carte matricielle, 14 % des utilisateurs d'un code reçu par SMS et 8 % des utilisateurs d'un token. **Au global, c'est donc environ un utilisateur sur cinq (19 %) qui a éprouvé des difficultés lors de l'utilisation initiale d'un dispositif d'authentification forte**. Peu de difficultés sont mentionnées pour le fait de devoir répondre à une question secrète ou de saisir sa date de naissance au moment du paiement (respectivement 6 % et 5 % des utilisateurs).

Ces difficultés **sont d'ordres multiples et peuvent intervenir à différents moments** : 27 % des personnes ayant rencontré des difficultés ont eu du mal à comprendre le mode de fonctionnement du dispositif, 26 % à y accéder, 28 % à l'activer ou procéder à l'enregistrement des données ou encore 24 % au moment même de l'utiliser. 21 % font également mention d'autres difficultés qui tiennent davantage à l'implication dans le dispositif d'un objet matériel : batterie de téléphone portable déchargée, changement de numéro non signalé à la banque, impossibilité de retrouver chez soi la carte matricielle…

Un accompagnement des utilisateurs vers ces nouveaux dispositifs par tous les acteurs concernés reste donc nécessaire. **Parmi les acteurs perçus comme les plus pertinents pour communiquer** sur ces nouveaux dispositifs, **les banques** sont identifiées comme les acteurs devant prendre la parole sur ce sujet **(74 %)**, devant **les sites commerçants (43 %), les associations de consommateurs (24 %)** et les pouvoirs publics (16 %). Seuls 10 % expriment clairement ne pas vouloir de communication à ce sujet.

Au final, **environ un tiers des personnes qui a fait face à de telles difficultés (31 %) n'a pas pu ou su finaliser son achat**. Ramené à la population des utilisateurs d'au moins un dispositif (15 %), cela représente donc un peu moins de 5 % des utilisateurs qui ont renoncé à leur achat lors de la première confrontation à ce type de dispositif. Il est à noter qu'environ 4 personnes sur 5 n'ayant pu finaliser leur premier achat (82% pour l'utilisation du dispositif par SMS) ont réitéré par la suite au moins une transaction avec authentification.

Une partie des difficultés disparaît lors des utilisations ultérieures

Si l'on s'intéresse maintenant aux difficultés persistantes, qui se sont manifestées lors des utilisations suivantes, **la proportion de personnes ayant de nouveau fait face à des difficultés chute à 6 % des utilisateurs, 7 % pour les dispositifs d'authentification forte**. Dans un contexte où la majorité des utilisateurs interrogés a bien réitéré son usage du dispositif, on observe donc que la proportion de personnes ayant rencontré des difficultés est plus que divisée par deux entre la première utilisation et les suivantes.

Encore une fois, c'est le mini-lecteur de carte qui pose le plus de problèmes (11 %) devant la carte matricielle (6 %) et le code reçu par SMS (5 %). La proportion de personnes ayant eu des difficultés lors des utilisations suivantes est donc relativement faible dans l'échantillon considéré et on observe comme pour la question précédente que ces difficultés correspondent plus à des difficultés matérielles ou humaines (oubli de la question secrète, numéro de téléphone non enregistré ou incorrect, SMS reçu trop tardivement…) qu'à des problèmes ayant trait

véritablement aux dispositifs. Très peu d'utilisateurs mentionnent en effet des codes invalides ou des dispositifs défaillants.

Toutefois, lorsque les difficultés persistent, les individus ont davantage tendance à ne pas finaliser l'achat : 44 % contre 31 % dans le cas de difficultés liées à la première utilisation. Cela représente un peu moins de 3 % des utilisateurs.

3|3 Des dispositifs qui renforcent la sécurité et qui ne pénaliseraient pas les ventes en ligne

Une sécurité jugée renforcée, surtout par les dispositifs non-rejouables

Si les répondants estiment peu gênant le délai supplémentaire entraîné par ces nouveaux dispositifs, c'est sans doute parce que le rapport désagrément/sécurité est perçu comme positif. En effet, **les utilisateurs ont majoritairement le sentiment que ces dispositifs renforcent significativement la sécurité des paiements par carte bancaire sur Internet, et particulièrement les dispositifs impliquant la saisie d'un code unique**.

En première position, on trouve le dispositif d'authentification forte le moins répandu, à savoir **le token** : 97 % des utilisateurs de ce dispositif estiment que cela renforce la sécurité du paiement, dont 73 % beaucoup. En deuxième position, on trouve au contraire le dispositif le plus répandu, **la saisie d'un code unique reçu par SMS** : 94 % des utilisateurs estiment que la sécurité est confortée par ce dispositif, dont 53 % beaucoup. Viennent ensuite juste derrière **la carte matricielle** (93 %, dont 55 % beaucoup) et **le mini-lecteur de carte** (91 %, dont 56 % beaucoup). Les dispositifs d'authentification 'faibles' se traduisant par la saisie d'une information personnelle rassurent moins d'utilisateurs et les rassurent moins fortement : ainsi 75 % des personnes ayant déjà dû répondre à **une question secrète** lors d'un paiement en ligne ont le sentiment que cela accroît la sécurité, et seulement 23 % beaucoup. La saisie de la date de naissance ne rassure qu'un utilisateur sur deux (51 %) et seulement un sur dix beaucoup (10 %).

Au global, sur la base de l'ensemble des utilisateurs, **86 % ont le sentiment que la sécurité est renforcée par au moins un de ces dispositifs et même 96 % quand on restreint le champ aux dispositifs non-rejouables**. Ce sentiment de sécurité renforcée est majoritairement partagé par toutes les catégories de population, même s'il est un peu plus faible chez les 16-34 ans (81 %) et les cyberacheteurs occasionnels (82 %) dont l'inquiétude concernant les achats en ligne est plus forte à la base.

Ainsi, **76 % des utilisateurs disent se sentir plus en sécurité lorsqu'ils effectuent leurs achats en ligne avec ces nouveaux dispositifs**. Cette proportion monte même à 83 % parmi les personnes ayant déjà utilisé au moins un des 4 dispositifs d'authentification forte testés. Notons également que les acheteurs fréquents sont plus susceptibles de se dire plus en sécurité que les acheteurs occasionnels. En outre, ces dispositifs sont plus susceptibles de rassurer les utilisateurs peu inquiets que ceux qui éprouvent de l'inquiétude lorsqu'ils réalisent un achat par carte bancaire en ligne.

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

Ces dispositifs vont-ils favoriser ou non le développement des transactions en ligne ? **Pour près de 8 utilisateurs sur 10, cela ne va pas changer leur comportement en matière d'achats sur Internet**, ils continueront à acheter ni plus, ni moins. En revanche, **19 % déclarent que ces nouveaux dispositifs sont susceptibles de les amener à acheter davantage sur Internet**. Ce sont avant tout les utilisateurs qui achètent déjà beaucoup en ligne qui anticipent cet effet positif : 24 % des personnes qui effectuent déjà au moins un achat en ligne par semaine et 23 % de celles qui réalisent 2 ou 3 achats par mois.

A l'inverse, seuls 2 % (5 % des 16-24 ans) estiment que cela aura tendance à les dissuader d'acheter en ligne, 1 % déclarant qu'ils achèteront moins et 1 % qu'ils n'achèteront plus du tout.

Les utilisateurs déclarent majoritairement qu'à l'avenir ils porteront attention à la présence ou non d'un tel dispositif lors de leurs achats par carte bancaire en ligne. Ainsi, **17 % déclarent qu'ils feront leurs achats exclusivement sur des sites d'e-commerce présentant un tel dispositif et 54 % qu'ils les favoriseront, même s'ils pourront continuer à acheter sur un site n'en proposant pas**. 28 % en revanche n'y feront pas particulièrement attention.

Cela confirme les résultats de la question précédente : ces dispositifs ne dissuadent pas les cyberacheteurs potentiels et peuvent même apparaître comme un argument susceptible de se distinguer positivement. Dans le détail, on observe que l'attitude qui consiste à déclarer que les achats futurs se feront seulement sur les sites ainsi sécurisés concerne plutôt les catégories populaires (20 %) et les acheteurs occasionnels (29 % en cas de 3-4 achats par an et 38 % en cas d'achats moins fréquents) ainsi que les utilisateurs de la carte matricielle, du token ou du mini-lecteur de carte (respectivement 24 %, 37 % et 28 %). La deuxième attitude, qui consiste à les favoriser sans être exclusif, est davantage citée par les acheteurs très fréquents (65 %). Quant à l'attitude consistant à ne pas prêter attention à ces dispositifs, elle est surtout le fait des plus jeunes (44 % des 16-24 ans), des CSP+[28] (32 %), des Franciliens (33 %) ou encore des personnes qui ont eu recours à la saisie de la date de naissance (32 %).

Les cyberacheteurs les plus fréquents sont moins nombreux que la moyenne à envisager de se restreindre aux seuls sites présentant ces dispositifs d'authentification (8 % et 12 % contre 29 % et 38 % pour les cyberacheteurs plus occasionnels).

3|4 Conclusion

Un peu moins d'un an après le déploiement généralisé des dispositifs d'authentification non rejouable auprès des porteurs de carte, l'Observatoire constate que la fraude sur les paiements par carte à distance reste élevée et que la mise en œuvre des solutions d'authentification par les commerçants en ligne rencontre des difficultés.

Dans ce contexte, l'Observatoire recommande une mise en œuvre progressive et proportionnée, basée sur une approche par les risques, de l'authentification non rejouable du porteur pour les paiements sur Internet afin de lutter efficacement contre la fraude sans pénaliser le développement du commerce en ligne en France.

[28] Catégorie socio-professionnelle

L'Observatoire poursuivra par ailleurs ses travaux avec l'ensemble des acteurs concernés afin d'améliorer le taux de succès des transactions réalisées avec une authentification non rejouable et mener des actions de communication auprès de l'ensemble des acteurs, notamment les consommateurs, afin de les sensibiliser à la sécurisation des paiements en ligne. En la matière, les établissements bancaires sont perçus par les utilisateurs comme les plus à même, devant les e-commerçants, à les accompagner.

L'Observatoire se félicite de la migration de plusieurs grands e-commerçants comme Air France, Orange Boutique et Voyages-SNCF (dès juillet 2011 pour les transactions les plus risquées) vers des dispositifs d'authentification des paiements par carte, qui devrait permettre une augmentation significative du taux de transactions sécurisées par de l'authentification non rejouable et une baisse de la fraude en la matière pour les années à venir.

L'Observatoire salue par ailleurs la création, sous l'égide de la Banque Centrale Européenne, du forum européen sur la sécurité des moyens de paiement (« Forum on SECUrity on REtail PAYments – SecuRe Pay »), qui devra notamment permettre d'assurer la sécurisation des paiements par carte sur Internet à l'échelle européenne.

L'Observatoire constate enfin que l'expérience des cyberacheteurs au regard des dispositifs de sécurisation est globalement positive puisque 8 cyberacheteurs sur 10 indiquent en avoir déjà entendu parler, que 96 % d'entre eux estiment que les dispositifs d'authentification non rejouable présentés renforcent la sécurité des paiements par carte sur Internet, sans pénaliser a priori l'acte d'achat pour 80 % d'entre eux. Pour autant, des efforts restent à fournir pour limiter les difficultés engendrées lors de leur utilisation et les cas où l'acte d'achat ne peut être finalisé.

4 | VEILLE TECHNOLOGIQUE

4|1 Standardisation européenne et sécurité dans le domaine des cartes de paiement

Le Conseil européen des paiements (European Payments Council – *EPC*[29]) est l'organisme représentatif de l'industrie bancaire chargé du développement et de la promotion des instruments SEPA, parmi lesquels la carte occupe une place privilégiée. Les processus d'harmonisation des instruments SEPA ont toutefois suivi des voies différentes : pour les prélèvements et virements, ils ont conduit à la création de nouveaux instruments (*SDD* et *SCT*) au sein de systèmes spécifiés par l'EPC et auxquels doivent adhérer les banques européennes ; pour les cartes, l'objectif poursuivi par l'EPC est la définition de règles et principes permettant aux cartes de paiement émises au sein de la zone SEPA d'y être acceptées dans les mêmes conditions, indifféremment du lieu. Ces règles et principes constituent le « *SEPA Cards Framework* » et font l'objet de déclinaisons techniques dans le « *SEPA Cards Standardisation Volume - Book of Requirements* ».

Depuis la publication du « *SEPA Cards Framework* » en 2005, l'Observatoire a régulièrement souligné l'importance qu'il attache à la conduite d'une démarche harmonisée de standardisation et de certification au sein de l'espace SEPA. Les travaux réalisés dans ce cadre ont progressé depuis le dernier état d'avancement figurant dans le rapport 2007, et ce dans chacun des domaines d'interaction entre les parties lors d'une transaction par carte.

Le paiement par carte implique en effet de nombreux acteurs (porteurs, commerçants, prestataires techniques, établissements financiers et éventuellement systèmes d'échange), qui doivent être capables de s'échanger les différentes données de la transaction. Ces échanges requièrent une standardisation des matériels et des protocoles de communication au sein du système de paiement par carte : la carte, le terminal et les serveurs de l'acquéreur et de l'émetteur.

Les bénéfices attendus d'une telle démarche résident de manière générale dans une simplification des moyens techniques à mettre en œuvre pour l'ensemble des acteurs des systèmes de paiement par carte, ainsi que dans une interopérabilité accrue entre les différents systèmes existants. Cette étude présente un nouvel état des lieux des initiatives en cours visant à atteindre ces objectifs, en élargissant le champ des investigations aux paiements à distance ou réalisés en mode sans contact, ainsi qu'aux modalités de protection des données dans la filière acquisition.

[29] Les termes en italiques sont définis dans le glossaire, p.50-51.

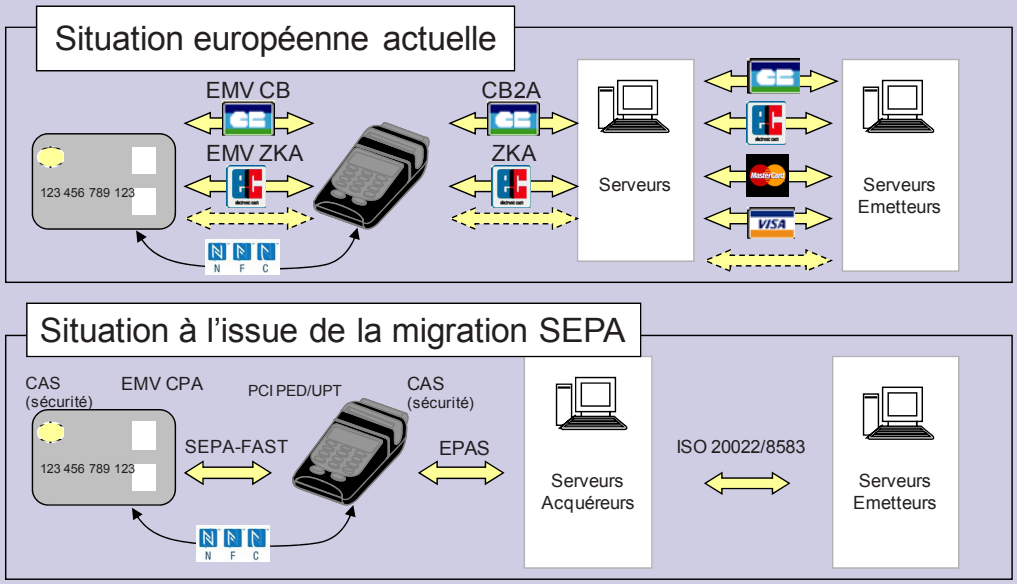
La sécurisation dans le cadre d'un paiement par carte de proximité

Encadré 5 : Évolution des standards techniques avec l'émergence de SEPA

La situation européenne actuelle est similaire à celle déjà observée en 2007, marquée par un cloisonnement des systèmes de carte de type interbancaire. Les paiements par carte transfrontaliers reposent donc sur les réseaux internationaux, même si des accords d'acceptation peuvent toutefois déjà exister entre deux systèmes nationaux.

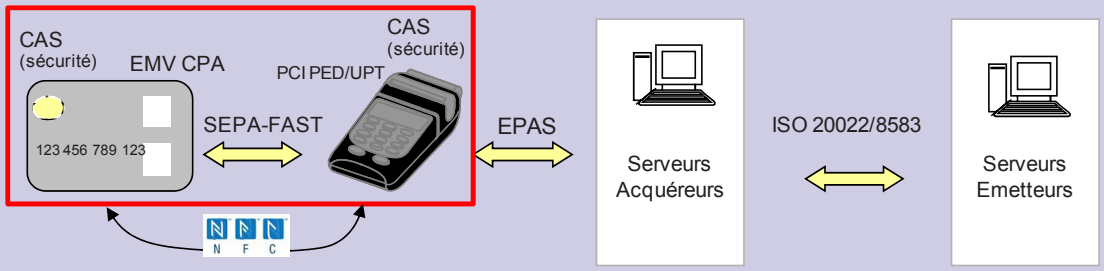
Ce cloisonnement se retrouve au niveau des protocoles d'échanges (entre la carte et le terminal, le terminal et les serveurs de l'acquéreur, ainsi qu'entre les serveurs de l'acquéreur et de l'émetteur), une même norme pouvant être implémentée de différentes façons selon les systèmes (cas de la norme *EMV*).

Les travaux de standardisation européens doivent conduire à l'adoption de spécifications communes sur l'ensemble de ces phases du paiement par carte, comme le rappelle le schéma ci-dessous :



Les travaux de standardisation dont il est fait référence ci-dessous étaient déjà initiés lors de la précédente étude conduite par l'Observatoire[30]. Le lecteur est donc invité à se reporter à cette dernière pour toute question relative au descriptif technique des normes concernées.

La standardisation de l'interface carte – terminal



30 Cf. chapitre 3.1 (p. 27) « Sécurité des paiements par carte et standardisation européenne », rapport 2007.

Il s'agit ici de répondre aux besoins de standardisation à la fois des spécifications propres à la carte et au terminal, ainsi qu'aux échanges entre ces deux éléments de façon à permettre l'acceptation des cartes sur l'ensemble des terminaux de la zone SEPA. Toutefois, les mêmes cartes devant rester compatibles avec les terminaux utilisés en dehors de cette zone, l'EPC a retenu comme base normative dès 2005 les spécifications techniques EMV, produites par un consortium réunissant les plus grands systèmes de carte internationaux[31][32].

- *Pour les cartes :*

Les cartes à piste répondent à la norme ISO 7811, laquelle définit les spécifications de la bande magnétique, son positionnement sur la carte, la technique de codage ainsi que les propriétés des caractères codés.

Concernant les cartes à puce, les standards EMV comprennent un certain nombre de dispositifs optionnels, pouvant conduire à des modalités de mise en œuvre différentes d'un système de carte à l'autre. Le « *CIR Technical Working Group* »[33] a donc travaillé dès 2003 sur un socle commun applicable à la zone SEPA, conduisant EMVCo à publier en 2005 un document reprenant les spécifications minimales requises pour le paiement en mode EMV (*CPA - Common Payment Application*). Si les cartes françaises « CB » ne sont pas aujourd'hui compatibles avec ces spécifications, les terminaux « CB » les implémentent d'ores et déjà.

- *Pour les téléphones mobiles :*

Le mode d'initiation des paiements par téléphone mobile, lors d'un paiement de proximité (ou à distance, en devenir) fait l'objet de réflexions plus récentes. Il nécessite néanmoins un niveau de sécurité équivalent à celui prévalant pour les paiements initiés à l'aide d'une carte, en tenant compte des spécificités propres à cet instrument. Différentes initiatives visent ainsi à définir un socle de sécurité pour les différents éléments constitutifs d'un téléphone mobile impliqués dans une transaction de paiement ainsi que pour les communications entre cet appareil et les infrastructures de la chaîne de paiement.

L'EPC, dont l'objectif est de publier un guide d'interopérabilité pour les transactions à distance (« *SEPA Interoperability Implementation Guidelines for Remote Card Payments* »), a ainsi signé des accords de coopération avec *GSMA* (voir ci-dessous), *Mobeyforum*, *GlobalPlatform* et l'Association Européenne Payez Mobile (*AEPM*), afin d'harmoniser les pratiques sécuritaires relatives à ce mode d'initiation des paiements par carte. Ces initiatives ont jusqu'à présent permis la publication par l'EPC d'un livre blanc sur les paiements mobiles attestant de son implication dans ce domaine[34]. Le processus de standardisation a par ailleurs démarré, notamment en ce qui concerne la gestion d'applications de paiement sur la carte *SIM* ou encore la définition d'un environnement sécurisé pour celle-ci[35].

- *Pour les terminaux :*

---

31 EMVCo regroupe American Express, JCB, Mastercard et Visa.

32 La Direction Générale de la Concurrence de la Commission européenne a ouvert une enquête sur le caractère potentiellement anticoncurrentiel de ce choix.

33 Le CIR-TWG (« Common Implementation Recommendations – Technical Working Group ») est un groupe de travail constitué d'utilisateurs européens d'EMV.

34 Ce document est publié sur le site internet de l'EPC (http://www.europeanpaymentscouncil.eu) et sera amendé courant 2011 pour y inclure une analyse plus détaillée sur les paiements mobiles à distance.

35 Le profil de protection pour la carte SIM publié fin 2010, résultant des travaux de l'AEPM, repose sur la méthodologie dite des « Critères Communs » (cf. rapport de l'Observatoire 2008, encadré 12 p. 49), avec un niveau de sécurité élevé (EAL4+).

Le groupe *CIR-TWG* a également formulé des spécifications fonctionnelles relatives à la sécurité des terminaux, les « *SEPA Financial Application Specifications for SCF Compliant EMV Terminals* » (*SEPA FAST*). Ces spécifications comportent un modèle unique de déroulement de transaction ainsi que des règles d'affichage communes et des messages uniformisés. Elles se déclinent en trois parties, relatives respectivement aux terminaux de paiement, aux automates et aux DAB. La première partie a été finalisée en 2010 et est en cours de révision afin d'y intégrer les paiements sans contact. La seconde partie est actuellement en cours de rédaction, alors que la dernière n'a pas encore commencé.

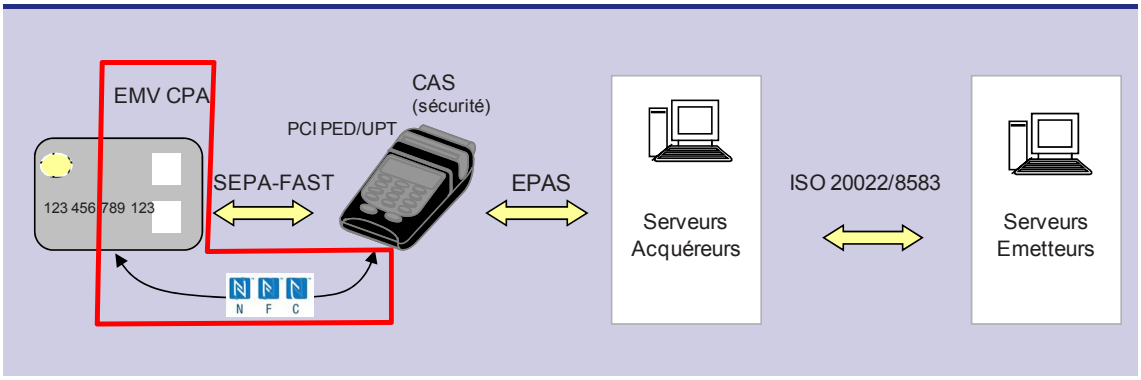
Les systèmes de carte internationaux imposent en outre le respect des règles *PCI PED* (*Payment Card Industry – PIN Entry Device*) et *PCI UPT* (*PCI - Unattended Payment Terminal*) aux fabricants de terminaux et automates[36]. En raison des nombreux accords de co-badgeage[37] existant entre ces systèmes et les systèmes nationaux (comme c'est le cas en France pour les cartes émises par les membres du Groupement des Cartes Bancaires « CB »), ces règles édictées par PCI SSC (cf. p.47) ont de fait acquis le caractère de standards. Elles visent à s'assurer que le niveau de protection physique et logique des appareils est propre à garantir un haut niveau de sécurité pour les données traitées par ces derniers.

L'Observatoire note que le groupe *ERIDANE*[38], qui était en charge de l'élaboration des spécifications relatives aux différents composants des matériels d'acceptation (claviers, écrans, lecteurs, logiciels…) a arrêté ses travaux depuis la parution du rapport 2007, ceux-ci n'étant à ce jour repris par aucune autre initiative.

* * *

Le groupe *CAS (« Common Approval Scheme »)*[39] a enfin défini des exigences de sécurité minimales pour les cartes et terminaux de façon à harmoniser les pratiques au sein de la zone SEPA et permettre la mise en œuvre du futur cadre de certification européen harmonisé (cf. § 4). Ces exigences ont été reprises par l'EPC et intégrées dans le « *SEPA Cards Standardisation Volume – Book of Requirements* »[40] dans une version 5.5 actuellement en préparation.

- *Pour les échanges en mode sans contact*



36 Cf. chapitre 1 (p. 9) « Les mesures de sécurité PCI sont-elles adaptées au marché français», rapport 2009.

37 Le co-badgeage consiste à apposer sur les cartes les logos de systèmes de carte partenaires.

38 ERIDANE rassemblait des systèmes de paiement par carte européens, des fabricants de terminaux et des commerçants.

39 CAS réunit les principaux systèmes de cartes européens et internationaux.

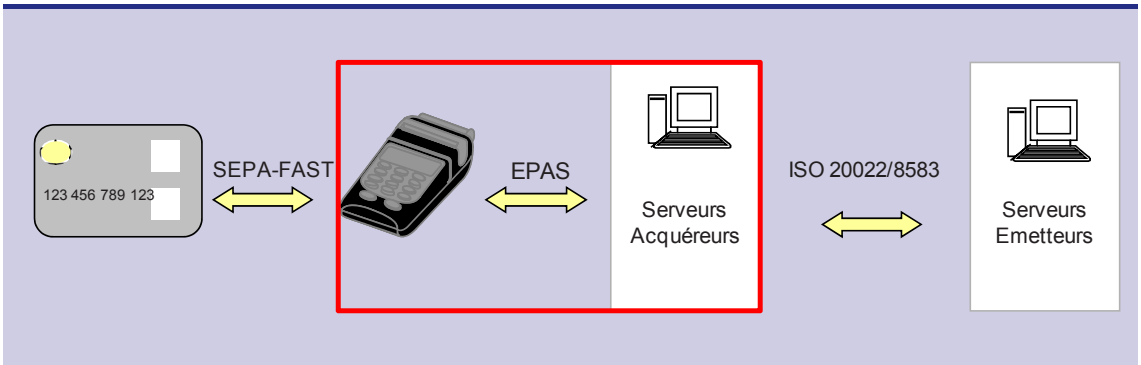
40 Document rédigé par l'EPC, basé sur le *SEPA Cards Framework* et définissant des exigences fonctionnelles et de sécurité applicables aux cartes et terminaux.

Les paiements en mode sans contact, qu'ils soient initiés par une carte ou un téléphone mobile, sont majoritairement réalisés selon la technologie NFC (« Near Field Communication »), qui s'est imposée ces dernières années sur le marché des communications sans fil à courte portée par sa compatibilité avec les appareils déployés notamment dans le secteur des transports, et sa reconnaissance par les organismes internationaux normatifs tels l'ISO ou *l'ETSI* (*European Telecommunications Standard Institute*).

Les échanges en mode sans contact sont en outre encadrés par des normes similaires à celles en vigueur pour les paiements en mode contact, dont elles sont issues. Ainsi, EMVCo a diffusé en 2005 et actualisé en 2007 le standard « *EMV Contactless Specifications for Payment Systems, EMV Contactless Communication Protocol Specification* » décrivant les fonctionnalités minimales requises pour les cartes et terminaux dans le cadre d'une transaction sans contact, indépendamment cependant de l'application utilisée, qui demeure quant à elle sous la responsabilité des systèmes de carte.

Enfin, l'EPC a plus récemment conclu un accord avec la GSM Association (GSMA), conduisant à la rédaction d'un document commun décrivant les rôles des différents acteurs impliqués dans la délivrance et la gestion du cycle de vie d'une application de paiement stockée sur la carte *SIM* d'un téléphone mobile, ainsi que les processus y afférents.

La standardisation de l'interface terminal – acquéreur



La standardisation du domaine terminal – acquéreur est un élément important dans le cadre de SEPA car elle représente un pré-requis à la liberté offerte aux commerçants de choisir le processeur de leur choix pour les opérations concernées (autorisation et acquisition de transactions, gestion du terminal, etc.).

Chaque système de carte peut actuellement utiliser un protocole propriétaire (cas de « *CB2A* » élaboré par « Cartes Bancaires »), qui bien que reposant sur une norme internationale (ISO 8583[41], limitée aux communications acquéreur – émetteur mais utilisée par extension pour les communications terminal – acquéreur) ne permet pas de garantir une interopérabilité totale au sein de la zone SEPA. Le consortium *EPAS* (*Electronic Protocol Application Software*) a été constitué afin de remédier à cette situation et de mettre au point un protocole homonyme sur la base de la norme ISO 20022[42] encadrant l'échange de messages financiers. Le développement d'EPAS a été scindé en différentes phases : les spécifications relatives aux terminaux (protection des données lors des transferts) sont en cours de rédaction, celles couvrant les systèmes des commerçants (séparation des opérations d'achat et de paiement) sont en cours d'adaptation afin de prendre en compte le contexte du marché nord-américain. Enfin, les

41 Spécifications d'échange de messages initiés par cartes de transaction financière.

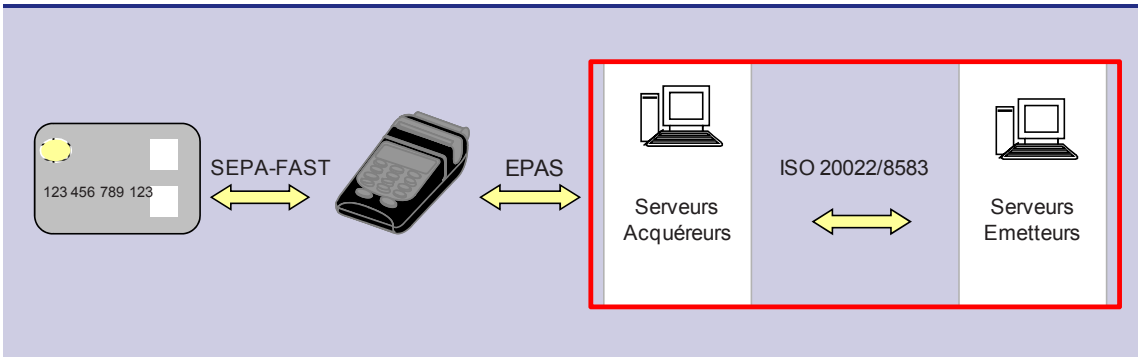
42 La norme ISO 20022 est aussi appelée « UNIFI » - UNIversal Financial Industry message scheme.

spécifications relatives au protocole de communication lui-même entre accepteurs et acquéreurs sont en cours de publication à l'ISO.

* * *

Les travaux réalisés par le groupe *CIR* ainsi que par *EPAS*, qui ont conduit à la publication des normes *SEPA FAST* (1ère partie) et *EPAS*, feront l'objet d'un test opérationnel dans le cadre du projet « *OSCAR* » (*Open Standards for Cards*). Ce projet est actuellement en phase préparatoire et devrait associer des représentants de l'ensemble des filières d'acceptation et d'acquisition.

La standardisation de l'interface acquéreur – émetteur



Les communications entre les serveurs des émetteurs et des acquéreurs représentent le dernier maillon de la chaîne de paiement sur lequel subsistent des freins à la mise en œuvre d'un des principes fixés par *l'EPC*, à savoir la séparation entre les structures d'acquisition et les organes de gouvernance des systèmes de paiement par carte[43].

La situation actuelle est marquée par la prédominance de protocoles d'échanges basés sur la norme ISO 8583, utilisée en particulier par les réseaux internationaux. Si *l'EPC* n'a pas engagé de travaux visant à la définition d'une nouvelle norme, il étudie actuellement, dans le cadre du groupe *ISO TC68 – WG9* une possible utilisation de la norme ISO 20022 (voir ci-dessus) également dans ce domaine. Aucune décision n'est toutefois prise à ce stade quant à la prépondérance d'une norme sur l'autre.

La sécurisation de la transaction de paiement lors d'un achat en ligne

L'interface de saisie des données personnelles en ligne

Les modalités de saisie des données personnelles des porteurs de cartes lors d'un achat en ligne ne sont encadrées par aucune norme. En effet, si la nature des informations demandées (nom du porteur à la commande, PAN, date d'expiration de la carte, CVx2 lors du paiement) résulte à la fois de contraintes opérationnelles pour les commerçants (liées à l'identification du client) ou pour les émetteurs (liées à l'authentification du porteur, cf. ci-dessous), aucune règle d'envergure internationale ne permet aujourd'hui de l'encadrer.

En France, la saisie du CVx2 lors de chaque achat est rendue obligatoire par l'application des obligations contractuelles liant un commerçant à sa banque acquéreur (contrat d'acceptation

[43] C'est le concept d' « unbundling » du *SCF*.

« CB » ou MasterCard). Ce n'est toutefois pas le cas des achats réalisés à l'aide d'une carte « VISA-only » (non co-badgée « CB »).

Si ces règles ne font l'objet d'aucune harmonisation au sein de la zone SEPA et restent sous la responsabilité des systèmes de carte nationaux et internationaux, l'EPC a publié une résolution[44] visant à rendre la saisie du CVx2 obligatoire pour tout acte d'achat. A cette fin et à partir de janvier 2012, les acquéreurs seraient astreints à transmettre le CVx2 aux émetteurs, et ces derniers contraints de refuser les autorisations pour les transactions ne comportant pas cette donnée, ou un CVx2 erroné. Ceci ne s'appliquera toutefois pas aux actes d'achat récurrents, les commerçants ne devant pas conserver le CVx2 dans leurs systèmes.

L'authentification du porteur

L'authentification du porteur, lequel a été identifié précédemment par son nom et son numéro de carte, n'est là encore encadrée par aucune norme. Toutefois, Visa Inc. a développé une architecture technique et un protocole (« 3D-Secure ») permettant à la banque émetteur d'authentifier son client lors de chaque transaction en ligne, la mise en œuvre d'un tel dispositif s'accompagnant d'un mécanisme incitatif pour les acquéreurs et les accepteurs de report de la fraude sur la banque émetteur (« *liability shift* » ou transfert de responsabilité). Cette architecture a depuis été reprise par Mastercard et JCB. Applicable depuis 2005, elle n'a été adoptée de façon significative en France que depuis le 1er octobre 2008, date d'entrée en vigueur du transfert de responsabilité « 3D-Secure » pour le système de paiement par carte « CB » pour les transactions domestiques.

Le protocole « 3D-Secure » n'impose aucune méthode d'authentification et les banques l'ont très largement mis en œuvre en 2008 avec une authentification statique du porteur. Suite aux recommandations formulées par la Banque de France en juillet 2008 et applicables à l'ensemble des porteurs à compter de juillet 2010, les banques françaises ont généralisé auprès de leur clientèle des méthodes d'authentification non rejouable, utilisant des mots de passe à usage unique[45]. La résolution de *l'EPC* comporte également un volet relatif à l'utilisation d'infrastructures permettant la mise en œuvre d'une authentification dynamique, visant à leur généralisation à l'horizon fin 2013. L'Eurosystème, dans son 7ème rapport d'étape sur SEPA publié en octobre 2010[46], attire l'attention de l'ensemble des acteurs en Europe sur la nécessaire adoption de mécanismes d'authentification renforcée pour les transactions de paiement par carte sur Internet.

La protection des données dans la filière acquisition

Les mesures dites *PCI*, développées par l'organisme « *PCI SSC* » (*Payment Card Industry Security Standard Council*), s'appliquent de manière mondiale à de nombreux acteurs de la filière d'acceptation et d'acquisition (banques acquéreurs, commerçants, prestataires de service exploitant des plates-formes de paiement, etc.) Elles concernent à la fois les transactions transfrontalières et les transactions domestiques dans le cas de cartes co-badgées avec un système national. Une description plus complète de ces mesures, qui sont, de fait, des standards, figure dans le rapport 2009 de l'Observatoire (chapitre 1, p. 9). On retiendra plus particulièrement ici les mesures « *PCI DSS*[47] », qui visent à protéger les données transmises au travers des systèmes d'information de la chaîne d'acquisition ou stockées dans ces systèmes.

---

44 Il s'agit de la résolution « Preventing Card Fraud in a mature EMV Environment » publié le 31 janvier 2011.

45 Également dénommée « authentification dynamique » par la suite.

46 Consultable à l'adresse suivante : http://www.ecb.int/press/pr/date/2010/html/pr101022_1.fr.html

47 PCI Data Security Standard.

L'EPC s'inscrit dans une démarche similaire dans ce domaine, en s'appuyant sur l'application des normes ISO 2700X[48] afin d'assurer la sécurité des données. Considérant le niveau de sécurité élevé des transactions réalisées en mode *EMV*, il promeut enfin la généralisation des mesures *PCI* à toute transaction réalisée en mode piste ou à distance.

La certification[49]

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 par ailleurs engagé une réflexion visant à créer un cadre de certification harmonisé en Europe. Les objectifs poursuivis résident dans l'indépendance des organismes de certification par rapport aux systèmes de paiement par carte et dans la reconnaissance mutuelle des certifications accordées au sein de la zone SEPA.

L'EPC s'appuie dans ce cadre sur les travaux du groupe *CAS* qui a pour objectif de définir à la fois des exigences de sécurité pour les cartes et terminaux (cf. ci-dessus) et une méthodologie commune d'évaluation, reposant sur la méthodologie des « Critères Communs » (cf. rapport 2005, encadré 12 p. 45).

L'EPC travaille actuellement en étroite collaboration avec le groupe *CAS* afin de valider les exigences sécuritaires et de créer un organisme de certification (« Certification Management Body » ou *CMB*), dont l'objet serait de faciliter la reconnaissance mutuelle des certificats délivrés par les différentes autorités de certification (nationales ou internationales) et plus généralement d'encadrer le processus d'évaluation et de certification. En parallèle, *CAS* est à l'origine du projet *OSeC* (« *Open standards for Security Certification* »), destiné à valider la faisabilité technique et économique d'une évaluation sécuritaire des terminaux selon la méthodologie des « Critères Communs ». Les modalités de coordination entre les travaux de *l'OSeC*, regroupant les principaux systèmes de carte nationaux et internationaux, et ceux du futur CMB restent cependant à définir.

Les délais de disponibilité des standards et de déploiement des produits

Reprenant l'approche de l'étude figurant dans le rapport 2007, le tableau suivant présente de manière prévisionnelle les dates de disponibilité et de mise en œuvre des différentes initiatives présentées ci-avant.

48 Série de normes dédiées à la sécurité de l'information, définissant le cadre de mise en œuvre d'un système de gestion de la sécurité, d'un catalogue de mesures de sécurité et d'un processus de gestion du risque.

49 Les processus de certification ont été abordés dans le rapport 2008 de l'Observatoire, ch. 4 p.47.

Encadré 6 : Calendrier d'élaboration et de déploiement des standards

Spécifications	Initiative concernée	Caractère obligatoire	Disponibilité du standard	Mise en œuvre
Domaine Carte - Terminal				
Standards EMV cartes et Terminaux	EMV Co	oui	Disponible	Parc CB 100 % EMV
Recommandations détaillées d'implémentation EMV pour la carte et les terminaux (CPA)	CIR / EMV Co	-	Disponible	Parc des terminaux CB compatibles avec CPA
Spécifications fonctionnelles pour les terminaux	SEPA-FAST	-	Fin 2011	À partir de 2011/2012
Exigences de sécurité pour la carte	CAS	Oui	Disponible	À partir de 2010
Domaine Terminal - Acquéreur				
Exigences fonctionnelles et sécuritaires	EPAS	-	Fin 2010	À partir de 2012/2013
Exigences de sécurité pour le terminal	CAS	oui	Fin 2010	À partir de 2011
(ERIDANE a arrêté ses travaux, alors qu'EPAS n'a plus pour objectif la rédaction de spécifications techniques détaillées)				
Domaine Acquéreur - Émetteur				
Exigences fonctionnelles	TC68 – WG9	-	Début 2011	À partir de 2012/2013
(Le groupe A2IEG n'a plus pour objectif la rédaction de spécifications techniques détaillées)				
Domaine Certification				
Exigences sécuritaires communes	CAS	oui	Fin 2011	À partir de 2011
Méthodologie commune de certification sécuritaire	CAS	oui	Fin 2010	À partir de 2011
Méthodologie commune de certification fonctionnelle	CAS	-	2008/2010	À partir de 2011

Conclusion

L'interopérabilité entre les différents systèmes de paiement en Europe demeure un enjeu majeur du projet SEPA pour les cartes. Les projets en cours sur chacun des domaines d'interaction entre la carte, le terminal et les serveurs acquéreurs et émetteurs en témoignent ; ils étaient pour la plupart déjà engagés lors de la précédente étude en 2007, sous l'égide de l'EPC ou de groupes interprofessionnels adhoc. Même si l'Observatoire ne peut que constater le retard pris sur nombre de ces projets, force est de constater que les démarches actuelles visant à la définition de cadres harmonisés de standardisation et de certification au sein de l'espace SEPA sont marquées par une volonté affichée des différents intervenants de collaborer plus avant à cette fin. L'Observatoire encourage dès lors ceux-ci à poursuivre les travaux y afférents sur l'ensemble de la chaîne de paiement.

L'Observatoire recommande en outre aux acteurs de la zone SEPA de poursuivre leur collaboration avec les organismes initiateurs des normes au plan international (tels PCI SSC et EMV Co), voire à devenir membres actifs de leurs organes de gouvernance, de façon à être plus impliqués dans la rédaction de ces normes. Seule une attitude volontariste de prise en compte des intérêts européens dans ce processus permettrait en effet d'asseoir la suprématie d'un cadre normatif harmonisé auprès d'intervenants actifs sur une scène plus large.

L'Observatoire recommande par ailleurs de porter une attention particulière aux nouveaux modes d'initiation des paiements de proximité par carte sans contact ou mobile. Apparues plus récemment, ces techniques devraient en effet connaître à court ou moyen terme une forte

croissance qui devra s'effectuer dans des conditions de sécurité équivalentes à celles en vigueur aujourd'hui en mode contact. Une démarche d'harmonisation similaire devra donc être entreprise par les acteurs concernés.

Les paiements initiés sur Internet, également en forte croissance et sujets à des taux de fraude plus élevés qu'en paiement de proximité, bénéficieraient également de la définition de normes visant à encadrer l'authentification du porteur, les modalités de saisie des données personnelles en ligne ainsi que leur transmission dans la filière acquisition.

L'Observatoire accueille ainsi favorablement les messages communiqués dans le 7ème rapport d'étape de l'Eurosystème sur SEPA visant à :

– généraliser les moyens d'authentification renforcés pour les paiements à distance, dans la continuité des actions engagées par la Banque de France depuis 2008 auprès des banques ;

– créer un forum européen sur la sécurité des moyens de paiement de détail, sous l'égide de l'Eurosystème et des superviseurs bancaires nationaux. Ce dernier, créé début 2011, a pour objectif d'harmoniser et de renforcer le niveau de sécurité de l'ensemble des moyens de paiement en Europe, dont la carte. Un élargissement de sa composition serait à ce titre bénéfique afin de bien intégrer l'ensemble des acteurs de marché dans cette démarche.

Glossaire

AEPM (Association Européenne Payez Mobile) : association française de banques et opérateurs de télécommunication, dont l'objectif est de favoriser le développement des paiements par téléphone mobile en Europe, par la rédaction de spécifications techniques et fonctionnelles et la conduite de phases pilotes à l'échelle de grandes agglomérations françaises.

A2I-EG (Acquirer to Issuer Expert Group) : groupe de travail composé de systèmes de carte nationaux (« CB », ZKA, SIBS…) et internationaux (Mastercard, VISA), de représentants des banques (FBF), de l'EPC, de processeurs (Equens) et de représentants de l'industrie (CECA), dont l'objet est d'analyser une possible convergence des normes en vigueur dans le domaine émetteur à acquéreur. Remplacé par le groupe ISO TC68 – WG9

CAS (Common Approval Scheme) : groupe de travail international composé de systèmes de carte nationaux (« CB », ZKA, 4B…) et internationaux (Visa, Mastercard), de processeurs (Atos), de représentants des banques (UK Cards Association) et d'organismes de certification (Paycert). Ce groupe est dédié à la définition d'exigences sécuritaires pour les cartes et terminaux ainsi qu'à la mise en œuvre d'un cadre de certification harmonisé.

CB2A (Cartes Bancaires Accepteur Acquéreur) : norme d'échanges entre les systèmes d'acceptation et les systèmes acquéreurs, développée par le Groupement des Cartes Bancaires « CB ».

CIR-TWG (Common Implementations Recommandations – Technical Working Group) : groupe de travail européen rassemblant les organismes en charge de l'implémentation de la norme EMV (systèmes de carte, processeurs, industriels). Ce groupe a été en charge dès 2003 du processus d'harmonisation des spécifications EMV afin de définir un minimum requis sur ce périmètre. Ces travaux ont conduit à la publication des spécifications EMV CPA par EMVCo.

CMB (Certification Management Body) : structure de gouvernance mise en place dans le cadre du schéma harmonisé de certification européen défini par l'EPC, et regroupant des représentants de l'ensemble des acteurs de l'écosystème de la carte. Son rôle précis reste aujourd'hui à définir.

CPA (Common Payment Application) : description fonctionnelle d'une application de paiement répondant aux exigences des Common Core Definitions (CCD), lesquels constituent une base technique requise afin de réaliser une transaction EMV.

EMV (Europay Mastercard Visa) : norme internationale, définie et maintenue par EMVCo, visant à sécuriser les échanges entre les cartes équipées d'une puce et les terminaux lors de paiements de proximité (en mode contact ou sans contact). Les éléments soumis aux spécifications EMV font l'objet d'évaluations sécuritaires et de processus d'homologation.

Glossaire (suite)

EPAS (Electronic Protocol Application Software) : initiative regroupant des fabricants de terminaux, des systèmes de carte nationaux et internationaux, des processeurs, des industriels et organismes de recherche afin de mettre au point un protocole de communication entre les terminaux et les serveurs acquéreurs.

EPC (European Payments Council) : organisme international représentatif de l'industrie bancaire, chargé du développement et de la promotion des instruments SEPA.

ERIDANE : projet lancé par le Berlin Group (lui-même composé de systèmes de carte, processeurs et industriels) et visant à définir un standard de sécurité pour les terminaux de paiement.

ETSI (European Telecommunications Standards Institute) : organisme en charge de la définition de standards dans le domaine des technologies de l'information et des télécommunications (dont les communications par mobile, radio ou Internet).

GlobalPlatform : association internationale en charge de la rédaction de spécifications techniques pour les infrastructures embarquées dans les cartes, dispositifs de paiement et systèmes. GlobalPlatform, qui regroupe des représentants de l'ensemble des acteurs de la chaîne de paiement par carte, a également orienté ses travaux vers les paiements par téléphone mobile depuis 2007, dans l'objectif de standardiser les chargements d'applications de paiement « Over The Air » et les modalités de gestion de ces applications.

Mobeyforum : forum créé en 2000, regroupant des établissements financiers, des industriels, des processeurs et des réseaux internationaux, visant au développement de l'usage de cet appareil dans les transactions financières.

OSCAR (Open Standards for Cards) : projet regroupant à terme des systèmes de carte, des industriels, des processeurs, des laboratoires, des banques et des commerçants, ces acteurs étant actuellement en phase de recrutement. L'objectif est de tester les nouveaux standards sur le domaine carte-terminal-acquéreur (SEPA-FAST, EPAS et les exigences CAS pour les terminaux), ainsi qu'à établir un processus de certification couvrant ce périmètre.

OSeC (Open standards for Security Certification) : projet destiné à valider la faisabilité technique et économique d'une évaluation sécuritaire des terminaux selon la méthodologie préconisée par CAS (Critères Communs).

PCI (Payment Cards Industry) : représenté par son Security Standard Council (SSC), lequel est constitué de ses membres fondateurs (systèmes de carte internationaux). Cet organisme promulgue des normes de sécurité visant à protéger les données (PCI DSS), les terminaux (PCI PED et UPT) et les applications de paiement (PA DSS).

SCF (SEPA Cards Framework) : document rédigé par l'EPC et regroupant les règles et principes applicables aux systèmes de carte désireux de se conformer aux standards SEPA.

SCT (SEPA Credit Transfer) : virement européen au format SEPA.

SDD (SEPA Direct Debit) : prélèvement européen au format SEPA.

SEPA-FAST (SEPA - Financial Application Specifications for SCF Compliant EMV Terminals) : spécifications relatives au déroulement des transactions entre les cartes et les terminaux, et définissant des règles d'affichage communes et des messages uniformisés.

SIM (Subscriber Identity Module) : puce utilisée en téléphonie mobile pour stocker les informations spécifiques à l'abonné d'un réseau mobile.

Volume (SEPA Cards Standardisation Volume - Book of Requirements) : déclinaisons techniques du *SCF*.

ZKA (Zentraler Kreditausschuss) : association professionnelle regroupant les banques allemandes.

4|2 La sécurité des modes de paiement par carte prépayée

Dans son rapport 2007, l'Observatoire a effectué un premier état des lieux relatif aux offres de cartes prépayées en France. Cette étude a permis de mettre en exergue deux types de produits, selon que la valeur est enregistrée sur un serveur ou sur la carte elle-même, ainsi que les enjeux y afférent en termes de sécurité.

L'évolution plus récente de l'offre, marquée par une diversification sans cesse croissante tant en termes d'acteurs impliqués que d'usages, a conduit l'Observatoire à actualiser cette étude pour ce qui concerne les cartes dont la valeur est stockée sur un serveur distant. En effet, même si la part de marché des cartes prépayées semble encore anecdotique tant en émission qu'en acquisition, la distribution de ces cartes prend de l'ampleur en France et pourrait être amplifiée par la mise en œuvre du nouveau statut d'émetteur de monnaie électronique, introduit par la nouvelle Directive monnaie électronique au niveau européen.

Seront ainsi abordés dans cette étude les caractéristiques et les cinématiques d'utilisation de ces cartes, le régime réglementaire applicable à ces nouveaux acteurs, qui sera modifié dans les prochains mois avec la transposition en France de la nouvelle Directive monnaie électronique, et les enjeux liés à ces nouveaux instruments.

Les cartes prépayées considérées ici sont limitées aux cartes interbancaires, excluant donc les cartes strictement mono-enseignes (cartes cadeaux, cartes de fidélité), conformément aux missions de l'Observatoire.

Filière	Émission (nombre de cartes)	Acquisition (transactions)	
		Volume	Valeur
Part des cartes prépayées	< 1 %	< 0,01 %	< 0,02 %

Source : banques et schemes membres de l'Observatoire, interrogés dans le cadre de la présente étude

▲ Tableau 12 – Part de marché indicative des cartes prépayées en France

Les différents types de cartes prépayées

Représentant la majeure partie des cartes prépayées disponibles sur le marché, les cartes considérées dans cette étude se caractérisent par un enregistrement des fonds sur les serveurs de leur émetteur. Les cartes prépayées sur lesquelles est stockée la valeur, en France le porte-monnaie électronique Moneo, ne sont donc pas reprises ici. Pour une description des cartes Moneo, on se référera au rapport 2007 de l'Observatoire (chapitre 1.2, p 13).

Description

Les cartes prépayées sous revue peuvent être subdivisées en trois grandes catégories, selon le réseau de distribution mis en œuvre :

– les cartes prépayées peuvent tout d'abord être distribuées par un établissement de crédit ou de paiement. Résultant souvent d'un partenariat avec un acteur privé, il s'agira de cibler un type de clientèle particulier, comme les jeunes, en leur offrant une solution leur permettant de maîtriser leurs dépenses tout en profitant de programmes de fidélisation liés au partenaire. Les acteurs impliqués sont généralement des établissements de crédit français et des opérateurs de télécommunication, formant ensemble une société financière

émettrice de la carte[50]. Certains établissements de crédit émettent enfin ces cartes en leur nom, tout en offrant un programme de fidélisation similaire[51] ;

– une seconde catégorie concerne les cartes distribuées par des acteurs de la sphère économique (entreprises, banques et assurances, commerçants, secteur public) afin de régler certaines prestations à des particuliers. Parmi ces dernières on trouve :

  - pour les entreprises, les règlements des frais professionnels ou des mesures incitatives ponctuelles ;
  - pour les banques et assurances, les règlements des indemnisations et des remboursements divers ;
  - pour les commerçants, les règlements des frais professionnels et les cartes cadeaux à destination des consommateurs ;
  - pour le secteur public, le règlement des prestations sociales et des indemnisations.

  Ces cartes étant distribuées à l'initiative des organismes ou entreprises, leur rechargement incombe à ces derniers[52] ;

– enfin, de nombreuses cartes sont désormais disponibles sur Internet ou auprès de commerçants bénéficiant d'une expérience acquise dans la commercialisation de cartes non bancaires, téléphoniques ou de fidélisation (commerces de proximité ou grande distribution). Résultant d'un partenariat entre un acteur privé et un système de paiement par carte tel que Visa ou MasterCard, il s'agira alors, avant tout de combiner l'expertise de ces sociétés dans le domaine de la monétique (en matière de commercialisation et gestion opérationnelle des flux) et l'étendue du réseau d'acceptation lié au système de paiement par carte concerné. L'émetteur de la carte est dans ce cas généralement situé à l'étranger[53]. Ces cartes peuvent enfin prendre la forme de cartes virtuelles distribuées et utilisables exclusivement sur Internet.

La croissance du marché est majoritairement le fait de cette dernière catégorie, laquelle est particulièrement sensible aux préconisations exposées ci-après en matière réglementaire, de lutte contre le blanchiment ou de sécurité des dispositifs mis en œuvre. L'analyse se concentrera donc sur cette catégorie de cartes prépayées quand il s'agira d'aborder les types d'usage, les cinématiques d'utilisation ou les aspects réglementaires et sécuritaires.

Le rôle des différents acteurs impliqués dans le cycle de vie des cartes prépayées est détaillé dans la partie traitant des aspects réglementaires.

Les types d'usage de ces cartes

Les différentes cartes prépayées sont utilisables sur l'ensemble du réseau d'acceptation affilié au système de paiement par carte concerné, et permettent donc d'effectuer des achats et retraits comme une carte de paiement classique.

Afin de limiter les cas d'utilisation aux montants disponibles à tout moment sur les serveurs de son émetteur, ces cartes requièrent une autorisation systématique lors d'un paiement ou d'un retrait d'espèces.

---

50 On notera à titre d'exemple la carte Jump (BNP Paribas et Orange), émise par la société financière OBPS.

51 Cas des cartes Indépendance (LCL), Independence Day (Crédit Mutuel), Carte Prépayée (Crédit du Nord), etc.

52 Rentrent notamment dans cette catégorie les cartes Prepay Solutions (Edenred et Mastercard) et Visa Liberty.

53 Les cartes PCS (Prepaid Card Services), Toneo First, Ecocard, Net+ Prepaid rentrent dans cette catégorie.

Par rapport à une carte de paiement classique, les cartes prépayées permettent de développer de nouveaux types d'usage ou répondent à des objectifs, détaillés ci-dessous.

Permettre un paiement par carte pour les acteurs non bancarisés

Les cartes prépayées permettent à des personnes en interdiction bancaire ou ne souhaitant pas être bancarisées d'obtenir un moyen de paiement utilisable sur l'ensemble du réseau d'acceptation du système de paiement par carte considéré. Ces cartes sont donc émises en coopération avec un tel réseau. Elles se distinguent peu des cartes anonymes décrites ci-dessous, les porteurs pouvant augmenter leurs plafonds de rechargement en justifiant de leur identité auprès du prestataire de service de paiement gestionnaire de la carte.

Permettre un paiement anonyme lors d'achats en ligne

Les cartes prépayées répondent également à un besoin d'anonymisation apparu dans certains domaines sur Internet, tels les sites pour adultes, les sites de rencontres et surtout les sites de jeux en ligne, en forte croissance depuis la mise en œuvre d'un cadre juridique spécifique en 2010. Une offre large et diversifiée en matière d'approvisionnement du compte ou d'achat de forfaits représente en effet pour ces sites un argument commercial au même titre que les offres promotionnelles ponctuelles.

Les acteurs impliqués dans la distribution de telles cartes, gestionnaires de comptes de monnaie électronique, n'exercent pas, de façon générale, cette activité à titre principal. Les cartes représentent en effet un moyen de paiement attaché audit compte.

Ces cartes permettent donc de régler des achats sur l'ensemble du réseau d'acceptation proposé par le système de paiement par carte auquel est affiliée la carte prépayée, le compte débité (préalablement chargé par virement, carte bancaire, recharges achetées avec des espèces, etc.) étant le compte de monnaie électronique tenu par l'établissement. Les cartes concernées sont nombreuses[54].

Ces cartes sont enfin anonymes dans la limite de certains plafonds (voir ci-dessous les règles anti-blanchiment). Au-delà, le porteur doit justifier de son identité auprès du prestataire de service de paiement gestionnaire de la carte.

Permettre les transferts de fonds entre particuliers

Les cartes permettant de réaliser des transferts de fonds entre particuliers sont distribuées sous la forme d'une offre constituée de deux produits : une carte principale, chargée par son titulaire à l'aide de moyens de paiement traditionnels (espèces, carte bancaire, virement), sert à recharger, par Internet ou SMS, une carte secondaire détenue par un tiers[55]. Ce type d'offre vise à concurrencer les dispositifs de transferts de fonds classiques[56], à destination notamment de populations de migrants, en s'affranchissant des structures physiques de mises à disposition des fonds, auxquelles se substituent l'usage des réseaux d'acceptation étendus des systèmes de paiement par carte.

54 On citera à titre d'exemple les cartes Net+ Pay (partenariat Neteller et Mastercard), Ultreia (Ticket Surf International et Mastercard), Ecocard (PSI-Pay et Mastercard), Toneo First (Central Telecom et Mastercard) ou encore PCS (Creacard et Mastercard).

55 A titre d'exemple, on notera les offres Transcash (Visa).

56 Comme par exemple Western Union.

Cinématiques d'utilisation

Activation de la carte

L'activation de la carte prépayée (1) doit être distinguée de la gestion du code PIN (2) et de la vérification de l'identité du porteur (3), ces trois processus étant généralement distincts et subséquents :

(1) l'activation des cartes prépayées s'effectue le plus souvent en ligne ou par envoi d'un SMS selon des modalités convenues avec le gestionnaire de compte de monnaie électronique. Certains gestionnaires associent également l'activation de la carte au numéro de téléphone portable utilisé pour l'envoi de ce premier SMS. Les rechargements ou transferts ultérieurs réalisés par envoi de SMS ne pourront alors être initiés qu'avec le téléphone ayant servi à envoyer le SMS d'activation ;

(2) l'activation de la carte peut déclencher l'envoi du code PIN qui lui est associé. Ce dernier peut également être envoyé par courrier (« PIN mailer »), cette procédure étant alors indépendante de l'activation ;

(3) la vérification de l'identité du porteur, laquelle permet d'augmenter les plafonds d'utilisation en paiement ou en retrait, est généralement distincte et postérieure à l'activation du support. Avant cette vérification, le porteur peut utiliser la carte prépayée dans la limite de plafonds imposés par le gestionnaire du compte de monnaie électronique[57] et devant répondre aux règles applicables en matière de lutte contre le blanchiment et le financement du terrorisme.

Chargement/rechargement de la carte

Les modalités de rechargement d'une carte dont la valeur est stockée sur les serveurs de l'émetteur sont nombreuses :

– le porteur peut tout d'abord acheter des codes de rechargement auprès d'un distributeur agréé par l'émetteur, auprès du gestionnaire du compte, ou en ligne. Le rechargement du compte de monnaie électronique s'effectue alors par saisie de ce code sur le site Internet de l'émetteur (ou du gestionnaire du compte), la carte prépayée pouvant alors être utilisée à concurrence du solde de ce compte.

  La carte peut également être rechargée dans ce cadre par envoi d'un SMS ou appel à un serveur vocal interactif. Dans le premier cas, le porteur envoie un message à un numéro indiqué par l'émetteur, selon un format prédéfini comportant notamment le numéro du compte, le montant, le compte destinataire, le code préalablement obtenu. Dans le second, ces informations sont composées sur le clavier téléphonique en suivant les instructions du serveur vocal.

  Dans aucun de ces cas la carte prépayée n'intervient directement dans le processus de rechargement ;

– dans le cas d'un rechargement sur Internet, le prestataire de service de paiement teneur de compte de monnaie électronique est considéré comme un commerçant en ligne. Le compte est alors approvisionné en utilisant l'un des moyens de paiement offert au porteur de la carte (paiement par carte, virement, etc.) ;

– enfin, une carte peut être approvisionnée par transfert de monnaie électronique d'une autre carte. Il s'agira en fait d'effectuer un « virement » de compte à compte, soit en saisissant

[57] Voir la partie réglementaire sur la lutte anti-blanchiment.

l'ordre sur le site Internet de l'émetteur (ou du gestionnaire de compte), soit en envoyant un SMS comme vu précédemment.

Utilisation de la carte

Les cartes prépayées bénéficiant le plus souvent d'accords entre l'émetteur et un réseau international, leur utilisation est donc calquée sur celle d'une carte de paiement classique. Les transactions sont toutefois soumises à une autorisation systématique en ligne afin de limiter l'usage de la carte à la somme disponible sur le compte de monnaie électronique associé.

Outre cette dernière caractéristique, les cartes prépayées peuvent être utilisées en mode contact, sans contact, ou par mobile, comme toute carte de paiement classique.

Remboursement des fonds

Les fonds préchargés sur le compte de monnaie électronique auquel est associée la carte de paiement peuvent être remboursés, en partie ou en totalité, au profit du détenteur de ce compte (et donc du porteur de la carte). Ce remboursement peut s'opérer avant la date d'expiration de la carte. Il est soumis à une vérification de l'identité du porteur au-delà d'un plafond, lequel est susceptible d'évoluer dans le cadre de la transposition de la directive 2009/110/CE (voir ci-dessous, 57).

Traitement des incidents

Les cartes prépayées comportent une date d'expiration au même titre qu'une carte de paiement classique. A l'issue de la période de validité, elles ne peuvent donc plus être utilisées, ni rechargées.

En cas de vol, le porteur doit mettre la carte en opposition en contactant le gestionnaire du compte de monnaie électronique auquel est rattachée la carte (et non l'émetteur qui se situe généralement à l'étranger). Le gestionnaire fournit en effet un numéro dédié à cette démarche ou demande au porteur d'appeler le service client à cette fin. Les transactions sont alors bloquées et une nouvelle carte peut être émise.

La responsabilité du porteur quant aux dépenses engagées avant et après la mise en opposition suit le régime applicable aux cartes de paiement classiques, suivant les dispositions transposées en droit français de la Directive sur les services de paiement (voir rapport 2009 de l'Observatoire, annexe A, p. 59). Celles-ci peuvent en outre faire l'objet de clauses contractuelles spécifiques applicables aux paiements de faibles montants, conformément aux articles L. 133-28 et suivants du Code monétaire et financier.

La réglementation applicable aux cartes prépayées

L'Autorité de contrôle prudentiel (ACP) est en charge de l'agrément des organismes financiers, aux fins d'émission et de gestion de cartes prépayées sur le territoire français, ainsi que de la réception de notifications des activités passeportées en France en libre prestation de services ou en libre établissement. La liste des organismes financiers ainsi autorisés est disponible sur le site de la Banque de France.

L'ACP est également en charge du contrôle des organismes financiers établis en France.

La Banque de France s'assure en parallèle de la sécurité des moyens de paiement, autres que la monnaie fiduciaire, et de la pertinence des normes applicables en la matière. Elle veille au bon fonctionnement et à la sécurité des systèmes de paiement, conformément à la responsabilité explicite que lui a confiée le législateur dans le cadre de l'article L. 141-4 du Code monétaire et financier.

Au cours du dernier trimestre de l'année 2011, la transposition de la directive 2009/110/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice, ainsi que la surveillance prudentielle de ces établissements, va modifier le cadre juridique de l'émission et la distribution de monnaie électronique.

Qualification des cartes prépayées

Les cartes prépayées sont en règle générale analysées comme de la monnaie électronique dont la définition est prévue par l'article 1er du règlement du CRBF n° 2002-13. La transposition de la directive 2009/110/CE va introduire dans le Code monétaire et financier une nouvelle définition qui s'inspirera de celle qui existe aujourd'hui, en prenant en compte les avancées technologiques réalisées depuis la transposition de la première Directive monnaie électronique (directive 2000/46/CE).

Conformément à l'article 3 du règlement du CRBF n° 2002-13, l'émetteur continuera de supporter une obligation de rembourser les unités de monnaie électronique non utilisées aux détenteurs qui lui en feront la demande. En principe, ce remboursement s'effectuera sans frais sauf cas prévus par le Code monétaire et financier.

Statut des émetteurs de cartes prépayées

En application des articles L. 311-1, L. 311-3 et L. 511-5 du Code monétaire et financier ainsi que des articles 1er et 2 du règlement précité, l'émission et la distribution de monnaie électronique nécessite un agrément d'établissement de crédit.

A la suite de la transposition de la directive 2009/110/CE, l'activité d'émission et de gestion de cartes prépayées exercée à titre de profession habituelle sera réservée aux émetteurs de monnaie électronique (qui comprendront les établissements de crédit et les établissements de monnaie électronique) habilités à intervenir sur le territoire français. Les établissements de paiement ne seront donc toujours pas autorisés à émettre et à gérer de la monnaie électronique et par conséquent des cartes prépayées contenant des unités de monnaie électronique.

L'Autorité de contrôle prudentiel délivre l'agrément d'établissement de crédit en application de l'article L. 511-10 du code précité et délivrera celui d'établissement de monnaie électronique conformément aux dispositions issues de la transposition de la directive 2009/110/CE. Un établissement de crédit ou un établissement de monnaie électronique agréé dans un autre État partie à l'accord sur l'Espace économique européen pourra agir en France s'il a accompli les formalités du passeport européen[58]. Les formalités du passeport européen se caractérisent par une déclaration faite par l'établissement à l'autorité compétente de son pays d'origine par laquelle il l'informe de son intention d'agir dans un autre pays membre. L'autorité compétente du pays d'accueil est alors informée par son homologue qu'un établissement va agir sur son territoire par le biais du passeport européen.

[58] prévues aux articles L. 511-21 et suivants du Code monétaire et financier pour les établissements de crédit, et par les futures dispositions pour les établissements de monnaie électronique.

Le nouveau statut prudentiel des établissements de monnaie électronique sera en grande partie calqué sur celui des établissements de paiement, à l'exception du capital minimum qui sera porté à 350 000 euros et de la mise en œuvre d'une nouvelle méthode de calcul des fonds propres (méthode D).

L'exercice illégal de la profession d'émetteur de monnaie électronique est puni de trois ans d'emprisonnement et de 375 000 euros d'amende.

Distribution des cartes prépayées

Dans le cadre des futures dispositions, les émetteurs de monnaie électronique pourront recourir à des personnes physiques ou morales pour distribuer pour leur compte la monnaie électronique. Cette activité comprend également le remboursement de monnaie électronique. Elle s'effectuera dans le cadre d'un contrat d'externalisation de prestations de services ou d'autres tâches opérationnelles essentielles ou importantes au sens du règlement du CRBF n° 97-02. Ces nouvelles dispositions devraient faciliter la distribution de monnaie électronique qui relève actuellement, pour les personnes non agréées en qualité d'établissement de crédit, du statut d'intermédiaire en opérations de banque et en services de paiement régi par les articles L. 519-1 et suivants du même code.

Cartes prépayées co-marquées

Certaines cartes prépayées sont co-marquées, c'est-à-dire qu'un émetteur agréé émet et gère des cartes prépayées sur lesquelles figure le nom d'une société non agréée. Dans ce cas, les informations figurant sur la carte prépayée et mentionnées dans les conditions d'utilisation doivent clairement indiquer que les cartes sont émises et gérées par l'émetteur agréé et que celui-ci demeure notamment responsable du remboursement. La société non agréée ne pourra qu'effectuer la distribution de ces cartes prépayées dans les conditions prévues par les futures dispositions issues de la transposition de la directive 2009/11/CE.

Cas particuliers : émission et gestion de cartes prépayées sans agrément d'émetteur de monnaie électronique

L'émission et la gestion de cartes prépayées généralement sous forme de cartes cadeaux peuvent, dans certaines conditions liées au caractère limité de l'acceptation des cartes prépayées, bénéficier de l'exemption d'agrément prévue à l'article L. 511-7, II du code précité. Dans le cadre des futures dispositions encadrant la monnaie électronique, une exonération d'agrément d'émetteur de monnaie électronique sera prévue. Dans ce cas, la capacité maximale de chargement en monnaie électronique du support mis à disposition des détenteurs sera limitée à 250 euros. Pour bénéficier de cette exonération, les entreprises doivent procéder à une déclaration auprès de l'Autorité de contrôle prudentiel.

Dispositions concernant la lutte contre le blanchiment des capitaux et le financement du terrorisme

Pour mémoire, les personnes qui émettent de la monnaie électronique sont soumises au dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) prévu aux articles L. 561-2 et suivants du Code monétaire et financier. Les établissements de monnaie électronique, dans le cadre de la transposition de la directive n° 2009/110/CE relative à la monnaie électronique, seront des organismes assujettis aux obligations en matière de LCB-FT et au contrôle de l'Autorité de contrôle prudentiel aux termes de l'article L. 561-36 du code précité.

Des évolutions du dispositif de LCB-FT applicable sont par ailleurs envisagées dans le cadre de la transposition en cours de la directive n° 2009/110/CE relative à la monnaie électronique.

L'ACP examinera les questions posées par les cas individuels dans le cadre de l'analyse de dossier d'agrément. En outre, la commission consultative de l'ACP instituée en matière de LCB-FT pourra être saisie de questions relatives à la monnaie électronique sur lesquelles des lignes directrices pourraient être jugées utiles.

Les enjeux liés à ces nouveaux instruments

Ces nouveaux moyens de paiement doivent s'accompagner d'une protection des consommateurs…

Accompagner les personnes non bancarisées dans l'utilisation d'une carte de paiement

Les cartes prépayées, en l'absence de tout lien avec un compte bancaire traditionnel[59], permettent à des personnes en interdiction bancaire ou ne souhaitant pas être bancarisées de bénéficier d'un moyen de paiement, de surcroît innovant.

Ces cartes permettent en effet de régler des achats auprès d'un réseau d'acceptation étendu, tout en bénéficiant à la fois de la souplesse d'utilisation d'une carte et de son niveau de sécurité intrinsèque. Les cartes prépayées se substituent donc en partie aux espèces pour cette population, voire à d'autres moyens de paiement moins efficients pour l'ensemble des porteurs.

Elles ne peuvent en outre être utilisées que dans la limite du montant préchargé sur le compte de monnaie électronique auquel elles sont attachées. Elles autorisent donc une maîtrise accrue des dépenses courantes, toute transaction devenant impossible une fois cette limite atteinte.

La délivrance de cartes prépayées, sur Internet ou en commerce de proximité, doit toutefois s'accompagner de mesures préventives destinées à éduquer le porteur sur le bon usage de sa carte et la conduite à tenir en cas d'incident. Les émetteurs et distributeurs de telles cartes doivent pour cela mettre en place des plans de communication adéquats tout au long du cycle de vie de la carte.

Assurer la transparence tarifaire

Les cartes prépayées se caractérisent par une tarification particulière, comprenant généralement des frais de gestion périodiques auxquels s'ajoutent des commissions prélevées lors de chaque opération de rechargement, de paiement ou de retrait. Ces dernières représentent une part du montant de la transaction ou un montant fixe, variables selon le distributeur de la carte.

[59] Les cartes émises par les établissements de crédit français ont été exclues de cette étude.

La diversité des tarifications en vigueur selon l'émetteur ou le distributeur de la carte, ainsi que sa relative complexité au regard de ses nombreuses modalités d'utilisation, doivent conduire les acteurs concernés à informer clairement le porteur lors de la souscription de la carte et à chaque transaction subséquente.

Ce dernier doit en outre pouvoir identifier facilement les voies de recours en cas d'incident affectant son compte de monnaie électronique ou sa carte (cf. ci-dessous).

Règles de médiation applicables aux cartes prépayées

La Directive monnaie électronique prévoit l'extension aux émetteurs de monnaie électronique des procédures de réclamation et de recours extrajudiciaires applicables aux établissements de paiement (art. 13). Les établissements de paiement relevant du régime de la médiation bancaire (art. L 315-1 du Code monétaire et financier), c'est ce dispositif qui sera étendu, par la future législation, aux émetteurs de monnaie électronique (art. L. 316-1 nouveau du Code monétaire et financier). Les principales règles applicables en ce domaine, qui sont rappelées ci-après, paraissent devoir concerner, sans différences notables, les cartes prépayées. Tout au plus convient-il d'insister sur l'effort spécifique d'information du client qu'impose cette catégorie d'instrument tant dans la forme, en raison de la nature des supports utilisés, que sur le fond, du fait de la fréquence potentielle des litiges transfrontaliers et d'une relation de clientèle tripartite (porteur, émetteur, distributeur) au lieu de bipartite habituellement. Par ailleurs, il n'est pas exclu que les médiateurs soient confrontés, dans l'élaboration de leurs préconisations, à des difficultés pour évaluer les responsabilités respectives dans un litige entre l'émetteur et le distributeur (hors champ de la procédure).

Principales règles de médiation applicables aux cartes prépayées :

- nomination et compétence du médiateur : tout émetteur de carte prépayée doit désigner un médiateur indépendant, compétent pour examiner les réclamations ou litiges émanant d'un porteur personne physique utilisant sa carte à des fins non professionnelles ;
- information du porteur : les coordonnées du médiateur doivent figurer sur la carte (et / ou le document fixant les conditions d'utilisation de celle-ci) et, lorsqu'elle est distribuée par internet, sur le site distributeur. Par ailleurs, les établissements émetteurs doivent déclarer leur médiateur au Comité de la médiation bancaire. Sur la base de ces informations, le Comité tient à la disposition du public un répertoire des médiateurs consultable sur le site internet de la Banque de France ;
- saisine : le porteur peut saisir le médiateur, par écrit, après avoir épuisé les recours ouverts auprès du service clientèle de l'établissement. Dans le cas d'un émetteur basé à l'étranger, le porteur devra adresser sa requête auprès de l'instance extrajudiciaire constituée dans le pays d'origine de l'établissement. Les coordonnées de ces instances sont répertoriées sur le site du réseau FIN-NET[60] consultable sur internet ;
- effets de la saisine : la saisine suspend le délai de prescription des recours judiciaires ;
- avis du médiateur : le médiateur dispose de deux mois, à compter de sa saisine, pour formuler un avis. Les parties demeurent libres d'accepter ou non les conclusions du médiateur. En cas d'acceptation, l'avis est notifié par écrit aux parties concernées ;
- confidentialité : les constatations du médiateur et les déclarations qu'il recueille ne peuvent, sauf accord des parties, être produites en justice ou communiquées à des tiers ;
- gratuité : la procédure de médiation est gratuite.

[60] FIN-NET est un réseau de résolution des litiges financiers. il se compose des organismes de traitement extrajudiciaire des réclamations qui sont établis dans les pays de l'Espace économique européen et qui sont chargés de régler les litiges entre les consommateurs et les prestataires de services financiers.

… et d'une vigilance de la part de l'ensemble des acteurs

Une vigilance accrue de la part des émetteurs est nécessaire lorsque ces cartes permettent les transferts de fonds

Certaines cartes prépayées autorisent des transferts de fonds entre porteurs[61], détenteurs de cartes rattachées au même compte de monnaie électronique. Toutefois, ces types d'opérations sont porteurs de nouveaux risques, notamment en matière de lutte contre le blanchiment et le financement du terrorisme.

Les transferts de personne à personne sont en effet susceptibles d'être utilisés à des fins criminelles afin notamment d'éviter le transport physique des fonds.

Les opérations de transfert de fonds nécessitent donc une vigilance particulière de la part de l'émetteur, se traduisant par la fixation de seuils, par des exigences d'identification et par le déploiement d'outils permettant une surveillance continue des opérations.

Les distributeurs commerçants ont également un rôle à jouer

Les cartes peuvent être distribuées sur Internet ou en point de vente. Dans ce dernier cas, les distributeurs concernés peuvent être des commerçants de proximité ou des grandes ou moyennes surfaces. Dans tous les cas, ces distributeurs sont soumis à un devoir de vigilance lors des différentes opérations affectant le cycle de vie des cartes prépayées : (1) à la vente du support, (2) lors de la vente de recharges, (3) lors du remboursement du solde de monnaie électronique le cas échéant.

Dans les deux premiers cas, les contrôles à opérer s'appliquent alors aux moyens de paiement utilisés afin de régler l'achat de la carte ou de la recharge, particulièrement dans le cas des règlements en espèces.

Dans le dernier cas (remboursement), qui implique un règlement en espèces du commerçant au porteur de la carte, le premier devra s'assurer de l'authentification du porteur par tout moyen approprié et selon les dispositions contractuelles liant le commerçant à l'émetteur de la carte.

Les aspects sécuritaires doivent également être pris en compte

Dispositifs liés à l'utilisation d'une carte de paiement classique

Les cartes prépayées ayant en grande partie les caractéristiques techniques et fonctionnelles des cartes de paiement classiques, leurs porteurs s'exposent aux mêmes types de risques : contrefaçon de l'instrument de paiement, vol du support, compromission des données de carte sur Internet, etc. Ces risques ont été traités dans les rapports précédents de l'Observatoire, qui a ainsi recommandé l'application des mesures sécuritaires suivantes :

[61] Ces opérations sont parfois dénommées P2P (Person to Person).

Encadré 7 – Mesures sécuritaires préconisées

Type de risque	Mesures préconisées	Références
Contrefaçon	Insertion d'un hologramme	Rapport 2003
	Utilisation de procédés cryptographiques pour l'identification des composants	Rapport 2003
	Certification des composants (carte, terminal)	Rapports 2005, 2007, 2009
Vol de la carte	Généralisation de la norme EMV	Rapports 2003, 2005, 2007
	Authentification du porteur par code PIN	Rapports 2007, 2009
	Application de seuils pour les transactions sans contact ou en mode prépayé	Rapports 2007, 2009
	Utilisation de systèmes de détection de la fraude	Rapports 2003, 2009
Compromission des données de carte	Lutte contre le phishing, campagnes de communication	Rapports 2004, 2006
	Protection des données de bout en bout (chiffrement), utilisation de réseaux privés	Rapports 2003, 2004, 2005, 2006, 2008, 2009
	Utilisation du CVx2 pour les transactions à distance	Rapports 2004, 2008, 2009
	Utilisation de cartes virtuelles dynamiques	Rapports 2005, 2008
	Protection des données sensibles par l'application de normes internationales	Rapports 2005, 2006, 2007, 2008, 2009
	Renforcement de la sécurité physique des automates et dispositifs d'émission immédiate	Rapports 2006, 2008
	Limitation de l'utilisation des lecteurs de piste dans les automates	Rapport 2006
	Utilisation de PAN dédiés à certains modes d'utilisation (sans contact, mobile)	Rapport 2007
	Fonction de désactivation des transmissions radio en mode sans contact	Rapports 2007, 2009
	Utilisation d'étuis imperméables aux ondes radio	Rapports 2007, 2009
Usurpation d'identité sur Internet	Authentification renforcée du porteur (dite également « authentification non rejouable »)	Rapport 2008

L'ensemble de ces mesures s'applique donc aux cartes de paiement prépayées. En particulier, ces dernières doivent donc contenir des éléments visuels permettant d'avoir une assurance raisonnable quant à leur authenticité et bénéficier des mesures de sécurité renforcées liées à la présence d'une puce. Ces cartes présentent par ailleurs certains risques inhérents à la notion même de chargement du compte ou de la carte, décrits ci-après.

Parmi les cartes prépayées disponibles actuellement sur le marché, certaines comportent une puce au standard EMV. Ces cartes possèdent donc un niveau de sécurité élevé lié à la présence de la puce, assimilable à celui prévalant pour les cartes interbancaires de paiement classiques[62].

[62] Ce niveau de sécurité est par ailleurs soumis à différents tests et certifications (voir rapport 2008 de l'Observatoire, ch. 4, p. 47).

D'autres cartes prépayées sont en revanche émises avec une piste magnétique seule[63], laquelle est par nature sujette à une compromission facilitée des données qu'elle abrite à des fins de contrefaçon et peut être réutilisée ultérieurement avec des données acquises frauduleusement (voir ci-après). Il est donc important que ces cartes prépayées intègrent elles aussi une puce au standard EMV afin de les prémunir contre ce type de risque.

On notera en revanche que les possibilités d'utilisation frauduleuse de la carte sont réduites au montant préchargé sur le compte auquel est rattachée la carte. Les cartes prépayées peuvent donc également contribuer à limiter les montants des transactions frauduleuses sur Internet.

Dispositifs propres aux cartes prépayées et à leur mode de fonctionnement

La sécurité du processus de rechargement dépend de l'instrument utilisé à cette fin, alors que les cartes prépayées présentent des risques spécifiques liés au support utilisé.

Sécurité du processus de rechargement

Les cartes prépayées peuvent être rechargées selon les processus opérationnels et sécuritaires décrits ci-dessous :

a) Une première option est le rechargement en ligne, par crédit du compte auquel est rattachée la carte. Le gestionnaire du compte offre au porteur en général divers modes de règlement : par carte, virement, ou encore saisie d'un code inscrit sur un ticket préalablement acheté auprès d'un commerçant de proximité. La sécurité du processus de rechargement est donc liée d'une part aux modalités de connexion du porteur de la carte sur le site désigné, d'autre part aux transactions de paiement elles-mêmes.

   La connexion aux espaces personnels sur Internet s'effectue en règle générale au moyen de données statiques (identifiant et mot de passe), par nature soumis à des risques élevés de compromission selon diverses techniques (hameçonnage ou « phishing »[64], virus, ingénierie sociale[65], etc.). La sécurité de l'ensemble repose donc sur celle associée aux opérations de paiement effectuées lors de chaque rechargement :

   - lorsque l'opération sous-jacente est un paiement par carte, il convient d'identifier la carte et d'authentifier de manière forte son porteur, en utilisant par exemple des protocoles de type « 3D-Secure »[66] ou tout mécanisme permettant un niveau de sécurité équivalent ;
   - lorsque le compte est approvisionné par virement d'un compte bancaire, l'utilisateur devra en pratique se connecter à son site de banque en ligne afin d'initier le virement. Celui-ci est couvert par les recommandations de la Banque de France en matière de protection des opérations sensibles en ligne, à savoir l'utilisation d'une authentification non rejouable soit à l'enregistrement du BIC/IBAN du bénéficiaire, soit au moment de l'ordre de virement unitaire ;
   - enfin, lorsque la carte est rechargée par saisie d'un code obtenu sur un ticket, les aspects sécuritaires sont reportés sur l'opération d'achat du ticket auprès d'un commerçant : le règlement du ticket s'analyse alors comme tout autre achat de proximité, devant être

63 C'est le cas notamment des cartes Transcash, Ecocard ou Visa Liberty.

64 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.

65 Acquisition frauduleuse de données personnelles en exploitant les failles humaines et sociales de la victime potentielle.

66 Protocole, mis en œuvre par Visa et Mastercard, permettant d'authentifier le porteur de la carte lors d'un achat à distance. Voir le rapport 2008 de l'Observatoire pour plus de détails.

dénoué par l'utilisation de moyens de paiement (carte, chèque, espèces) qui doivent être mis en œuvre dans le respect des règles de sécurité qui leur sont propres.

b) La carte peut également être rechargée en envoyant un SMS ou en contactant un serveur vocal interactif. La sécurité du processus de rechargement repose alors sur l'identification et l'authentification du porteur. Dans le cas d'un envoi de SMS, celui-ci doit généralement être transmis à partir d'un téléphone portable dont le numéro a été déclaré au gestionnaire du compte de monnaie électronique. Dans le cas d'un appel à un serveur vocal interactif, l'authentification s'opère par la saisie du numéro de carte suivi d'un code connu du seul porteur.

c) Enfin, le rechargement sur un DAB ou un terminal de paiement permet de lier la carte prépayée à un compte bancaire (cas des DAB) ou d'effectuer une transaction par carte (sur des terminaux de paiement). L'authentification du porteur est ici assurée par la saisie de son code PIN, l'opération bénéficiant alors des mesures de sécurité liées à l'usage de la carte (authentification dynamique de la carte, contrôle du code PIN, chiffrement des données, etc.).

Risques liés au support

Les cartes prépayées achetées au sein de commerces de proximité peuvent enfin l'être dans le seul objectif d'obtenir un support idoine pouvant accueillir des données acquises frauduleusement par ailleurs. Les cartes à piste sont particulièrement sensibles à ce type de fraude, notamment si la technologie employée pour la piste magnétique est obsolète et permet en conséquence un réencodage de données encore plus aisé. L'impact en matière de fraude peut dans ce cas s'avérer conséquent, au regard de l'étendue du réseau d'acceptation dont bénéficient ces cartes.

Face à ce type de risques, seule la présence sur la carte d'une puce au standard EMV constitue une réponse adéquate, en permettant une authentification de la carte elle-même lors d'une opération de paiement de proximité ou de retrait et en protégeant physiquement les données sensibles liées à la carte ou au porteur.

Conclusion

La présente étude s'est concentrée sur les cartes prépayées rechargeables dont la valeur est stockée sur les serveurs de l'émetteur, lequel peut se situer à l'étranger. Les cartes Moneo et les cartes prépayées distribuées par les établissements bancaires français à destination de populations très ciblées (jeunes en particulier), ainsi que les cartes distribuées par les acteurs de la sphère économique, n'ont donc pas fait l'objet de nouveaux développements depuis l'étude publiée dans le rapport 2007 de l'Observatoire sur le même thème.

Même si la part de marché des cartes prépayées, analysées comme de la monnaie électronique, est encore anecdotique en France tant en émission qu'en acquisition, la distribution de ces cartes est en pleine croissance et pourrait être amplifiée par la mise en œuvre au niveau européen du nouveau statut d'émetteur de monnaie électronique introduit par la Directive 2009/110/CE.

Ces cartes s'adressent en priorité aux personnes non bancarisées ou soucieuses de conserver l'anonymat, notamment lors d'achats effectués sur Internet, ainsi qu'aux populations de migrants. Elles sont utilisables sur l'ensemble du réseau d'acceptation du système de paiement par carte avec lequel l'émetteur a passé un accord, et sont rechargeables dans certaines limites

sur Internet, par SMS ou par serveur vocal interactif, ce qui les place au centre d'une stratégie de paiements multicanaux qui caractérise désormais de nombreux émetteurs.

Face aux enjeux que représentent ces cartes au regard de la protection des consommateurs, de l'utilisation potentiellement détournée qui peut en être faite et de la sécurité, les membres de l'Observatoire émettent les recommandations suivantes :

- si ces cartes autorisent une maîtrise accrue des dépenses en vertu de l'utilisation limitée au montant chargé sur le compte de monnaie électronique associé, leur distribution doit s'accompagner de mesures visant à protéger les consommateurs, notamment en les informant sur les modes d'utilisation de ces instruments et en assurant la transparence tarifaire ;
- le mode de distribution de ces cartes fait également reposer sur les points de vente concernés, des mesures de vigilance liées aux moyens de paiement utilisés lors de la vente de cartes ou de recharges et à l'authentification du porteur lors de remboursements. L'utilisation potentielle de ces cartes à des fins de transferts de fonds de particulier à particulier nécessite en outre de mettre en place des dispositifs de surveillance adaptés ;
- ces cartes présentent enfin un profil de risques similaire aux cartes de paiement classiques et doivent donc être soumises aux mêmes mesures de sécurité, tant pour les transactions de proximité (utilisation de cartes à puce, en mode EMV avec saisie du code PIN, mesures propres aux paiements sans contact…), que pour les transactions à distance (utilisation du code CVx2, sécurisation des achats en ligne par transmission de codes à usage unique), même si les transactions sont par construction de plus faibles montants que celles réalisées avec des cartes traditionnelles. Ces cartes se caractérisent toutefois également par des risques propres liés au processus de rechargement et à leur mode de distribution : pouvant être acquises et utilisées de façon anonyme dans la limite de certains plafonds, elles sont vulnérables à la contrefaçon et doivent prévoir des dispositifs de sécurité adaptés afin de s'en prémunir (présence d'une puce notamment).

La mise en œuvre de ces dispositifs de sécurité s'inscrit enfin dans le cadre d'un processus plus large d'harmonisation au plan européen du niveau de sécurité attendu des moyens de paiement de détail, mené au sein du forum « Security of Retail Payments (SecuRe Pay) » récemment créé par le SEBC et réunissant superviseurs et surveillants nationaux. Ce processus s'avèrera particulièrement déterminant s'agissant de produits impliquant de nombreux acteurs disséminés au sein de l'espace SEPA et pouvant offrir leurs services au sein de l'Union Européenne dans le cadre de la libre prestation de service.

4|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 six 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 en cours partout en Europe, avec une progression correcte dans la plupart des pays, globalement en léger retard sur l'engagement des banques européennes au sein de l'EPC d'avoir achevé cette migration à fin décembre 2010.

État de la migration en France

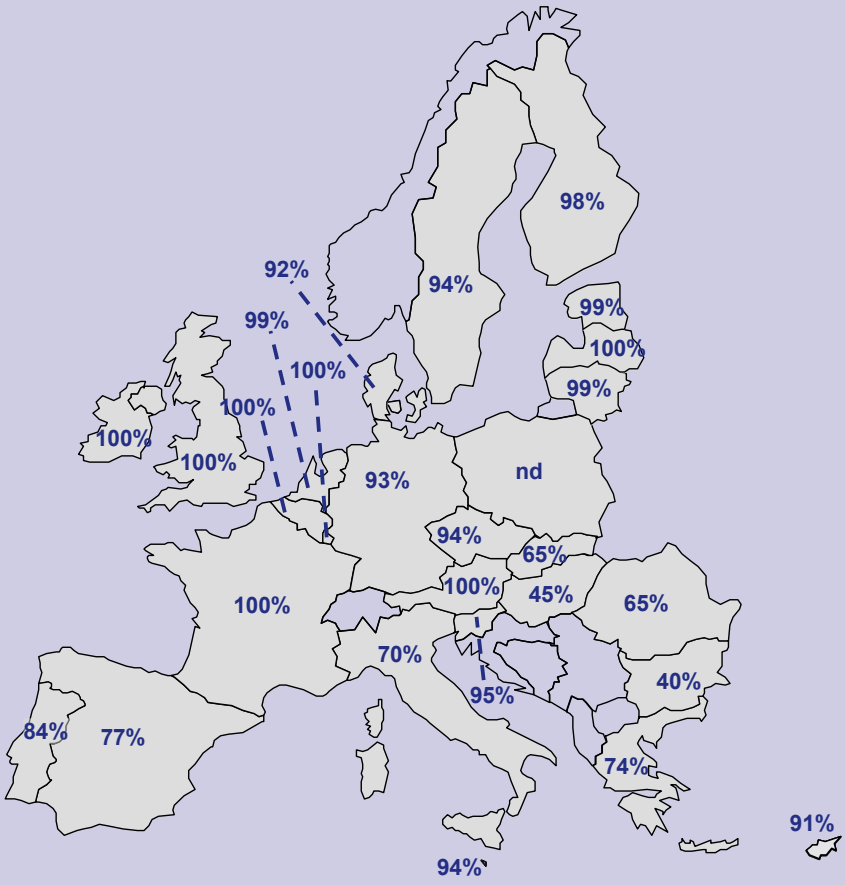
En France, la migration aux standards EMV est quasiment terminée. Fin mars 2011, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes « CB », 99,5 % des terminaux et automates[67], et 100 % des distributeurs automatiques de billets étaient conformes aux spécifications EMV. Le 0,5 % restant de terminaux et automates, peu utilisés, seront migrés lors de leur remplacement normal.

[67] Le taux de migration des terminaux et automates apparaît en légère baisse cette année (99,5 % contre 99,8 % en 2009) en raison de la modification du mode de comptabilisation des automates des péages autoroutiers (avant, un péage comptait pour un seul point de vente indépendamment du nombre d'automates présents, le Groupement des Cartes Bancaires « CB » retient désormais le nombre d'automates du péage).

État de la migration en Europe

Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2011, 85,6 % des cartes interbancaires circulant au sein des 27 États membres de l'Union européenne sont maintenant conformes à la spécification EMV (+ 15,8 points par rapport à mars 2010). Pays par pays, la situation reste contrastée (voir Encadré 8). Alors que la mise en conformité aux règles d'interopérabilité de SEPA a commencé depuis début 2008, la migration EMV de certains pays reste peu avancée (Bulgarie, Hongrie). La migration a en revanche fortement progressé en Espagne, en Grèce et en Roumanie.

Encadré 8 – Déploiement des cartes EMV en Europe



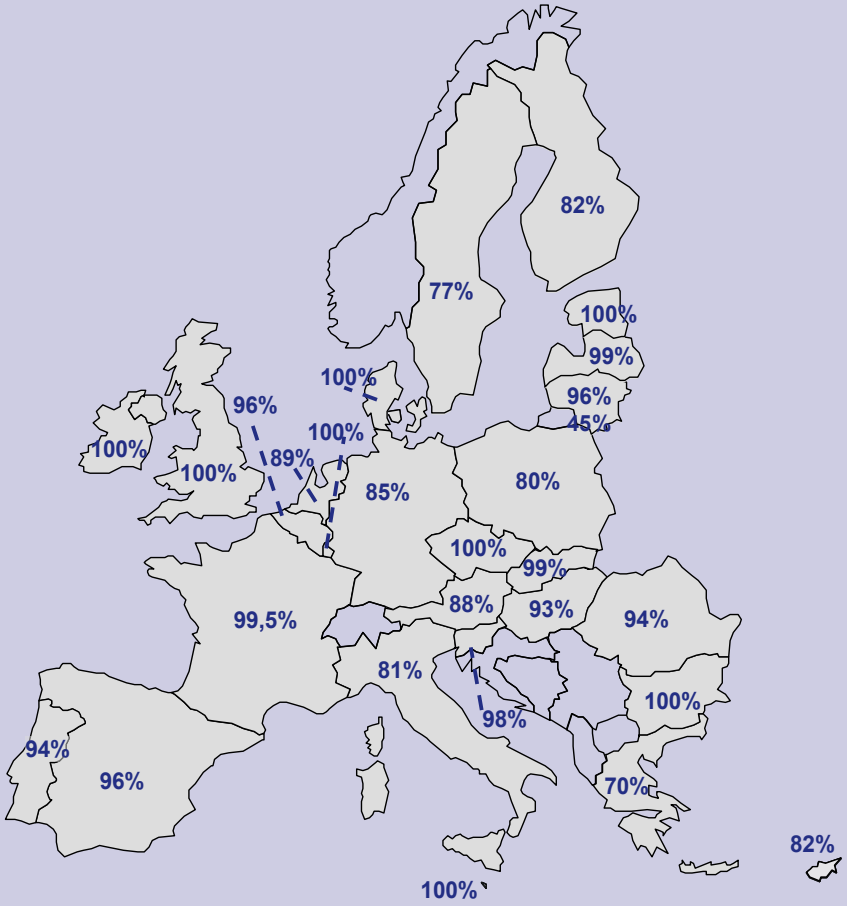
Source : European Payments Council – mars 2011

Par rapport à l'an dernier, on constate une nette progression de la migration des cartes au standard EMV. Toutefois, plusieurs pays conservent toujours un parc constitué majoritairement de cartes non conformes au standard, comme la Bulgarie, la Hongrie et la Pologne.

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

Concernant l'acquisition, la migration vers EMV progresse sensiblement : à fin mars 2011 92,0 % des terminaux de paiement (voir Encadré 9) et 96,6 % des distributeurs automatiques de billets (voir Encadré 10) sont conformes à EMV (soit une progression de 12 points pour les terminaux de paiement et de 2,2 points pour les distributeurs automatiques de billets par rapport à mars 2010). La disparité entre les différents pays a fortement diminué.

Encadré 9 – Déploiement des terminaux et automates EMV en Europe



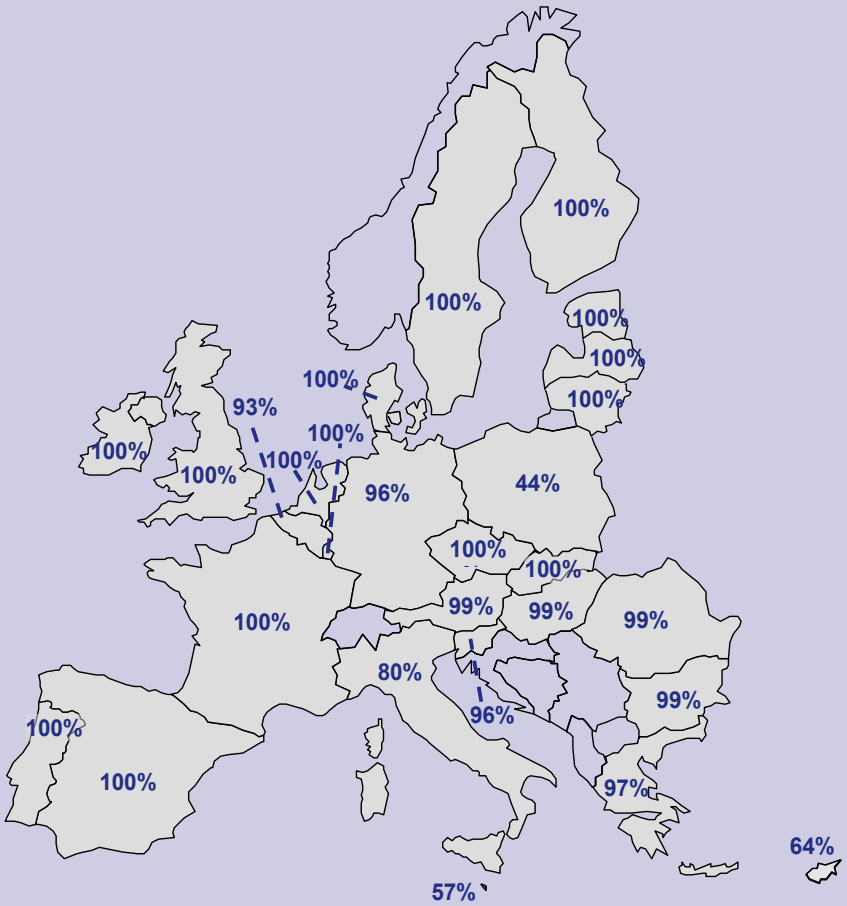
Source : European Payments Council – mars 2011

Les pays du Nord de l'Europe ont pratiquement rattrapé leur retard et on ne constate désormais plus de différences notables avec les pays du Sud de l'Europe, où la migration avait été la plus rapide.

La migration est achevée en Bulgarie. La situation a très fortement évolué en Allemagne par rapport à mars 2009. La migration a également progressé en Lituanie, en Suède, en Finlande et aux Pays-Bas.

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.

Encadré 10 – Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2010

La migration des distributeurs de billets est pratiquement achevée dans la plupart des pays. Les données polonaises n'ont pas été actualisées depuis début 2009 et elles ne reflètent donc peut-être pas la réalité du déploiement. L'Italie reste légèrement en deçà des niveaux de déploiement des autres pays mais son niveau d'équipement s'est encore amélioré depuis mars 2010.

5 | LES ENJEUX SÉCURITAIRES LIÉS AUX ÉVOLUTIONS DES SYSTÈMES DE PAIEMENT PAR CARTE EN FRANCE ET EN EUROPE

A l'heure où l'avenir du marché européen de la carte de paiement implique des décisions stratégiques de la part des systèmes nationaux et internationaux, l'Observatoire a souhaité évaluer quels étaient les enjeux sécuritaires à considérer dans ce cadre.

A ce jour existent en Europe des systèmes de paiement par carte internationaux qui, compte tenu de leur très large réseau d'acceptation, permettent aux porteurs de réaliser des paiements dans tous les pays européens et à l'international. A leurs côtés coexistent de nombreux systèmes domestiques interbancaires ou privatifs, d'importance très inégale.

Dans le cadre de la mise en place du SEPA, ces systèmes disposent désormais de deux options : soit ils continuent d'exercer leur activité au niveau national, sur un réseau d'acceptation et pour un nombre de clients restreint, soit ils étendent cette activité à l'espace SEPA. De plus, trois initiatives visant à créer un système de paiement par carte européen ont été annoncées.

Quelle que soit l'option retenue, le processus de décision doit prendre en compte un certain nombre d'enjeux sécuritaires, qui préexistaient à la mise en œuvre du SEPA mais qui prennent une nouvelle dimension dans ce cadre. Deux de ces enjeux apparaissent particulièrement prégnants au regard de leur impact avéré en matière de fraude : la protection du support physique et des données de carte lors des transactions de proximité et la réutilisation de ces supports et données à des fins frauduleuses lors des transactions à distance.

Dans le cadre de la présente étude, l'Observatoire a donc souhaité axer cette réflexion sur ces deux sujets d'importance.

5|1 Les enjeux sécuritaires européens dans le domaine de la carte

Aujourd'hui en Europe, les seules statistiques de fraude disponibles proviennent de l'OSCP en France et de la communauté bancaire nationale au Royaume-Uni[68]. Ces données montrent deux fortes tendances :

– l'importance croissante de la fraude sur les transactions transfrontières effectuées dans les pays n'ayant pas adopté les standards EMV ;

– une vulnérabilité notable sur les transactions à distance, principalement celles concernant les paiements par carte sur Internet.

[68] Via l'organisation « UK Cards Association ».

La compromission des données de carte contenues sur la piste magnétique

Les cartes de paiement sont aujourd'hui très majoritairement pourvues d'une puce EMV au sein de l'espace SEPA. Sauf quelques cas particuliers[69], elles sont toutefois également dotées d'une piste magnétique, laquelle répond à des caractéristiques techniques normalisées et contient des informations pouvant potentiellement être réutilisées à des fins frauduleuses.

Les caractéristiques physiques des pistes magnétiques

Les bandes magnétiques figurant sur les cartes de paiement doivent répondre à la norme internationale ISO 7811, définissant les caractéristiques physiques (emplacement, taille, densité d'enregistrement, contenu) de chacune des trois pistes (ISO1, ISO2 et ISO3) composant la bande[70].

Les pistes magnétiques situées au verso des cartes de paiement sont plus ou moins robustes aux attaques visant à copier des données ou à les effacer du support. Les pistes dites à forte coercitivité (« HiCo ») résistent intrinsèquement mieux au détournement de données[71]. Toutes les cartes émises en France répondent à cette dernière caractéristique. Certaines cartes émises à l'étranger et distribuées en France possèdent encore toutefois une piste à faible coercitivité (« LoCo »), les rendant particulièrement vulnérables à la contrefaçon.

Les données contenues sur les pistes magnétiques

Le contenu des trois pistes constituant les bandes magnétiques est normalisé dans le cadre de l'ISO. Ainsi, les pistes contiennent notamment le numéro de la carte, le nom de son titulaire, la date de fin de validité de la carte, ainsi que différents indicateurs relatifs à la vérification du PIN[72] ou de la carte[73] par l'émetteur lors d'une transaction de retrait ou de paiement en mode connecté.

Le « skimming »

Cette technique de fraude consiste à capturer les données écrites sur les pistes magnétiques des cartes à l'insu de leur détenteur. Ceci peut être mis en œuvre dans les distributeurs automatiques de billets (DAB) ou guichets automatiques de banque (GAB), dans les terminaux de paiement isolés (distributeurs de carburant, péages[74], parkings, etc.), ou plus rarement dans les terminaux de paiement en point de vente.

Ces appareils doivent être physiquement modifiés, afin de se voir adjoindre un module additionnel (appelé « skimmer ») permettant de copier les données de la piste avant de poursuivre la transaction normalement. En règle générale, les cartes subissant un « skimming » ne sont donc pas conservées par les automates[75].

---

69 Les cartes VPay (Visa) sont ainsi conçues à l'origine comme des cartes à puce uniquement.

70 Les « pistes » auxquelles il est fait mention dans ce document représentent l'ensemble des pistes constituant les bandes magnétiques aux normes ISO.

71 Même si la haute coercitivité ne réduit pas entièrement le risque de compromission.

72 Clé (PVKI) ou valeur (PVV) de vérification.

73 Valeur (CVV) ou code (CVC) de vérification, souvent référencés sous le terme CVx, qui ne doit pas être confondu avec le CVx2 imprimé au dos de la carte elle-même et utilisé lors des transactions à distance.

74 On notera toutefois des projets en cours de la part de sociétés d'autoroutes visant à utiliser la puce.

75 La capture de la carte par l'automate est appelée « card trapping ».

Le code PIN du porteur n'étant pas écrit sur la piste magnétique[76], le « skimming » s'accompagne en outre fréquemment de dispositifs permettant d'obtenir frauduleusement le code PIN du porteur de la carte lors de sa saisie. Des caméras peuvent être placées sur les DAB/GAB à cet effet, leurs claviers modifiés afin d'enregistrer la saisie ou, plus simplement, le porteur observé durant l'opération.

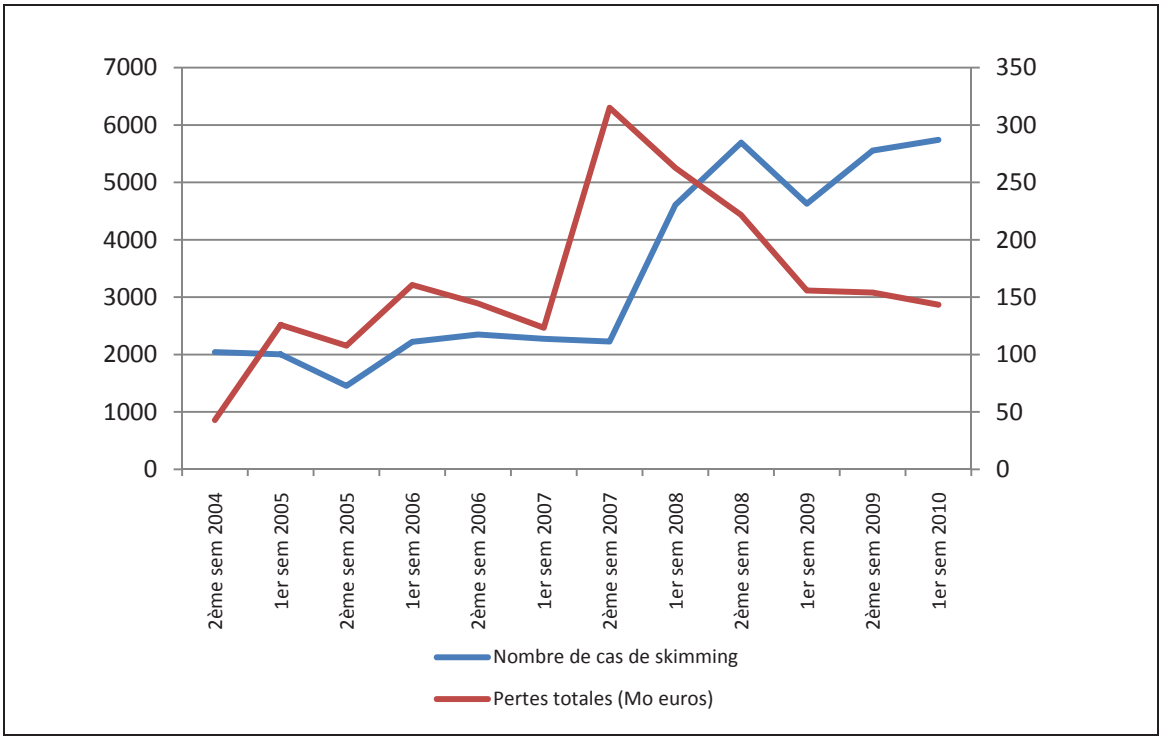
Les données capturées sont ensuite soit stockées jusqu'à ce que le fraudeur récupère le dispositif ultérieurement, soit immédiatement ré-encodées sur une autre carte, vierge, insérée par le fraudeur dans le même appareil, soit enfin transmises à ce dernier à distance.

Ces mêmes données peuvent alors être réutilisées de deux façons :

– en réalisant des transactions à distance dans des pays ou sur des sites ne demandant pas systématiquement la saisie du cryptogramme visuel CVx2 situé au dos de la carte ou une authentification renforcée du porteur (par exemple via le dispositif « 3D-Secure », voir p. 77) ;

– en réalisant des transactions de proximité ou des retraits dans les pays où la norme EMV n'a pas été déployée.

Le « skimming » demeure enfin l'une des techniques de fraude les plus employées afin de contrefaire des cartes, comme le montre l'évolution du nombre de cas de fraude par semestre depuis l'année 2004. En Europe, le montant des pertes subies par les émetteurs en raison du « skimming » est toutefois en retrait en raison du déploiement progressif d'EMV, la fraude se déplaçant dorénavant sur les pays n'ayant pas déployé cette norme, comme les États-Unis.



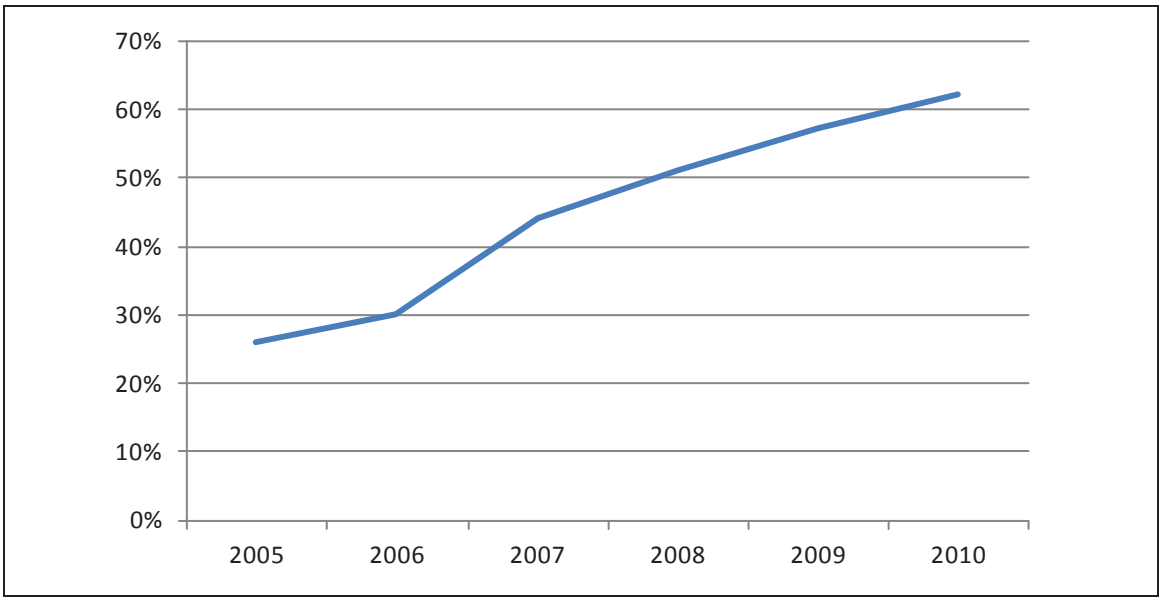
Source EAST (ATM crime report 1H2010)

▲ Tableau 13 – **Progression en Europe du nombre de cas de « skimming » et des pertes associées**

[76] La validité du code PIN est en effet déduite des valeurs de contrôles écrites sur la piste (PVKI, PVV), mais le code PIN n'apparaît pas lui-même sur la piste magnétique.

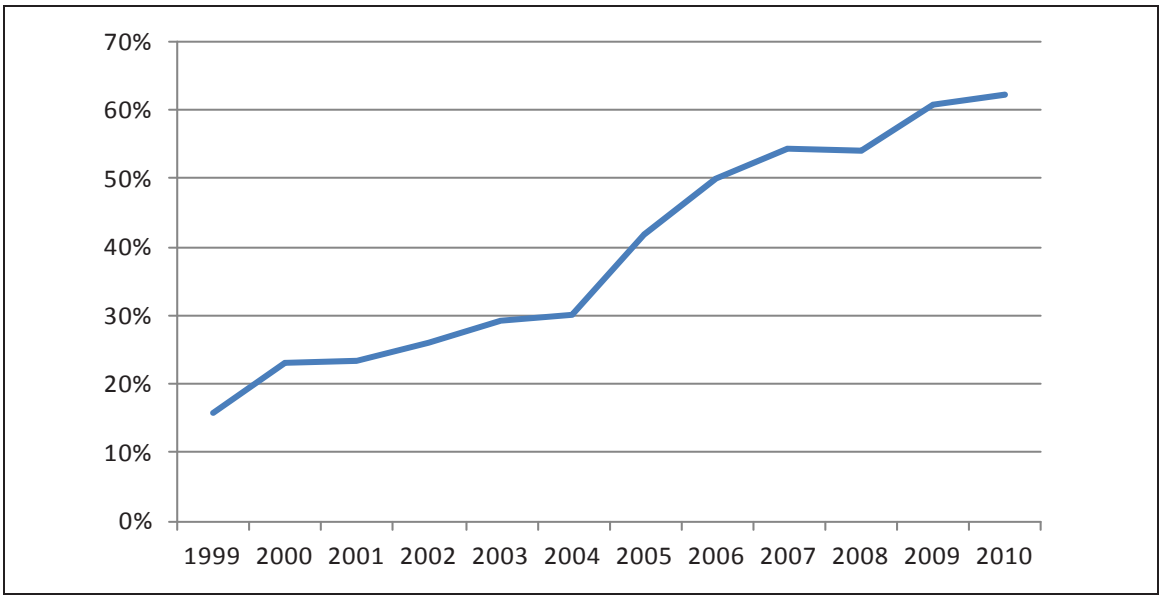
La réutilisation de ces données sur les environnements de vente à distance

Les transactions par carte à distance connaissent depuis plusieurs années une croissance régulière, tant en valeur qu'en volume. Les paiements par carte en ligne, bien que ne représentant qu'une faible partie de l'ensemble des paiements par carte (8,6% en France en 2010), représentent toutefois désormais la majeure partie de la fraude sur ce moyen de paiement (voir ci-dessous) et constituent à ce titre un enjeu prioritaire dans le cadre des réflexions en cours quant à l'avenir des systèmes de paiement par carte en Europe.



Source : Observatoire de la Sécurité des Cartes de Paiement

▲ Tableau 14 – **Part de la fraude sur les paiements à distance par rapport à la fraude totale en France**



Source : Financial Fraud action UK – "Fraud the facts 2010"

▲ Tableau 15 – **Part de la fraude sur les paiements à distance par rapport à la fraude totale au Royaume-Uni**

Les environnements soumis à la fraude sur les paiements par carte à distance

Les paiements à distance peuvent être réalisés sur Internet, par mail ou par téléphone (ces deux derniers canaux étant regroupés sous le terme MOTO[77]).

Ces différents canaux diffèrent essentiellement dans le mode de collecte des données nécessaires à la réalisation de la transaction : Internet offre en effet la possibilité de réaliser les transactions de façon totalement automatisée entre le consommateur et les serveurs de l'acquéreur, voire de l'émetteur. En revanche, certaines transactions MOTO nécessitent la présence d'un intermédiaire (généralement le service clientèle du commerçant) lors de la saisie des données de transactions, ce qui rend d'autant plus complexe leur sécurisation.

Les données utilisées pour les paiements par carte à distance

Les données utilisées pour réaliser un paiement par carte à distance (nom, le numéro de sa carte, sa date d'expiration) peuvent être obtenues frauduleusement de différentes façons :

– en capturant les données de carte par « skimming » (voir ci-dessus)[78] ;

– en dérobant la carte elle-même ;

– en récupérant les données de carte par hameçonnage (« phishing »)[79].

Afin de lutter contre la réutilisation des données obtenues par « skimming » ou hameçonnage l'usage du cryptogramme visuel CVx2, situé au dos de la carte, a été mis en place. Toutefois, cette mesure n'est pas encore généralisée à l'ensemble de l'espace SEPA, a fortiori au niveau mondial.

5 | 2 Les moyens permettant de répondre à ces enjeux

Afin d'empêcher le détournement de données sur les paiements de proximité

La suppression de la piste magnétique

Les cartes, initialement émises avec une piste magnétique, ont progressivement intégré une puce dans différentes régions du monde. Dans l'espace SEPA, la migration aux normes EMV, laquelle nécessite l'emploi d'une puce, est en voie d'achèvement, comme indiqué p. 66 de ce rapport. Si l'utilisation des cartes à puce garantit un haut niveau de sécurité, se pose alors la question du maintien de la piste sur ces cartes en raison des risques exposés au §1.

Plusieurs instances (Europol, l'Eurosystème, l'EPC) ont récemment pris position en faveur d'un abandon de la piste magnétique sur les cartes de paiements. Toutefois, et quoique poursuivant le même objectif, ces déclarations diffèrent sensiblement dans leur contenu :

– dans son 7ème rapport d'étape sur SEPA paru en octobre 2010, l'Eurosystème a recommandé l'émission par défaut de cartes à puce sans piste magnétique dès 2012. Si les

77 Voir rapport 2008, p.27

78 De manière théorique, il est également possible de capturer des données de cartes en écoutant les transactions réalisées en mode sans-contact (« telepickpocketing ») ;

79 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.

acteurs du marché décidaient de maintenir une piste sur les cartes pour des raisons pratiques, celle-ci ne devrait alors contenir aucune donnée permettant la réalisation de transactions de paiement ;

– Europol a observé dans son rapport 2011[80] un déplacement de la fraude vers les pays n'ayant pas déployé les normes EMV. Bien que ne formulant pas de recommandation, un lien explicite est fait entre le manque d'harmonisation dans la mise en œuvre de ces normes au niveau international et le maintien de la piste magnétique sur les cartes par leurs émetteurs ;

– l'EPC[81] a de son côté adopté courant 2011 une résolution[82] visant à s'assurer que chaque émetteur et acquéreur ait la possibilité, s'il le souhaite, de refuser les transactions réalisées en mode piste.

La mise en œuvre de ces recommandations se heurte toutefois à divers obstacles, tant du côté des porteurs que des accepteurs et des émetteurs de cartes :

– pour les porteurs, se pose la question de la possibilité de réaliser des transactions par carte dans les pays n'ayant pas migré à la puce. Les solutions envisagées consisteraient à les doter de deux cartes différentes, l'une à piste, l'autre à puce, en fonction des usages envisagés ;

– pour certains accepteurs, le fait de se voir imposer l'utilisation de la puce lors de toute transaction peut avoir des conséquences opérationnelles importantes. Les sociétés d'autoroutes, par exemple, utilisent aujourd'hui, pour des raisons de rapidité, exclusivement la piste magnétique pour le paiement aux péages ;

– pour les émetteurs, les problématiques semblent plus nombreuses et couvrir différents domaines : tout d'abord, la distribution de cartes à puce induit une modification dans le processus industriel de fabrication et de personnalisation, lequel peut s'avérer long à mettre en œuvre. Ensuite, l'émission de cartes à puce seule rend inopérante toute procédure de secours en cas d'indisponibilité de la puce, par exemple en utilisant la piste magnétique[83]. Enfin, la commercialisation de différentes cartes en fonction des usages pourrait peut-être avoir des conséquences sur les conditions tarifaires des banques, selon que les coûts induits par ces nouvelles cartes sont répercutés ou non sur la clientèle ;

Les solutions alternatives

Afin de répondre à ces problématiques, certains pays ont proposé des solutions alternatives à la suppression de la piste. Il ne s'agit alors pas de prévenir toute tentative de « skimming », mais de limiter les cas possibles de réutilisation des données compromises sur différents environnements.

Parmi ces solutions, la désactivation des cartes sur certaines zones géographiques permet d'interdire leur utilisation en mode piste dans les pays n'ayant pas déployé EMV. A l'initiative du porteur, ou sous l'impulsion plus directe de l'émetteur, l'acceptation de la carte peut ainsi être géographiquement restreinte, limitant par là-même les possibilités de fraude.

Cette solution présente l'intérêt de ne pas émettre deux cartes différentes en fonction de leurs usages. Elle nécessite toutefois une démarche volontaire du porteur envers sa banque, qui peut être fréquente si ce dernier voyage régulièrement dans un pays n'ayant pas migré à EMV,

80 Intitulé "EU Organised Crime Threat Assessment 2011".

81 European Payment Council, organe représentatif des banques au niveau européen.

82 Résolution « Preventing Card Fraud in a mature EMV Environment », janvier 2011.

83 Cette procédure, dite de « fallback », est toutefois fortement déconseillée par l'EPC.

comme les États-Unis d'Amérique. En outre, cette solution nécessite une communication incitative de la part des émetteurs de façon à couvrir une part la plus large possible de leur clientèle.

Pour sécuriser les paiements par carte à distance

L'authentification renforcée du porteur

La saisie du cryptogramme visuel CVx2, rendue obligatoire dès 2003 sur les sites marchands hébergés en France, reste souvent optionnelle sur les sites d'autres pays. Une tendance de fond existe aujourd'hui, tant de la part des systèmes de paiement par carte internationaux que des banques elles-mêmes, visant à généraliser ce procédé. Toutefois, si le CVx2 permet de lutter contre la réutilisation frauduleuse des données de la carte obtenues par « skimming » [84], il ne permet pas de s'assurer que le porteur est bien celui qu'il prétend être, ce qui peut s'avérer déterminant en cas de vol du support par exemple[85].

Le principal enjeu sécuritaire dans le domaine des paiements par carte à distance est donc de renforcer l'authentification du porteur en ligne, comme l'Observatoire le préconise dans son rapport de 2008[86], en promouvant les mécanismes d'authentification dite « non rejouable » chaque fois que cela est possible et pertinent. Sa mise en œuvre repose très majoritairement aujourd'hui sur l'utilisation du protocole « 3D-Secure »[87], lequel permet à la banque du porteur d'authentifier son client au moyen de divers procédés (généralement en lui envoyant un code à usage unique par SMS).

En France, le Groupement des Cartes Bancaires « CB » a adopté le protocole « 3D-Secure » en octobre 2008 et les banques ont achevé d'équiper leurs porteurs en authentification non rejouable en 2010 (cf. chapitre 3). Toutefois, afin de rendre le dispositif totalement opérationnel et efficace, les efforts des parties prenantes (banques, systèmes de paiement par carte et commerçants) doivent désormais porter sur deux axes d'amélioration :

– « 3D-Secure » (ou tout protocole équivalent) doit être déployé sur l'ensemble des sites marchands, afin d'éviter le déplacement de la fraude vers les sites les moins protégés ;

– ce déploiement doit de plus être orchestré au niveau international, afin cette fois d'éviter le déplacement de la fraude vers les pays les moins protégés.

L'authentification du porteur lors d'achats en ligne peut également être mise en œuvre par d'autres dispositifs, tel que celui proposé par « Buyster », établissement de paiement créé par les trois plus importants opérateurs de téléphonie mobile (Orange, SFR, Bouygues) et agréé en France. La généralisation de ce type de solutions permettra également de contribuer à la lutte contre la fraude sur les paiements à distance.

---

84 En effet, n'étant pas présent sur la piste magnétique, il ne peut être copié par ce moyen.

85 Le code CVx2 peut également avoir été visuellement copié depuis le support physique même, ou intercepté lors d'une transaction à distance, avec les autres données de la carte.

86 Voir rapport 2008, chapitre 3.1.

87 Protocole, déployé dès 2001 par Visa Inc. puis adopté par la suite par Mastercard Worldwide, prévoyant une redirection de l'internaute vers sa banque lors d'un achat en ligne. « 3D-Secure » n'a été progressivement déployé en France qu'à partir d'octobre 2008, date d'entrée en vigueur du transfert de responsabilité en cas de fraude vers l'émetteur de la carte.

Les solutions alternatives

Plutôt que de devoir protéger les données de carte contre le vol à cause de leur caractère réutilisable notamment en paiement à distance, une autre solution consiste à remplacer ces données statiques par des données dynamiques, à usage unique. Ces numéros sont utilisables aussi bien sur Internet que par téléphone ou par courrier. On retrouve dans cette catégorie de solutions ce qui est communément appelé « cartes de paiement virtuelles ».

Un numéro de carte est dit dynamique lorsqu'il n'est associé qu'à une seule opération de paiement et ne peut resservir. La difficulté technique associée à la mise en œuvre d'une telle solution est la délivrance par la banque émettrice des numéros de carte à usage unique à ses porteurs en s'assurant de leur confidentialité. Lorsque la délivrance du numéro dynamique se fait par Internet, elle s'accompagne donc d'une authentification préalable du porteur qui elle aussi doit être renforcée sous peine de maintenir une vulnérabilité pour ce type de paiement.

5|3 Les évolutions des systèmes de paiement par carte

Panorama actuel des systèmes de paiement par carte et initiatives européennes

Le marché européen des cartes de paiement est actuellement dominé par les systèmes de paiement par carte internationaux (principalement Visa et Mastercard) qui, compte tenu de leur très large réseau d'acceptation, permettent aux porteurs de réaliser des paiements dans tous les pays européens et dans le monde.

Aux côtés de ces systèmes internationaux coexistent de nombreux systèmes domestiques interbancaires ou privatifs, d'importance très inégale et dont le réseau d'acceptation se limite aux frontières du pays concerné. Toutefois, un système de paiement par carte domestique a la possibilité de nouer des relations avec un ou plusieurs réseaux internationaux et d'apposer sa marque sur ses cartes, bénéficiant ainsi d'une acceptation étendue à l'international[88], en Europe et au-delà. C'est le cas par exemple du système de paiement Cartes Bancaires « CB » en France.

Dans ce contexte, l'Eurosystème, tout comme la Commission européenne, encouragent l'émergence d'initiatives menant à la création d'un ou plusieurs système(s) de paiement par carte européen(s) accompagnant la mise en œuvre d'une Europe des paiements telle que définie par le projet SEPA[89]. A ce jour, trois initiatives sont en cours :

– *EAPS* (« Euro Alliance of Payment Schemes ») permet aux systèmes nationaux de s'allier afin de devenir interopérables et ainsi étendre leur réseau d'acceptation au-delà de leurs frontières nationales. Ce projet regroupe ses membres fondateurs (Bancomat, Eufiserv, Euro 6000, Link, SIBS et Girocard). L'interopérabilité est assurée par un ensemble d'accords bilatéraux, dans l'objectif de bénéficier d'économies d'échelle associées à une forte augmentation du volume de transactions ;

– le projet *Monnet*, créé à l'initiative de banques françaises, allemandes, espagnoles, portugaises, italiennes et anglaises notamment, vise à la création ex-nihilo d'un système interbancaire régi par des règles applicables de façon multilatérale entre ses membres.

88 Pratique dite du « co-badgeage ».

89 Voir par exemple le 7ème rapport d'étape de l'Eurosystème sur SEPA.

Bien que voué à fédérer avant tout des établissements de crédit, ce projet resterait ouvert aux systèmes de paiement par carte nationaux ;

– *Payfair* enfin est présenté comme un nouveau système de paiement par carte à l'initiative des commerçants. Répondant aux préconisations de l'EPC, son enjeu est aujourd'hui principalement de s'adjoindre les services d'établissements émetteurs et acquéreurs.

Si l'émergence d'un système de paiement par carte européen aux côtés des systèmes internationaux peut aider à la mise en œuvre de mesures de sécurité répondant plus directement aux enjeux européens, il n'en reste pas moins nécessaire que les systèmes internationaux doivent également mettre en œuvre ces mesures afin d'assurer une égalité de concurrence entre les acteurs et d'éviter un déplacement de la fraude vers les pays les moins bien protégés au niveau international.

Une nécessaire harmonisation au plan européen

Quel que soit l'avenir du paysage européen dans le domaine de la carte, il suppose une mise à niveau de l'ensemble de ses acteurs, systèmes nationaux existants, initiatives en cours et systèmes internationaux en exercice au sein du SEPA, quant à la mise en œuvre de mesures permettant de répondre aux enjeux sécuritaires du paiement par carte au niveau européen.

A ce jour, plusieurs instances européennes, comme l'Eurosystème, Europol ou l'EPC, ont édicté des règles ou émis des recommandations visant à lutter contre le « skimming » et la fraude sur le paiement par carte à distance, les deux enjeux prioritaires de sécurité à ce jour.

Certaines de ces règles sont déjà implémentées par les systèmes en place au sein du SEPA. Les principaux systèmes internationaux ont par exemple déjà en partie intégré la sécurisation des supports et des transactions à distance, sans pour autant mettre en œuvre le retrait de la piste magnétique sur les cartes ou généraliser l'authentification non rejouable, seule à même de lutter efficacement contre la fraude sur Internet.

Pour autant, se pose la question de savoir comment s'assurer de la mise en œuvre coordonnée des recommandations émises en la matière, que ce soit au niveau des systèmes internationaux, des initiatives européennes en cours ou même des systèmes nationaux souhaitant répondre aux standards européens SEPA[90].

Certains acteurs plaident ainsi pour la mise en place d'une agence indépendante sous la responsabilité de la BCE et ayant pour mission de s'assurer que l'ensemble des systèmes actifs en Europe respectent les standards techniques conformes aux règles SEPA et qu'une plus grande transparence sur les statistiques de fraude au niveau européen soit instaurée.

La récente création du forum sur la sécurité des moyens de paiement de détail (« Forum on the SECUrity of REtail PAYments - SecuRe Pay »), sous l'égide de la BCE et réunissant les surveillants et superviseurs nationaux ainsi que des acteurs de marché le cas échéant, pourrait, dans ce contexte, répondre à ces préoccupations.

[90] Les travaux de mise en conformité au « SEPA Cards Framework » de l'EPC ne concernent pas uniquement les enjeux de sécurité mais abordent également des questions liées à la gouvernance des systèmes de paiement par carte et à leur mode de gestion des transactions. On citera notamment la séparation des fonctions de gouvernance et de traitement opérationnel des transactions, la contribution statistique à une base de fraude européenne, ou l'utilisation de protocoles de communication standardisés.

5|4 Conclusion

A l'heure où les systèmes de paiement par carte nationaux font face à de multiples choix pouvant engager leur avenir (se conformer ou non au SEPA, sous quelle forme...), les questions de sécurité apparaissent au centre des préoccupations et sont souvent décisives : la mise en conformité aux règles du SEPA peut en effet impacter durablement la gouvernance, la structure et la conduite des opérations de ces systèmes.

Parmi ces questions de sécurité, la lutte contre le « skimming » et la protection des paiements par carte à distance représentent des enjeux particulièrement importants, au regard de leur impact en terme de fraude. Si certaines mesures ont déjà été mises en œuvre dans ce cadre, comme l'émission de carte aux normes EMV ou le déploiement du protocole « 3D-Secure », elles ne répondent en l'état que partiellement aux enjeux soulevés. La migration aux normes EMV étant désormais quasiment achevée en Europe, se pose la question de la suppression de la piste sur les cartes ou du blocage de ces dernières sur les zones géographiques non migrées. Le protocole « 3D-Secure », ou toute solution équivalente permettant d'authentifier le porteur légitime de la carte, doit quant à lui s'accompagner de modes d'authentification basés sur des codes non rejouables connus du seul porteur et généralisés à l'ensemble des acteurs européens sur des bases restant à définir.

A l'heure où trois initiatives visant à créer un nouveau système de paiement par carte européen ont à ce jour été annoncées afin de proposer une alternative aux systèmes internationaux sur le marché européen des cartes de paiement, il convient de s'assurer que ces enjeux sécuritaires sont bien pris en compte par l'ensemble des acteurs, et les mesures adéquates adoptées de manière coordonnée afin d'assurer une égalité de traitement entre ces derniers.

La récente création du forum sur la sécurité des moyens de paiement de détail (« SecuRe Pay) », sous l'égide de la BCE et réunissant les surveillants et superviseurs nationaux ainsi que des acteurs de marché lorsque nécessaire, pourrait dans ce cadre permettre de contribuer efficacement à l'objectif d'harmonisation européenne de la sécurité ainsi que d'assurer une plus grande transparence dans les statistiques de fraude sur les paiements par carte en Europe.

ANNEXE A | 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 et 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 intra-communautaires

Les opérations de paiement concernées 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 (UE + Lichtenstein, Norvège et Islande), en euros ou dans la devise nationale d'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, au titulaire de la carte, l'opération non autorisée 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.

[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 entre en vigueur le 8 juillet 2010.

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.

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 intra-communautaires. 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

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

laquelle le client avait auparavant droit. A cette fin, les règles applicables aux opérations nationales ou intra-communautaires sont applicables avec des adaptations.

Ainsi, les opérations de paiement concernées par ces adaptations sont les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer, 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[3], 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, à Mayotte, 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] qui n'est pas partie à l'accord sur l'EEE (UE + Lichtenstein, Norvège et Islande).

ANNEXE B | 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 40 jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

– les cartes nationales permettent exclusivement d'effectuer des paiements ou des retraits 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 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. A 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 carte 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. A cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des cartes de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

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

En outre, le Ministre chargé de l'économie 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 C.

Les membres de l'Observatoire autres que 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 et des finances. Son mandat est de trois ans, renouvelable. Monsieur Christian NOYER, Gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément à l'article R. 142-3 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 de l'industrie 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 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 de déploiement de la technologie « 3D-Secure ».

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat, tenus au secret professionnel par l'article R. 142-25 du Code monétaire et financier, sont tenus de conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. A 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.

ANNEXE C | 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 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. 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

Représentant du secrétaire général de l'Autorité de contrôle prudentiel

Philippe RICHARD
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
Philippe HUBERT

Sur proposition du Ministre de l'économie, de l'industrie et de l'emploi :

– Le haut fonctionnaire de défense ou son représentant :
Claude MAUDELONDE

– Le directeur général du Trésor ou son représentant :
Alexis ZAJDENWEBER

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 :
Virginie GALLERAND

Sur proposition du garde des sceaux, Ministre de la justice :

– Le directeur des affaires criminelles et des grâces ou son représentant :
Alexandra VAILLANT
Nathalie KHOKHOLKOFF

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
Jean-Philippe RITZ

Sur proposition du Ministre de la défense :

– 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
Directeur – Fédération bancaire française

Bernard GOURAUD
Directeur des technologies – Banque Populaire – Caisse d'Epargne

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 VIGUIER
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 générale – Association FO Consommateurs (AFOC)

Christian HUARD
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 – Ecole 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)

ANNEXE D │ DOSSIER STATISTIQUE

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

- les 130 membres du Groupement des Cartes Bancaires « CB » par l'intermédiaire de celui-ci, 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 2010 : 88,6 millions

- dont 64,1 millions de cartes de type « interbancaire » (« CB », MasterCard et Moneo) ;
- et 24,4 millions de cartes de type « privatif ».

Cartes mises en opposition en 2010 : environ 640 000

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. A 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.

Le marché des cartes de paiement en France – Émission

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
Cartes de type « interbancaire »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiements de proximité et sur automate	6 453,78	284,62	112,41	7,24	29,40	3,08
Paiements à distance hors Internet	130,71	11,47	8,48	0,70	2,80	0,30
Paiements à distance sur Internet	324,03	26,22	76,88	3,48	9,04	0,65
Retraits	1 476,75	110,23	26,05	2,86	17,92	2,54
Total	**8 385,27**	**432,55**	**223,82**	**14,27**	**59,17**	**6,57**
Cartes de type « privatif »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiements de proximité et sur automate	179,78	15,68	5,27	0,95	5,77	0,86
Paiements à distance hors Internet	5,66	0,35	0,06	0,01	0,16	0,02
Paiements à distance sur Internet	4,53	0,59	0,50	0,05	1,55	0,10
Retraits	5,42	0,47	nd	nd	nd	nd
Total	**195,39**	**17,09**	**5,82**	**1,01**	**7,47**	**0,97**
Total général	**8 580,66**	**449,64**	**229,64**	**15,28**	**66,65**	**7,54**

Source : Observatoire de la sécurité des cartes de paiement

Le marché des cartes de paiement en France - Acquisition

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
Cartes de type « interbancaire »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiements de proximité et sur automate	6 453,78	284,62	134,52	9,64	30,15	3,95
Paiements à distance hors Internet	130,71	11,47	6,23	1,39	1,88	0,69
Paiements à distance sur Internet	324,03	26,22	13,16	1,72	2,54	0,37
Retraits	1 476,75	110,23	23,24	3,81	6,43	1,33
Total	**8 385,27**	**432,55**	**177,14**	**16,57**	**41,00**	**6,34**
Cartes de type « privatif »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiements de proximité et sur automate	179,78	15,68	5,31	1,33	4,20	1,37
Paiements à distance hors Internet	5,66	0,35	0,05	0,01	0,05	0,02
Paiements à distance sur Internet	4,53	0,59	0,24	0,04	0,26	0,04
Retraits	5,42	0,47	nd	nd	nd	nd
Total	**195,39**	**17,09**	**5,60**	**1,38**	**4,51**	**1,42**
Total général	**8 580,66**	**449,64**	**182,74**	**17,94**	**45,51**	**7,76**

Source : Observatoire de la sécurité des cartes de paiement

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire » - Émission

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**653,6**	**31 921,2**	**64,7**	**8 039,9**	**96,8**	**24 412,0**
Cartes perdues ou volées	608,6	29 334,9	42,2	3 793,2	18,8	4 085,4
Cartes non parvenues	6,9	349,6	0,9	112,1	0,1	10,5
Cartes altérées ou contrefaites	38,0	2 230,8	14,7	3 040,5	70,8	18 693,6
Numéro de carte usurpé	0,0	5,9	5,5	981,4	5,3	1 415,4
Autres	0,0	0,0	1,4	112,6	1,7	207,0
Paiements à distance hors Internet	**402,2**	**24 946,1**	**39,6**	**3 485,1**	**21,6**	**3 132,6**
Cartes perdues ou volées	1,4	98,6	13,0	1 604,4	8,1	1 116,6
Cartes non parvenues	0,0	1,0	0,1	3,2	0,0	7,4
Cartes altérées ou contrefaites	0,0	0,2	9,7	1 239,8	5,3	861,1
Numéro de carte usurpé	400,8	24 846,3	16,2	580,9	7,7	1 114,5
Autres	0,0	0,1	0,7	56,8	0,6	33,0
Paiements à distance sur Internet	**554,2**	**72 904,5**	**376,5**	**35 815,3**	**85,3**	**10 085,4**
Cartes perdues ou volées	4,6	290,5	120,2	10 686,1	27,3	3 073,0
Cartes non parvenues	0,7	0,7	0,4	27,0	0,1	6,1
Cartes altérées ou contrefaites	1,4	1,8	103,3	10 399,5	22,5	2 747,6
Numéro de carte usurpé	547,6	72 611,4	148,5	14 152,1	34,3	4 112,1
Autres	0,0	0,1	4,1	550,6	1,2	146,6
Retraits	**101,9**	**25 944,3**	**7,5**	**1 486,0**	**92,0**	**15 109,9**
Cartes perdues ou volées	97,2	24 964,0	4,2	883,8	11,4	1 502,4
Cartes non parvenues	0,4	106,1	0,0	4,7	0,0	8,7
Cartes altérées ou contrefaites	4,1	856,6	3,2	566,6	78,1	13 177,3
Numéro de carte usurpé	0,0	1,2	0,0	5,1	0,6	76,9
Autres	0,1	16,3	0,1	25,9	2,0	344,7
Total	**1 711,9**	**155 716,1**	**488,4**	**48 826,4**	**295,7**	**52 739,9**

Source : Observatoire de la sécurité des cartes de paiement

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**653,6**	**31 921,2**	**183,1**	**31 898,9**	**277,9**	**59 677,0**
Cartes perdues ou volées	608,6	29 334,9	70,7	3 210,9	45,3	9 682,8
Cartes non parvenues	6,9	349,6	3,0	172,8	3,4	645,8
Cartes altérées ou contrefaites	38,0	2 230,8	28,4	9 182,6	88,2	22 821,3
Numéro de carte usurpé	0,0	5,9	75,5	18 693,6	137,4	26 401,4
Autres	0,0	0,0	5,5	639,0	3,6	125,7
Paiements à distance hors Internet	**402,2**	**24 946,1**	**nd**	**nd**	**nd**	**nd**
Cartes perdues ou volées	1,4	98,6	nd	nd	nd	nd
Cartes non parvenues	0,0	1,0	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,0	0,2	nd	nd	nd	nd
Numéro de carte usurpé	400,8	24 846,3	nd	nd	nd	nd
Autres	0,0	0,1	nd	nd	nd	nd
Paiements à distance sur Internet	**554,2**	**72 904,5**	**nd**	**nd**	**nd**	**nd**
Cartes perdues ou volées	4,6	290,5	nd	nd	nd	nd
Cartes non parvenues	0,7	0,7	nd	nd	nd	nd
Cartes altérées ou contrefaites	1,4	1,8	nd	nd	nd	nd
Numéro de carte usurpé	547,6	72 611,4	nd	nd	nd	nd
Autres	0,0	0,1	nd	nd	nd	nd
Retraits	**101,9**	**25 944,3**	**4,4**	**1 232,5**	**2,5**	**1 367,2**
Cartes perdues ou volées	97,2	24 964,0	2,2	473,5	0,6	222,6
Cartes non parvenues	0,4	106,1	0,0	6,4	0,0	3,0
Cartes altérées ou contrefaites	4,1	856,6	2,0	730,4	1,8	1 125,7
Numéro de carte usurpé	0,0	1,2	0,1	15,1	0,1	11,1
Autres	0,1	16,3	0,0	7,1	0,0	4,8
Total	**1 711,9**	**155 716,1**	**187,5**	**33 131,4**	**280,4**	**61 044,2**

Source : Observatoire de la sécurité des cartes de paiement

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif » - Émission

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger SEPA		Émetteur français, Acquéreur étranger hors SEPA	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**7,46**	**4 252,46**	**4,83**	**1 112,72**	**6,54**	**1 403,60**
Cartes perdues ou volées	2,75	324,19	0,42	91,65	0,77	183,95
Cartes non parvenues	0,88	209,13	0,05	8,04	0,14	22,60
Cartes altérées ou contrefaites	0,86	204,85	1,58	427,60	4,73	846,97
Numéro de carte usurpé	0,65	261,38	2,59	541,94	0,89	346,26
Autres	2,32	3 252,92	0,21	43,49	0,01	3,82
Paiements à distance hors Internet	**6,89**	**2 324,24**	**3,20**	**532,87**	**2,62**	**643,35**
Cartes perdues ou volées	2,09	690,18	0,92	23,91	0,21	69,82
Cartes non parvenues	0,46	96,13	0,02	5,43	0,01	1,02
Cartes altérées ou contrefaites	2,13	584,69	0,88	115,58	1,17	207,73
Numéro de carte usurpé	1,40	575,59	1,33	357,80	1,24	364,15
Autres	0,81	377,66	0,05	30,15	0,01	0,63
Paiements à distance sur Internet	**1,37**	**965,73**	**0,60**	**154,85**	**0,57**	**108,31**
Cartes perdues ou volées	0,10	18,12	0,01	1,55	0,05	2,11
Cartes non parvenues	0,12	51,01	0,00	0,36	0,00	0,00
Cartes altérées ou contrefaites	0,03	1,93	0,01	1,65	0,02	0,52
Numéro de carte usurpé	0,87	732,90	0,58	151,06	0,50	105,16
Autres	0,25	161,76	0,00	0,22	0,00	0,52
Retraits	**2,71**	**570,57**	**nd**	**nd**	**nd**	**nd**
Cartes perdues ou volées	1,95	312,70	nd	nd	nd	nd
Cartes non parvenues	0,52	166,33	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,00	0,19	nd	nd	nd	nd
Autres	0,24	91,35	nd	nd	nd	nd
Total	**18,44**	**8 112,99**	**8,63**	**1 800,44**	**9,73**	**2 155,26**

Source : Observatoire de la sécurité des cartes de paiement

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

	Émetteur français, Acquéreur français		Émetteur étranger SEPA, Acquéreur français		Émetteur étranger hors SEPA, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**7,46**	**4 252,46**	**1,05**	**496,46**	**2,22**	**703,29**
Cartes perdues ou volées	2,75	324,19	0,06	8,60	0,14	20,64
Cartes non parvenues	0,88	209,13	0,03	0,86	0,00	0,44
Cartes altérées ou contrefaites	0,86	204,85	0,19	53,41	0,85	207,90
Numéro de carte usurpé	0,65	261,38	0,64	276,15	1,18	418,81
Autres	2,32	3 252,92	0,13	157,44	0,06	55,51
Paiements à distance hors Internet	**6,89**	**2 324,24**	**2,40**	**1 244,60**	**5,52**	**2 586,32**
Cartes perdues ou volées	2,09	690,18	0,38	119,42	0,97	347,71
Cartes non parvenues	0,46	96,13	0,03	6,96	0,00	0,00
Cartes altérées ou contrefaites	2,13	584,69	0,95	388,70	2,60	1 279,36
Numéro de carte usurpé	1,40	575,59	1,01	711,59	1,86	902,11
Autres	0,81	377,66	0,04	17,92	0,10	57,15
Paiements à distance sur Internet	**1,37**	**965,73**	**0,36**	**128,02**	**0,92**	**187,55**
Cartes perdues ou volées	0,10	18,12	0,02	16,64	0,02	3,56
Cartes non parvenues	0,12	51,01	0,00	0,11	0,00	0,37
Cartes altérées ou contrefaites	0,03	1,93	0,00	0,21	0,11	32,97
Numéro de carte usurpé	0,87	732,90	0,34	110,81	0,77	145,33
Autres	0,25	161,76	0,00	0,25	0,02	5,32
Retraits	**2,71**	**570,57**	**nd**	**nd**	**nd**	**nd**
Cartes perdues ou volées	1,95	312,70	nd	nd	nd	nd
Cartes non parvenues	0,52	166,33	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,00	0,19	nd	nd	nd	nd
Autres	0,24	91,35	nd	nd	nd	nd
Total	**18,44**	**8 112,99**	**3,81**	**1 869,08**	**8,67**	**3 477,16**

Source : Observatoire de la sécurité des cartes de paiement

ANNEXE E | DÉFINITION ET TYPOLOGIE DE LA FRAUDE RELATIVE AUX CARTES DE PAIEMENT

Définition de la fraude

A 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 :

1. 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 ;

2. 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 et carte utilisée en France,
  - émetteur français et carte utilisée à l'étranger ;
- le type de carte de paiement[2], y compris les porte-monnaie électroniques.

3. 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 obtenue à l'insu de son titulaire légitime, 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 ;
- *usurpation d'identité :* actes frauduleux liés à un paiement par carte et supposant l'utilisation de l'identité d'une autre personne ;
- *répudiation abusive :* contestation par le porteur, de mauvaise foi, d'un ordre de paiement valide dont il est l'initiateur ;

[3] Personal Account Number

– *piratage d'automates de paiement ou de retrait :* techniques qui consistent 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 ;

– l'émetteur est établi en France et l'acquéreur est établi à l'étranger ;

– l'émetteur est établi à l'étranger et l'acquéreur est établi en France.

Directeur de la publication **Robert Ophèle**
Directeur général des opérations
Banque de France

Rédacteur en chef **Yvon Lucas**
Directeur des systèmes de paiement
et infrastructures de marché
Banque de France

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 30 juin 2011
Dépôt légal 2ème trimestre 2011
ISSN 1768-2991