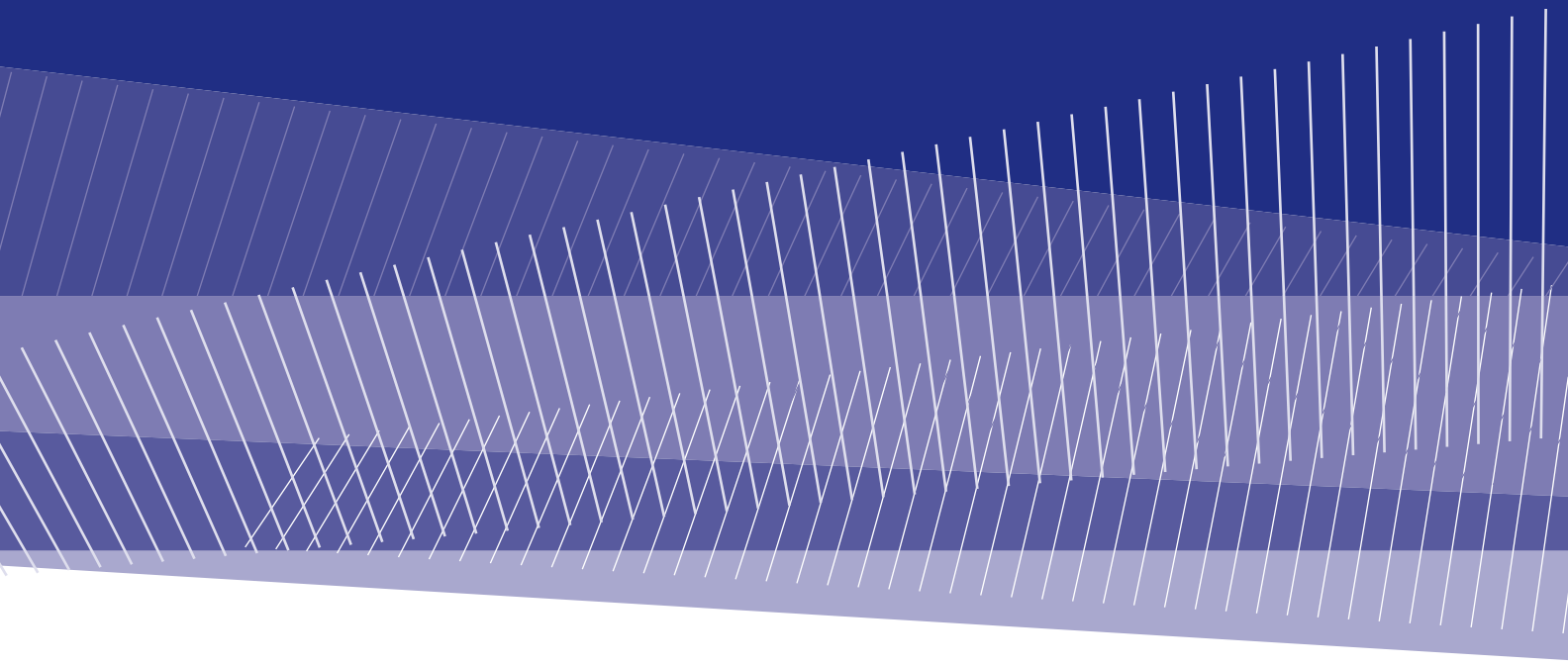
2007

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



Observatoire
de la sécurité
des cartes de paiement

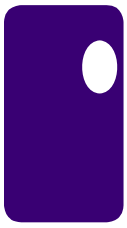
www.observatoire-cartes.fr

2007 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 2007
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Madame le Ministre de l'Économie, des finances et de l'emploi
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 7

1 | POLITIQUES DE SECURITE DES EMETTEURS ET DES ACCEPTEURS 9

Les systèmes d'acceptation concentrés 9
Les nouvelles offres de cartes prépayées 13

2 | STATISTIQUES DE FRAUDE POUR 2007 17

Vue d'ensemble 18
Répartition de la fraude par type de carte 19
Répartition de la fraude par zone géographique 20
Répartition de la fraude par type de transaction 21
Répartition de la fraude selon son origine 23

3 | VEILLE TECHNOLOGIQUE 27

Sécurité des paiements par carte et standardisation européenne 27
La sécurité des nouveaux mécanismes d'initiation du paiement par carte (paiement par téléphone mobile, carte sans contact) 36
État d'avancement de la migration EMV 43

4 | IMPACT DE LA DIRECTIVE SUR LES SERVICES DE PAIEMENT SUR LES RÈGLES APPLICABLES AUX CARTES DE PAIEMENT EN FRANCE 47

L'ouverture du marché des cartes à de nouveaux acteurs non bancaires 47
Une approche nouvelle de la réglementation applicable aux paiements 49
Harmonisation des obligations d'information 50
De nouvelles règles de révocation et de contestation 52
Conclusion 53

MISSIONS ET ORGANISATION DE L'OBSERVATOIRE 55

LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE 59

DOSSIER STATISTIQUE 63

AVANT-PROPOS

L'Observatoire de la sécurité des cartes de paiement a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne[1]. 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[2].

Conformément à l'alinéa 6 de l'article L. 141-4 du Code monétaire et financier, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'économie et des finances et transmis au Parlement. Il comprend en premier lieu deux études relatives aux politiques de sécurité des émetteurs et des accepteurs, l'une sur les systèmes d'acceptation concentrés, l'autre sur les nouvelles offres de cartes prépayées (1ère partie), puis une présentation des statistiques de fraude pour 2007 (2ème partie) et une synthèse des travaux conduits en matière de veille technologique (3ème partie). Enfin, le rapport comprend une étude portant sur l'impact de la directive sur les services de paiement sur les règles applicables aux cartes de paiement en France (4ème partie).

1 Les dispositions légales relatives à l'Observatoire figurent à l'article L. 141-4 du Code monétaire et financier.

2 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 d'établissements de crédit émetteurs et acquéreurs. Les seconds correspondent à ceux dans lesquels il existe un nombre réduit d'établissements de crédit émetteurs et acquéreurs.

1 POLITIQUES DE SECURITE DES EMETTEURS ET DES ACCEPTEURS

Dans le cadre de sa mission de suivi des politiques de sécurité mises en œuvre par les émetteurs et les accepteurs, l'Observatoire a mené en 2007 deux études : l'une sur les politiques de sécurité dans les systèmes d'acceptation concentrés, l'autre sur les mesures de sécurité appliquées aux nouvelles offres de cartes prépayées. Sur la base d'informations recueillies par questionnaire respectivement auprès de représentants d'accepteurs et d'industriels et auprès de représentants d'émetteurs, l'Observatoire a étudié les mesures de sécurité mises en œuvre pour les différents dispositifs concernés.

1 1 Les systèmes d'acceptation concentrés

Pour faire suite à son étude de 2005 relative à la protection des données de cartes dans la filière acquisition, l'Observatoire a étudié en 2007 la sécurité des systèmes d'acceptation concentrés utilisés par certains commerces. La question de la protection des données de cartes se pose en effet différemment dans de tels systèmes, constitués de plusieurs équipements jouant chacun un rôle dans la gestion de ces données. Un système d'acceptation concentré se compose en effet généralement d'un ensemble de terminaux ou d'automates de paiement, installés aux caisses du magasin et reliés à un serveur central. C'est ce dernier qui concentre les données de paiement et effectue la liaison avec les serveurs des acquéreurs. Compte tenu de la masse de données traitées, la protection de ces systèmes requiert une attention particulière.

Les systèmes d'acceptation concentrés sont déployés largement en France puisqu'ils concernent près de 150 000 terminaux d'acceptation et 50 000 automates de paiement, soit près de 20 % des points d'acceptation installés en France.

Pour la réalisation de cette étude, le secrétariat de l'Observatoire a recueilli les informations utiles sur la base d'un questionnaire renseigné par des représentants des établissements acquéreurs et des représentants du commerce membres de l'Observatoire[3], ainsi que par la société Ingenico. Y ont également répondu les constructeurs de systèmes d'acceptation au travers de leur association professionnelle, le « CONCERT International ».

Description des systèmes d'acceptation concentrés

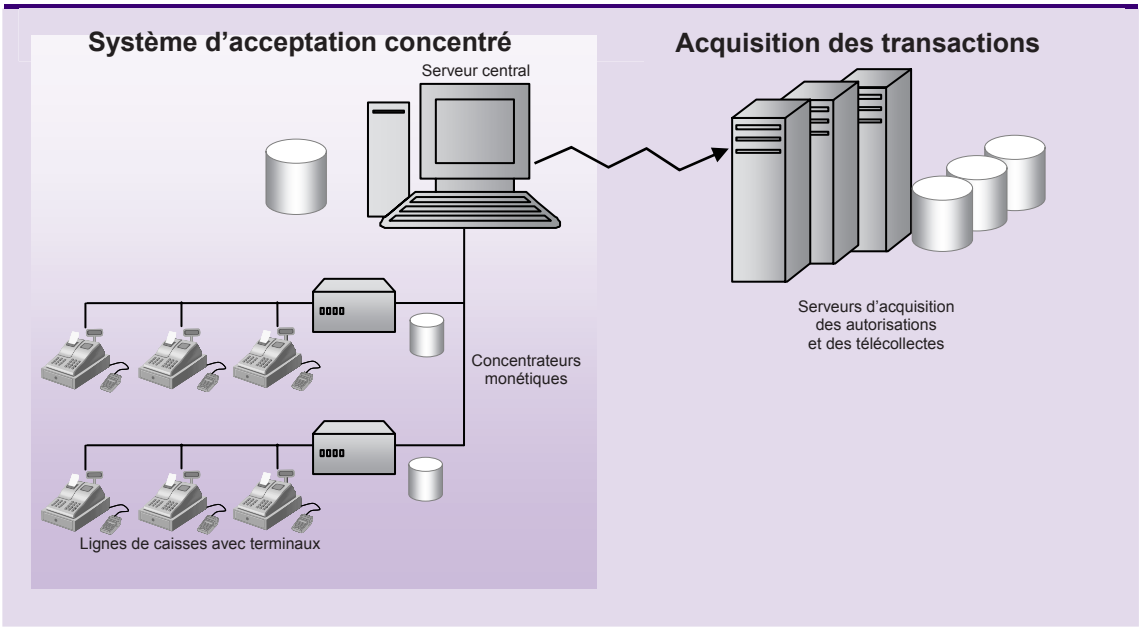
Contrairement aux points d'acceptation composés d'un simple « terminal de paiement autonome », relié à la caisse du magasin et connecté par les réseaux de communication au serveur de la banque acquéreur, l'organisation type d'un système d'acceptation concentré met en jeu différents niveaux de matériels. Les transactions des porteurs sont effectuées sur les terminaux associés aux caisses du magasin, celles-ci étant chacune connectée à un équipement informatique fédérateur, le concentrateur monétique. Les concentrateurs monétiques présents dans le système sont à leur tour reliés au serveur central, qui

[3] Caisse d'Epargne, Crédit Agricole, Groupement des Cartes Bancaires « CB », Mercatel

communique avec les centres d'acquisition, à la fois pour les processus d'autorisation et de télécollecte des transactions. Pour les besoins de l'étude, l'ensemble des opérations allant du paiement par carte à la caisse jusqu'à la transmission des données de transaction aux serveurs des banques acquéreurs a été pris en compte. Ceci inclut également les opérations d'archivage ou de gestion d'historique.

Les équipements composant un système d'acceptation concentré couvrent un grand nombre de fonctions, depuis la gestion de la caisse, du terminal, jusqu'au traitement et à l'archivage des données. Les constructeurs de ces matériels sont ainsi généralement en charge de leur conception mais également dans de nombreux cas de leur installation et de leur maintenance. Compte tenu de la complexité de mise en œuvre et de fonctionnement des matériels utilisés, ceux-ci doivent se conformer à un certain nombre de prescriptions de sécurité auxquelles sont attentifs les systèmes de paiement par carte, les banques, les commerçants, ainsi que les constructeurs eux-mêmes.

Encadré 1 – Schéma type de l'organisation d'un système d'acceptation concentré



Les données traitées dans les systèmes d'acceptation concentrés comportent le numéro de la carte, la date de fin de validité, le nom du porteur et les données de la piste magnétique (si elles sont lues). Ces données sont parfois stockées au niveau du concentrateur monétique ou du serveur central. Les données de la transaction (date, heure, montant, nature de l'objet acheté) peuvent également être stockées à ces différents niveaux. La manipulation de ces données est une opération sensible en termes de sécurité. Le personnel de caisse des commerçants est donc amené à respecter un certain nombre de prescriptions.

La sécurité des systèmes d'acceptation concentrés

Les données traitées et stockées dans les systèmes d'acceptation concentrés constituent, notamment en raison des volumes traités, des éléments sensibles, qui, s'ils étaient détournés ou copiés, pourraient être utilisés pour réaliser des paiements frauduleux.

Les représentants des acquéreurs, des commerçants et des fabricants de terminaux interrogés considèrent que les principales mesures de sécurité à mettre en œuvre doivent viser à protéger

les données traitées dans les terminaux de paiement ou stockées dans les systèmes d'information du commerçant, afin de se prémunir contre le vol de données.

Les banques acquéreurs requièrent ainsi de leurs clients commerçants qu'ils se conforment à un certain nombre d'exigences sécuritaires, d'ordre organisationnel et technique, élaborées par les systèmes de carte. Ces mesures de sécurité, qui sont reprises dans les contrats commerçants, incluent notamment les prescriptions du programme PCI DSS[4], programme qui spécifie un ensemble de dispositions de sécurité applicables pour le stockage des données et la conduite d'audits.

Protection du terminal de paiement électronique

Des mesures de sécurité sont mises en œuvre pour le personnel de caisse. L'une de ces mesures peut consister à ce que ce personnel ait le moins de contact possible avec la carte, afin d'empêcher l'installation de dispositifs de type « skimming »[5] ou la capture visuelle de données sensibles. De plus, les commerçants mettent en place une ségrégation des tâches et des contrôles stricts pour restreindre l'accès aux données sensibles uniquement aux personnes autorisées.

En complément, les commerçants sont tenus de s'équiper avec du matériel agréé et respectant les standards internationaux, tels que EMV[6], qui assure une protection accrue de la transaction, ou encore PCI PED[7], qui protège la saisie du code PIN sur le terminal de paiement.

Par ailleurs, afin de renforcer la sécurité des systèmes d'exploitation installés sur les différents matériels, la plupart des constructeurs font en sorte que le système d'exploitation du terminal, celui de l'application du client et le logiciel qui personnalise le terminal soient codés par des personnes différentes. De plus, les secrets présents dans les terminaux sont générés dans des sites certifiés à très haute sécurité.

Enfin, concernant les opérations de maintenance, des précautions particulières sont prises, telles que la traçabilité de l'ouverture de l'enceinte sécuritaire et la perte des « secrets bancaires » en cas d'ouverture non contrôlée des terminaux. De plus, dans de nombreux cas, le personnel de maintenance ne peut modifier lui-même le terminal de paiement électronique, qui doit alors être renvoyé chez le constructeur et suivre une nouvelle procédure de certification.

Protection du concentrateur monétique et du serveur central

Les standards PCI DSS exigent une protection physique des systèmes et l'utilisation de caméras pour surveiller les zones sensibles.

En complément, PCI DSS impose une protection logique des données, avec notamment la mise en place de pare-feux, l'utilisation systématique d'anti-virus actualisés sur tous les systèmes, le cryptage des données stockées et transmises, l'interdiction de stocker les données de la piste et le code PIN, l'attribution d'un identifiant unique à chaque personne disposant d'un accès, ainsi qu'une gestion des mots de passe sécurisée. Ainsi, les données de la carte et le code PIN sont transmis uniquement lors de la phase d'autorisation du paiement et sous forme cryptée.

---

4 Payment Card Industry – Data Security Standard (PCI DSS). Cf. Rapport annuel 2005 de l'Observatoire, encadré 3 p. 14

5 Cf. Rapport annuel 2003 de l'Observatoire, p. 22

6 Europay MasterCard Visa (EMV). Cf. Rapport annuel 2003 de l'Observatoire, encadré 13 p. 38

7 Payment Card Industry – Pin Entry Device (PCI PED)

Les représentants des commerçants ont toutefois rappelé que certaines des dispositions de protection prévues par PCI DSS pour les transactions en mode piste leur paraissaient inadaptées au contexte français dans la mesure où la grande majorité des paiements s'effectue en mode puce (EMV).

L'ensemble de ces mesures protège les données sensibles et le système d'acceptation concentré contre des attaques internes ou externes qui viseraient soit à le mettre hors service, soit à y pénétrer frauduleusement.

Certification des systèmes et suivi de la fraude

Les processus de certification mis en place par les systèmes de carte permettent de s'assurer de la bonne conformité des équipements aux référentiels de sécurité (cartes et terminaux compris), ce qui contribue à mieux protéger les données sensibles échangées.

Dans ce cadre, les industriels apportent une attention particulière au cycle de certification des systèmes d'acceptation concentrés, potentiellement plus long en raison d'une complexité accrue par rapport aux terminaux de paiement autonomes. Afin d'optimiser le processus de certification dans son ensemble, certains systèmes de carte et organismes de standardisation publient ainsi des versions de travail des spécifications à venir, ce qui permet aux constructeurs d'anticiper l'évolution de leurs matériels.

Par ailleurs, la mise en place d'audits est nécessaire pour assurer la bonne mise en œuvre de ces mesures de sécurité. Dans le cadre de PCI DSS, les commerçants réalisant un volume important de transactions par carte (typiquement les commerçants équipés de systèmes d'acceptation concentrés) doivent être régulièrement audités par des cabinets indépendants et certifiés par PCI SSC (« Payment Card Industry - Security Standards Council »). Ils doivent en particulier réaliser un audit annuel de sécurité sur le site de leur système d'information, ainsi qu'une analyse trimestrielle des vulnérabilités de leur réseau de télécommunication.

Enfin, d'après les informations recueillies lors de l'étude, les fraudes répertoriées font systématiquement l'objet d'une plainte par les commerçants et les acteurs concernés prêtent leur concours aux forces de police et de gendarmerie. En outre, le Groupement des Cartes Bancaires « CB » a mis en place un dispositif d'alerte systématique prévoyant qu'en cas de problème détecté sur un matériel donné, une notification du type d'attaque et un descriptif complet sont adressés à ses membres.

Conclusion

Les systèmes d'acceptation concentrés sont des dispositifs importants au sein de la chaîne de paiement car ils traitent un volume conséquent de données sensibles. Leur déploiement est très large en France puisqu'ils représentent près de 20 % du parc des terminaux et automates de paiement. Il est donc important d'empêcher le détournement de ces données à des fins malveillantes (contrefaçon, utilisation frauduleuse). En conséquence, des mesures de protection physique et logique doivent être mises en place, afin de se prémunir contre des attaques internes ou externes au système.

Les réponses fournies dans le cadre de l'étude conduite par l'Observatoire montrent que les différents acteurs sont conscients de ces enjeux et travaillent à la fois à l'élaboration de standards appropriés en matière de sécurité, mais également à la bonne application des recommandations sécuritaires, notamment au travers de programmes de certification couvrant l'ensemble des équipements et systèmes. La généralisation de la mise en œuvre de ces

standards est donc essentielle pour mieux protéger les données sensibles traitées par les systèmes d'acceptation concentrés.

Enfin, il apparaît que très peu de cas de compromission ont été répertoriés. Tous ont fait l'objet d'une plainte et d'une mise en alerte par le Groupement des Cartes Bancaires « CB », permettant d'une part de limiter leur impact, et d'autre part de résoudre les problèmes rencontrés sous de brefs délais.

1|2 Les nouvelles offres de cartes prépayées

L'Observatoire a mené en 2007 une étude sur les mesures de sécurité appliquées aux nouvelles offres de cartes prépayées, en particulier celles destinées à la clientèle jeune (« cartes cadeaux », « cartes jeunes », cartes « Moneo »). Cette clientèle, dont l'âge ne permet pas toujours la bancarisation, bénéficie par cette offre de l'accès à un moyen de paiement largement accepté. Les conditions d'emploi de ces cartes diffèrent toutefois de celles qui existent pour les cartes de paiement liées à un compte et ont été adaptées au cas particulier de la clientèle jeune. Aussi, l'Observatoire a souhaité mieux connaître ces conditions, ainsi que, plus largement, les mesures prises par les émetteurs afin de limiter les risques de fraude pour ces cartes, notamment pour protéger les porteurs en cas de vol ou de perte.

Pour ce faire, les informations utiles ont été recueillies, sur la base d'un questionnaire renseigné par des représentants des émetteurs de cartes de paiement de type « interbancaire » et de type « privatif », membres de l'Observatoire[8].

L'étude a permis de recueillir des informations principalement sur les cartes cadeaux et les cartes jeunes de type « interbancaire », ainsi que les cartes Moneo. Certains émetteurs de cartes de paiement de type « privatif » émettent aussi des cartes cadeaux, essentiellement afin de récompenser la fidélité de leurs porteurs. Il est également à noter que l'appellation « carte cadeau » est fréquemment employée par des commerçants pour désigner des cartes utilisables uniquement dans leur enseigne, mais que celles-ci ne sont juridiquement pas des cartes de paiement et n'entrent donc pas dans le champ de cette étude.

Descriptif des différents types de cartes prépayées

L'enquête conduite par l'Observatoire permet de distinguer deux modes de fonctionnement des cartes prépayées émises aujourd'hui en France. En effet, les fonds versés au crédit de la carte peuvent être enregistrés soit sur le système informatique de l'émetteur (enregistrement sur un serveur), soit sur la carte elle-même (enregistrement sur la puce).

Les cartes prépayées dont la valeur est enregistrée sur le serveur de l'émetteur (« cartes cadeaux », « cartes jeunes »)

Les « cartes cadeaux » ou autres « cartes jeunes » distribuées par les émetteurs bancaires français depuis environ trois ans sont des cartes de débit immédiat « CB », généralement co-badgées[9] avec Visa ou MasterCard. Environ 70 000 cartes de ce type sont actuellement

[8] Caisse d'Epargne, Banque Populaire, Crédit Agricole, CETELEM, La Banque Postale, BMS

[9] Le « co-badgeage » (« co-badging ») est l'apposition sur les cartes de paiement de logos de réseaux de cartes partenaires. Il se distingue du « co-marquage » (« co-branding ») qui consiste en l'apposition, en plus du logo de l'établissement de crédit émetteur, d'une marque d'un partenaire commercial.

utilisées en France. Ces cartes sont liées à une réserve de fonds prépayés à l'émetteur. Les fonds sont généralement apportés par une personne distincte du porteur, par exemple des parents. Lorsque le porteur désigné est un mineur, son représentant légal assure la responsabilité juridique du titulaire.

Ces cartes permettent le paiement de proximité et sur automate en France et à l'étranger et, selon le choix de l'émetteur, le paiement à distance et le retrait d'espèces. Elles offrent le même niveau de sécurité que toute carte « CB » : elles sont équipées d'une puce et leur utilisation requiert la frappe du code confidentiel. Le paiement ou le retrait ne sont possibles que dans la limite des fonds prépayés. C'est pourquoi ces cartes fonctionnent en autorisation systématique : chaque transaction donne lieu à une vérification en ligne que son montant est compatible avec la réserve de fonds prépayés qui reste disponible. L'émetteur gère la provision disponible de la carte dans un « compte technique » inscrit sur un serveur informatique. Le montant maximum prépayé est compris entre quelques dizaines et quelques centaines d'euros. Ces cartes peuvent, selon le choix de l'émetteur, être rechargeables ou non. Leur durée de validité est généralement limitée à un an.

Les cartes prépayées dont la valeur est enregistrée sur la carte (cartes « Moneo »)

Les émetteurs français de cartes de type « interbancaire » mettent à la disposition de leur clientèle depuis près de dix ans des cartes prépayées dites « porte-monnaie électroniques », les cartes « Moneo ». Environ un million de cartes Moneo sont actuellement utilisées en France. Il en existe trois types. Le premier est une carte bancaire « CB » sur laquelle la fonction Moneo est ajoutée, ce qui permet au porteur de choisir d'utiliser cette fonction pour ses achats de petit montant. Le prépaiement du porte-monnaie électronique est dans ce cas nécessairement effectué par débit du compte auquel est liée la carte « CB ». Le deuxième type de carte Moneo est appelé « Moneo bleu ». Comme dans le premier cas, cette carte est également liée à un compte bancaire et prépayée par débit de celui-ci. La différence par rapport à la précédente est que le porte-monnaie électronique n'est pas couplé à une carte « CB » et que le compte auquel il est attaché peut être un compte bancaire distinct de celui auquel est liée la carte « CB » du porteur. Le troisième type de carte Moneo est appelé « Moneo vert ». Il s'agit ici d'une carte anonyme, non liée à un compte, et prépayée par débit d'une carte « CB » ou par achat de coupons prépayés. Le développement de l'usage de Moneo dans les restaurants universitaires depuis deux ans s'appuie principalement sur la diffusion de Moneo verts.

Pour toutes les cartes Moneo, le paiement se fait sans saisie de code confidentiel ni demande d'autorisation (transaction dite « off-line »). Seul le rechargement des Moneo associés à un compte nécessite la frappe du code confidentiel. Les paiements sont limités à 30 euros et le solde maximum de la carte à 100 euros. Ces cartes ne permettent pas le retrait d'espèces. Certaines peuvent fonctionner aussi en mode dit « sans contact ».

La sécurité des cartes prépayées

Les cartes prépayées peuvent susciter un intérêt pour les fraudeurs ou les voleurs dans la mesure où elles peuvent représenter l'espoir d'un pouvoir d'achat immédiat. L'Observatoire souhaitait vérifier que les porteurs, notamment la population jeune, n'étaient pas de ce fait exposés à un risque accru d'agression physique. Les informations recueillies auprès des représentants des émetteurs montrent que les dispositifs de sécurité semblent avoir été adaptés à ce contexte. Les mesures appliquées aux cartes prépayées varient selon que la valeur prépayée est stockée sur un serveur ou sur la carte.

Les cartes prépayées dont la valeur est enregistrée sur le serveur de l'émetteur

Par définition, ces cartes ne sont pas exposées à des risques de détournement de la valeur inscrite sur la carte ou de création de fausse valeur. Les fonds restent détenus par l'émetteur et sont ainsi protégés comme dans le cas d'une carte de débit classique. Ce qui importe est donc que la carte ne puisse être utilisée à l'insu du porteur légitime.

Les émetteurs interrogés ont fait valoir que les cartes cadeaux et les cartes jeunes sont inactivées lorsqu'elles sont distribuées, même si le compte auquel elles sont rattachées est par définition prépayé. Cela signifie que le porteur doit les activer par une procédure prévue par l'émetteur pour pouvoir en faire usage. Chez un certain nombre d'émetteurs, ces cartes sont livrées en agence pour réduire encore le risque de détournement dans le circuit d'acheminement.

Une fois reçue et activée par le porteur légitime, la carte ne peut être utilisée à chaque transaction qu'avec saisie du code PIN, dont l'authenticité est vérifiée de manière cryptographique. Les transactions en vente à distance sont autorisées par certains émetteurs mais elles requièrent la frappe du cryptogramme visuel CVx2[10] et elles doivent également donner lieu à demande d'autorisation systématique.

Par ailleurs, l'intérêt pour les fraudeurs de contrefaire ces cartes est limité du fait que certains émetteurs ne permettent pas le retrait sur les distributeurs de billets, en France et à l'étranger. En cas de contrefaçon, les dispositions légales relatives à l'exonération de la responsabilité du porteur s'appliquent. En cas de perte ou de vol, les mécanismes habituels de mise en opposition prévalent.

Les cartes prépayées dont la valeur est enregistrée sur la carte

Ce type de carte présente un intérêt pour le voleur puisque celui-ci pourra directement réutiliser la valeur électronique enregistrée. En effet, les transactions ne sont pas protégées par code PIN compte tenu qu'elles sont de petit montant. La valeur prépayée restant enregistrée sur la carte perdue ou volée n'est pas remboursée au porteur légitime, qui est donc dans la même situation qu'en cas de perte de billets ou de pièces. Toutefois, les émetteurs ont souhaité limiter ce risque en plafonnant le chargement de la carte Moneo à 100 euros, ainsi que les transactions de paiement à 30 euros. Les émetteurs interrogés ont fait remarquer que la faiblesse des montants en jeu avait certainement contribué à limiter l'intérêt du vol par agression de cartes Moneo.

Il est également à noter qu'en cas d'opposition par le porteur pour perte ou vol, les rechargements des cartes Moneo liées à un compte sont automatiquement bloqués. La mise en opposition n'a pas de sens pour les Moneo verts, compte tenu qu'ils ne sont pas liés à un compte et qu'ils sont anonymes. Ces cartes pourraient continuer à être chargées mais cela suppose que le voleur les approvisionne, ce qui est peu probable.

Lors des transactions de paiement, les cartes Moneo sont authentifiées de façon dynamique par le terminal du commerçant. Ainsi, la contrefaçon des cartes, dont le composant électronique est par ailleurs évalué dans le cadre du Schéma national d'évaluation et de certification[11], est techniquement difficile et présente peu d'intérêt au regard des sommes enregistrées sur la carte.

---

[10] Cf. Rapport annuel 2005 de l'Observatoire, encadré 2 p. 13

[11] Cf. Rapport annuel 2005 de l'Observatoire, encadré 6 p. 30

Il existe également depuis peu des cartes Moneo fonctionnant en mode sans contact. S'agissant de cartes prépayées, le risque de détournement de valeur à l'insu du porteur (« télé-pickpocketing », cf. 3.2) n'est pas négligeable. Les politiques de sécurité des émetteurs et les mesures mises en œuvre réduisent toutefois la portée de ce risque. En particulier, compte tenu du mode de fonctionnement du porte-monnaie électronique Moneo, la valeur électronique qui serait détournée ne pourrait être convertie en monnaie scripturale que si elle était présentée à l'encaissement auprès d'un établissement de crédit.

Conclusion

Les offres de cartes prépayées proposées aujourd'hui à la clientèle française, notamment aux jeunes, se classent en deux grandes catégories en termes de mesures de sécurité.

Il existe d'une part des cartes prépayées dont la valeur reste enregistrée dans le système d'information de l'émetteur. Ces cartes, comme les cartes cadeaux ou les cartes jeunes de type « interbancaire », sont des cartes de débit immédiat à autorisation systématique. Les porteurs qui les utilisent bénéficient donc à la fois des protections en vigueur pour les cartes de paiement de type « interbancaire », comme la saisie du code PIN, mais aussi de mesures spécifiques. C'est le cas de la demande d'autorisation systématique et du plafonnement de la carte, qui réduisent les réutilisations possibles de la carte en cas de perte ou de vol.

Il existe d'autre part des cartes prépayées dont la valeur est enregistrée sur la carte utilisée par le porteur, comme les cartes Moneo. Celles-ci présentent donc un risque plus élevé de réutilisation en cas de perte ou de vol par le porteur légitime, d'autant que les transactions, qui sont généralement de petit montant, ne donnent pas lieu à saisie du code PIN. La protection du porteur est principalement assurée par le plafonnement des montants enregistrés sur la carte. Ceux-ci sont maintenus volontairement bas pour ne pas susciter d'intérêt particulier au regard du vol.

Les émetteurs interrogés ont en outre fait valoir qu'ils n'avaient relevé pour l'instant qu'un nombre marginal de cas de fraude sur leurs cartes prépayées.

2 | STATISTIQUES DE FRAUDE POUR 2007

Depuis 2003, l'Observatoire établit des statistiques de fraude des 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[12]. Une synthèse des statistiques pour 2007 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou 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 C de ce rapport.

Encadré 2 – Statistiques de fraude : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire s'appuie sur un échantillon de contributeurs qui rassemble les acteurs (émetteurs et commerçants) les plus représentatifs des systèmes de paiement par carte, qu'ils soient de type « interbancaire » ou « privatif ».
Les données fournies à l'Observatoire par les émetteurs portent ainsi sur :

– 381,1 milliards d'euros de transactions réalisées en France et à l'étranger à l'aide de 55,7 millions de cartes de type « interbancaire » émises en France (dont 1,1 million de porte-monnaie électroniques) ;
– 25,8 milliards d'euros de transactions réalisées (principalement en France) avec 25,7 millions de cartes de type « privatif » émises en France ;
– 23,8 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.

Émetteurs de cartes

Les données recueillies proviennent :

– de neuf émetteurs de cartes privatives : American Express, Banque Accord, Cetelem, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;
– des 150 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que d'Europay France et du Groupement Carte Bleue pour les données internationales ;
– des émetteurs du porte-monnaie électronique Moneo.

Commerçants

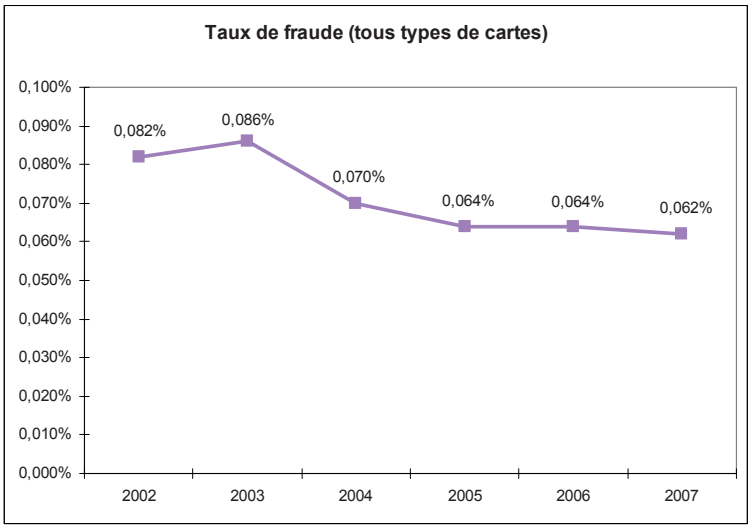
L'Observatoire a recueilli des statistiques de fraude auprès :

– d'accepteurs de cartes de paiement : France Loisirs, Monoprix et la SNCF ;
– de la Fédération du e-commerce et de la vente à distance (Fevad). Les données ont été obtenues auprès d'un échantillon de 30 entreprises représentant 45 % du chiffre d'affaires de la vente à distance aux particuliers ;
– de la Fédération des entreprises du commerce et de la distribution (FCD) et de Mercatel. Les données ont été collectées auprès d'un échantillon représentant environ 40 % du marché de la grande distribution et du commerce spécialisé.

[12] Cf. Rapport annuel 2003 de l'Observatoire, partie 3

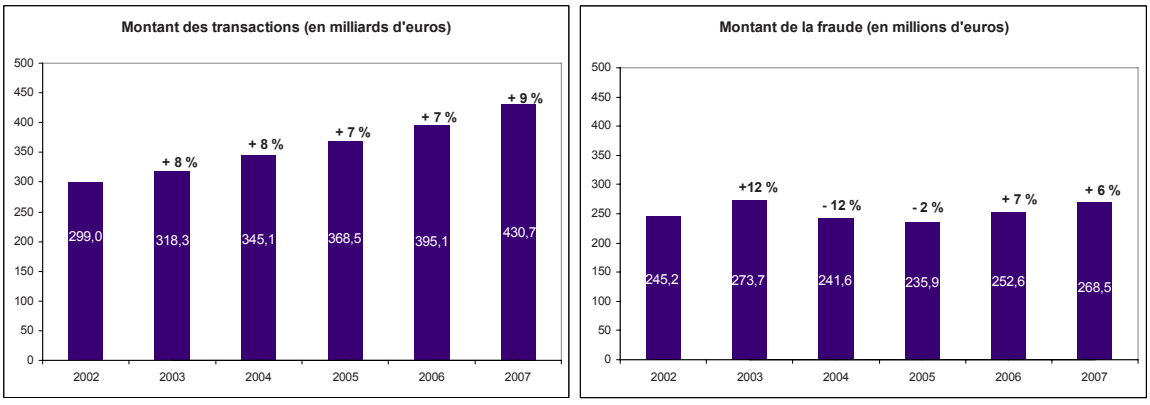
2|1 Vue d'ensemble

Le taux de fraude enregistré en 2007 dans les systèmes français est de 0,062 %. Il reste stable voire légèrement inférieur à celui des années précédentes (0,064 % en 2006 et en 2005 - voir Tableau 1). Cette stabilité s'explique, malgré des montants de fraude en hausse de 6,3 % (268,5 millions d'euros en 2007 contre 252,6 millions d'euros en 2006), par la croissance soutenue du montant des transactions (430,7 milliards d'euros en 2007 contre 395,1 milliards d'euros en 2006, soit + 9,0 % – voir Tableau 2). Le montant moyen d'une transaction frauduleuse est également en augmentation, à 130 euros contre 117 euros en 2006.



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 1 – **Evolution du taux de fraude pour tous types de cartes**



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 2 – **Evolution des montants de transactions et de fraude**

On observe également une stabilité 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 2007 à 0,049 %, à un niveau légèrement inférieur à celui de 2006 (0,050 %), pour un montant de fraude de 199,8 millions d'euros en 2007, contre 186,1 millions d'euros en 2006.

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 légère diminution. Il s'établit en 2007 à 0,044 % (pour un montant de fraude de 183,2 millions d'euros), contre 0,047 % en 2006 (pour un montant de fraude de 176,2 millions d'euros).

L'annexe C 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)

	2003	2004	2005	2006	2007
Cartes de type « interbancaire »	0,086 % (259,2)	0,069 % (224,1)	0,064 % (218,8)	0,065 % (237,0)	**0,063 %** (253,6)
Cartes de type « privatif »	0,082 % (14,4)	0,082 % (17,5)	0,067 % (17,1)	0,052 % (15,6)	**0,052 %** (15,0)
Total	0,086 % (273,6)	0,070 % (241,6)	0,064 % (235,9)	0,064 % (252,6)	**0,062 %** (268,5)

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 3 – **Répartition de la fraude par type de carte**

Pour les cartes de type « interbancaire », le taux de fraude est en légère baisse en 2007, et s'établit à 0,063 % (pour un montant de fraude de 253,6 millions d'euros), contre 0,065 % en 2006 (pour un montant de fraude de 237,0 millions d'euros). Pour ce type de carte, les taux de fraude émetteur et acquéreur sont respectivement de 0,049 % et de 0,044 % (contre 0,050 % et 0,047 % en 2006). La valeur moyenne d'une transaction frauduleuse est de 125 euros, contre 112 euros en 2006.

Pour les cartes de type « privatif », le taux de fraude reste stable à 0,052 % (pour un montant de fraude de 15,0 millions d'euros, contre 15,6 millions d'euros en 2006). Pour ce type de cartes, les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,044 % et à 0,046 % (contre 0,045 % et 0,046 % en 2006). La valeur moyenne d'une transaction frauduleuse s'élève à 432 euros en 2007, contre 430 euros en 2006.

2|3 Répartition de la fraude par zone géographique

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

	2003	2004	2005	2006	2007
Transactions nationales	**0,031 %** **(88,3)**	**0,033 %** **(103,9)**	**0,029 %** **(97,8)**	**0,031 %** **(109,6)**	**0,029 %** **(114,5)**
Transactions internationales	**0,648 %** **(185,3)**	**0,417 %** **(137,7)**	**0,408 %** **(138,1)**	**0,362 %** **(143,0)**	**0,368 %** **(154,0)**
Dont émetteur français et acquéreur étranger	0,690 % (79,3)	0,463 % (55,2)	0,458 % (64,1)	0,453 % (76,4)	0,476 % (85,3)
Dont émetteur étranger et acquéreur français	0,620 % (106)	0,391 % (82,5)	0,373 % (74,1)	0,295 % (66,5)	0,288 % (68,7)
Total	**0,086 %** **(273,7)**	**0,070 %** **(241,6)**	**0,064 %** **(235,9)**	**0,064 %** **(252,6)**	**0,062 %** **(268,5)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 4 – **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 : 57 % de la fraude portent sur les transactions internationales, alors que ce type de transaction compte pour environ 10 % de la valeur des paiements par carte enregistrés dans les systèmes français.

Dans un contexte de croissance soutenue du montant des transactions nationales (+ 9,4 %), le taux de fraude de celles-ci diminue légèrement en passant à 0,029 % en 2007 (contre 0,031 % en 2006) et demeure à un niveau très faible.

La fraude sur les transactions internationales augmente pour sa part en 2007, à la fois en taux et en montant. Le taux de fraude liée aux transactions des porteurs français à l'étranger augmente et s'établit à 0,476 % (pour un montant de fraude de 85,3 millions d'euros), contre 0,453 % en 2006 (pour un montant de fraude de 76,4 millions d'euros). Le taux de fraude liée aux transactions des porteurs étrangers en France est en légère baisse et s'établit à 0,288 % (pour un montant de fraude de 68,7 millions d'euros), contre 0,295 % en 2006 (pour un montant de fraude de 66,5 millions d'euros). Cette évolution favorable est probablement à rapprocher de la dynamique de migration des systèmes d'acceptation français à EMV qui permet de traiter de manière plus sécurisée les transactions effectuées par cartes étrangères.

Encadré 3 – Répartition du préjudice de la fraude

Poursuivant ses travaux entamés ces dernières années, l'Observatoire a pu en 2007 estimer, 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. Il est important de noter que ces indicateurs ne valent que pour le préjudice lui-même, et non pour les coûts totaux de traitement ou d'assurance engendrés par la fraude. Ces indicateurs donnent une tendance mais restent théoriques et ne peuvent refléter que la répartition directe de la fraude supportée par les acteurs. Par construction en effet, ils se réfèrent aux dispositions légales et réglementaires encadrant l'opposition par le porteur en cas de perte ou de vol, ainsi que la contestation par celui-ci en cas d'utilisation frauduleuse de sa carte. De plus, ils ne peuvent tenir compte totalement des pratiques commerciales des émetteurs ou acquéreurs.

Tous systèmes confondus, la répartition du préjudice pour les transactions nationales en 2007 est la suivante : 3 % sont supportés par les porteurs, 51 % sont supportés par les établissements émetteurs et acquéreurs et 46 % sont supportés par les commerçants, principalement en vente à distance.

De plus, sur les 268,5 millions d'euros de fraude enregistrés par les systèmes français en 2007, on estime que 78 millions d'euros (soit 29 %) sont supportés par les systèmes étrangers. Ceci s'explique notamment par la dynamique de migration des systèmes français à EMV qui permet depuis plusieurs années, dans le cadre des règles internationales de partage de responsabilité, de transférer une part importante de la fraude vers les systèmes étrangers n'ayant pas encore totalement migré vers EMV.

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 transfrontalières.

	Taux de fraude (Montant de la fraude, en millions d'euros)			
Transactions nationales	**2004**	**2005**	**2006**	**2007**
Paiements	**0,036 % (81,2)**	**0,033 % (82,8)**	**0,035 % (92,3)**	**0,032 % (95,6)**
- dont paiements de proximité et sur automate	0,029 % (63,5)	0,025 % (59,2)	0,024 % (59,1)	0,017 % (45,4)
- dont paiements à distance	0,177 % (17,7)	0,196 % (23,6)	0,199 % (33,2)	0,236 % (50,1)
- dont par courrier / téléphone	nd	nd	0,194 % (19,8)	0,201 % (23,8)
- dont sur Internet	nd	nd	0,208 % (13,4)	0,281 % (26,4)
Retraits	**0,027 % (22,7)**	**0,017 % (15,0)**	**0,019 % (17,4)**	**0,020 % (19,0)**
Total	**0,033 % (103,9)**	**0,029 % (97,8)**	**0,031 % (109,6)**	**0,029 % (114,5)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 5 – **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 diminue nettement, à 0,017 % (pour un montant de fraude de 45,4 millions d'euros), contre 0,024 % en 2006 (59,1 millions d'euros). Ceci s'explique par le renforcement des mécanismes cryptographiques mis en œuvre. Les paiements de proximité et sur automate comptent pour 70 % des transactions par carte nationales, et pour 40 % du montant de la fraude.

– le taux de fraude sur les paiements à distance est en hausse en 2007 et s'établit à 0,236 % (pour un montant de fraude de 50,1 millions d'euros), contre 0,199 % en 2006 (pour un montant de fraude de 33,2 millions d'euros). Les paiements à distance, qui représentent 5 % de la valeur des paiements par carte nationaux, comptent ainsi désormais pour 44 % du montant de la fraude. Cette hausse de la fraude s'inscrit elle-même dans un contexte de croissance très dynamique du volume et de la valeur des paiements à distance (+ 27,9 % entre 2006 et 2007). En outre, les chiffres pour 2007 montrent un creusement de l'écart du taux de fraude des paiements par courrier et téléphone, et de celui des paiements sur Internet, ce dernier augmentant plus significativement.

  Les analyses statistiques menées par la Fédération du e-commerce et de la vente à distance (Fevad) corroborent les données collectées par le Groupement des Cartes Bancaires « CB », tout en faisant apparaître que ces dernières intègrent probablement environ 20 % de contestations qui s'avèrent finalement régularisées par les porteurs. Les analyses comparées du Groupement des Cartes Bancaires « CB » et de la Fevad sur l'échantillon de cette dernière montrent une stabilité du taux de fraude sur les transactions nationales à distance pour les cartes de type « interbancaire », à 0,12 % (0,13 % en 2006). Cet écart significatif avec le taux de fraude global des paiements à distance relevé par l'Observatoire (0,236 %) suggère, comme l'an dernier, que le taux de fraude est moins élevé chez les spécialistes du commerce électronique. Le taux de fraude varie en effet selon les secteurs d'activité, et même d'un commerçant à l'autre, selon les mécanismes de sécurité mis en œuvre.

  L'année dernière, l'Observatoire avait insisté sur l'importance du respect des mesures de sécurité recommandées par les émetteurs, en particulier l'utilisation systématique du CVx2 en paiement à distance et la vérification de l'identité des acheteurs par les commerçants[13]. Dans ce contexte d'augmentation de la fraude sur les paiements à distance, l'Observatoire souhaite renouveler cette recommandation. De plus, l'Observatoire recommande à tous les acteurs concernés de mettre en œuvre des solutions de sécurité interopérables[14] permettant de renforcer l'authentification du porteur de la carte ;

– la fraude sur les retraits reste bien contenue en taux, à seulement 0,020 % (pour un montant de fraude de 19,0 millions d'euros), contre 0,019 % en 2006 (pour un montant de fraude de 17,4 millions d'euros). Les retraits représentent quelque 24 % des transactions nationales et comptent pour 17 % du montant de la fraude.

[13] Pour une vue d'ensemble des politiques de sécurité mises en œuvre dans ce domaine, on pourra se reporter au chapitre premier du rapport annuel 2004 de l'Observatoire.

[14] permettant aux porteurs d'utiliser une même solution auprès de différents commerçants quelles que soient leurs banques.

	Taux de fraude (Montant de la fraude en millions d'euros)	
Émetteur français – Acquéreur étranger	**2006**	**2007**
Paiements	**0,421 % (54,0)**	**0,483 % (65,2)**
- dont paiements de proximité et sur automate	0,288 % (28,1)	0,299 % (30,0)
- dont paiements à distance	0,840 % (26,0)	1,024 % (35,1)
- dont par courrier / téléphone	0,684 % (5,7)	0,790 % (7,6)
- dont sur Internet	0,898 % (20,3)	1,117 % (27,4)
Retraits	**0,555 % (22,4)**	**0,455 % (20,0)**
Total	**0,453 % (76,4)**	**0,476 % (85,3)**
Émetteur étranger – Acquéreur français	**2006**	**2007**
Paiements	**0,344 % (61,5)**	**0,334 % (62,8)**
Retraits	**0,107 % (5,0)**	**0,117 % (5,9)**
Total	**0,295 % (66,5)**	**0,288 % (68,7)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 6 – **Répartition de la fraude internationale par type de transaction**

En ce qui concerne les transactions internationales, l'Observatoire ne dispose d'une décomposition fine de la fraude par type de transactions que pour les seules transactions réalisées par des cartes françaises à l'étranger. Il constate, comme pour les transactions nationales, que :

- le taux de fraude sur les paiements de proximité et sur automate est nettement inférieur à celui sur les paiements à distance (0,299 % contre 1,024 %) ;
- le taux de fraude sur les paiements à distance est plus élevé pour les paiements sur Internet que pour les autres types de transaction à distance (1,117 % contre 0,790 %).

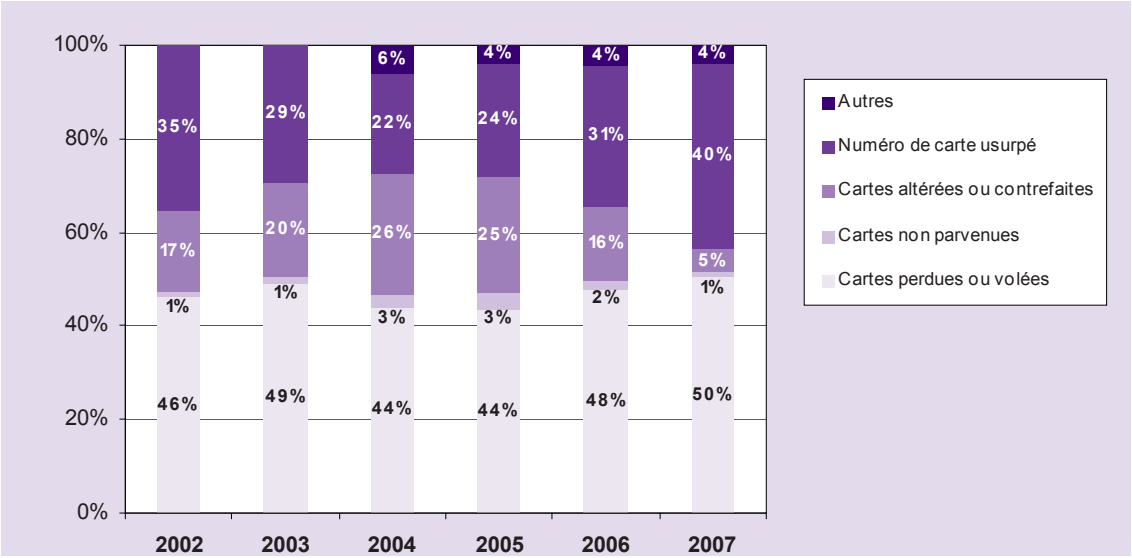
2|5 Répartition de la fraude selon son origine

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 « autre », 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 en 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 7 – **Répartition de la fraude selon son origine (transactions nationales, en valeur)**

En augmentation en 2007, l'origine de fraude la plus importante reste celle liée aux pertes et vols de cartes, qui représente plus de 50 % des paiements nationaux frauduleux. La contrefaçon de cartes n'est plus à l'origine que de 5 % des paiements nationaux frauduleux, contre 16 % en 2006 et 25 % en 2005. En revanche, la fraude par usurpation de numéro de carte, utilisée pour les paiements à distance, progresse encore en 2007 (comme en 2006 et 2005) et est désormais à l'origine de près de 40 % des paiements 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 (environ 50 %).

2007	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	57,7	50,4 %	55,2	52,3 %	2,5	28,3 %
Carte non parvenue	1,3	1,1 %	0,4	0,4 %	0,8	9,4 %
Carte altérée ou contrefaite	5,6	4,9 %	5,2	4,9 %	0,7	4,6 %
Numéro usurpé	45,5	39,7 %	44,8	42,4 %	0,7	7,9 %
Autres	4,5	3,9 %	-	-	4,5	49,7 %
Total	**114,5**	**100 %**	**105,6**	**100 %**	**9,0**	**100 %**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 8 – **Répartition de la fraude nationale selon son origine et par type de carte**

Encadré 4 – Indicateurs des forces de police et de gendarmerie

Pour l'année 2007, les forces de police et de gendarmerie enregistrent une légère baisse des cas recensés en matière de fraude relative aux cartes de paiement. 53 458 faits de falsification et usage de cartes de paiement ont été constatés, et 3 256 individus ont été mis en cause, motivant 1 349 mesures de garde en vue.

Les attaques de distributeurs automatiques de billets (DAB) diminuent également avec 391 piratages de DAB en 2007 (contre 515 en 2006, 200 en 2005, et 80 en 2004). A celles-ci s'ajoutent 36 attaques de distributeurs automatiques de carburant (DAC).

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

– l'interpellation de deux responsables d'un réseau international permettant la saisie de plus d'un millier de cartes de paiement contrefaites et d'un butin dépassant cent mille euros ;

– le démantèlement d'ateliers clandestins de fabrication de fausses cartes de paiement, avec saisie du matériel (ordinateurs, embosseuses, imprimantes thermiques, etc.) et des butins dont le montant s'élève à plusieurs dizaines de milliers d'euros.

Les autorités françaises ont continué en 2007 à coopérer étroitement avec leurs homologues européens, notamment des pays de l'Est. Cette démarche a conduit à des actions concrètes du point de vue opérationnel, et s'avère nécessaire pour lutter efficacement contre la fraude devant l'essor des groupes organisés et de la criminalité transfrontalière. Ainsi, les deux premiers mandats d'arrêt européens ont été mis en œuvre en Roumanie pour le compte des autorités françaises.

3 VEILLE TECHNOLOGIQUE

3.1 Sécurité des paiements par carte et standardisation européenne

Dans son rapport 2005[15], l'Observatoire saluait les avancées dans le domaine de l'harmonisation européenne apportées par l'adoption, par le Conseil européen des paiements (European Payments Council – EPC), du « cadre régissant les cartes SEPA » (SEPA Cards Framework – SCF). Il avait souligné l'importance, pour la promotion d'un niveau élevé de sécurité pour les cartes en Europe, que soient définies des normes techniques pour l'ensemble des domaines d'interaction entre les parties à une transaction par carte. Il avait également exprimé le souhait que soit mise en œuvre une certification sécuritaire des cartes et des terminaux, sur la base d'une méthodologie commune aux différents systèmes de carte européens, afin de garantir un même niveau de sécurité de ces matériels.

L'Observatoire a suivi, en 2006 et en 2007, l'avancement des travaux dans ces différents domaines. Plusieurs initiatives ont été lancées pour parvenir à une « standardisation », c'est-à-dire à une convergence des règles de fonctionnement et de communication, ainsi que des caractéristiques techniques des matériels utilisés pour le paiement par carte en Europe.

Les développements qui suivent permettent de comprendre l'importance de la standardisation des transactions par carte dans l'environnement européen, et font un état de l'avancement des travaux en matière de standardisation et de certification sécuritaire à fin 2007.

Importance de la standardisation dans le cadre d'un paiement par carte

Le paiement par carte implique 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 sur leurs matériels informatiques : identifiants du commerçant, du porteur et de la carte, ordre de paiement. Ces échanges requièrent une standardisation des matériels et des protocoles de communication au sein du système de paiement par carte, notamment au niveau de la carte, du terminal et des serveurs de l'acquéreur et de l'émetteur.

Cette standardisation peut atteindre un niveau de détail variable, selon le degré d'interopérabilité recherché. Pour réaliser les transactions informatiques entre les différentes composantes matérielles d'un système de paiement par carte, et permettre qu'elles puissent être exécutées sur des équipements divers, il est nécessaire de spécifier des règles communes pour leur fonctionnement et leur interconnexion.

Dans le cas de la coexistence, sur un même marché, d'un système de carte de type « interbancaire » et de plusieurs systèmes de carte de type « privatif », il est possible, ce qui est le cas en France, qu'une standardisation minimale soit convenue entre ces différents systèmes

[15] Cf. Rapport annuel 2005 de l'Observatoire, Chapitre 4 p. 41

pour permettre de faire fonctionner les cartes de type « privatif » sur les matériels d'acceptation du système de type « interbancaire ».

Encadré 5 : La standardisation

Une norme est définie comme « un document de référence qui apporte des réponses à des questions techniques et commerciales que se posent de façon répétée les acteurs, sur des produits, des biens d'équipement ou des services. Elle est élaborée en consensus par l'ensemble des acteurs d'un marché (producteurs, utilisateurs, laboratoires, pouvoirs publics, consommateurs…). Une norme est d'application volontaire et contractuelle. Dans certains cas, notamment les domaines liés à la sécurité et les conditions liées aux marchés publics, elle peut être rendue obligatoire. » (source : AFNOR). La normalisation peut porter sur des domaines techniques, mais aussi sur l'organisation ou les services. Les normes peuvent être définies au niveau national, européen ou international.

Il est d'usage de différencier les « normes », élaborées par des « organismes de normalisation » reconnus (comme l'ISO[16] au niveau international ou l'AFNOR[17] en France), et selon une méthodologie reposant sur la recherche du consensus, des « standards », qui peuvent proposer des solutions de même type, sans pour autant avoir été élaborés dans le même cadre formel. On parlera ainsi de standards pour des documents de référence élaborés par un ou plusieurs acteurs de marché et dont l'utilisation s'est généralisée.

L'utilisation de normes et de standards a généralement pour effet de faciliter les échanges par l'harmonisation des règles et des pratiques et en fournissant des références communes. Elle permet également de rendre des produits et services comparables entre eux et compatibles les uns avec les autres.

Les normes et standards peuvent être d'un niveau de précision plus ou moins détaillé. Dans le cas du paiement par carte, on peut ainsi distinguer les trois niveaux suivants :

– les besoins des utilisateurs : ce premier niveau concerne la définition des exigences fondamentales auxquelles doit répondre le système de paiement par carte. Il s'agit par exemple du besoin d'interopérabilité avec les systèmes internationaux, de la fiabilité, de la sécurité, et de la simplicité d'usage pour les porteurs. Ce niveau de normalisation est principalement défini par la profession bancaire ;

– les spécifications fonctionnelles : ce deuxième niveau consiste à normaliser les fonctionnalités du système. Elles sont établies conjointement par la profession bancaire et par les fabricants de cartes et de terminaux. Elles définissent les protocoles d'échange et les formats des données, pour qu'ils puissent être traités par tout type de matériel, quels qu'en soient le fabricant et le prestataire informatique choisis ;

– les spécifications techniques : ce niveau est le plus détaillé. Il concerne notamment l'architecture technique du produit et les développements informatiques. Les spécifications techniques sont définies par les industriels.

De plus, la création de l'Espace unique de paiement en euros, le « SEPA », étend le besoin d'interopérabilité aux échanges entre les différents systèmes de paiement par carte existants, puisque, notamment, les cartes émises au sein d'un système doivent pouvoir être acceptées sur un autre.

Les avantages attendus 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. En effet, pour les émetteurs de cartes, cela assurera le fonctionnement de leurs cartes sur un réseau d'acceptation élargi aux autres pays européens. Les commerçants pourront choisir librement leur prestataire d'acquisition tout en gardant leur équipement. Les fabricants

16 International Organization for Standardization

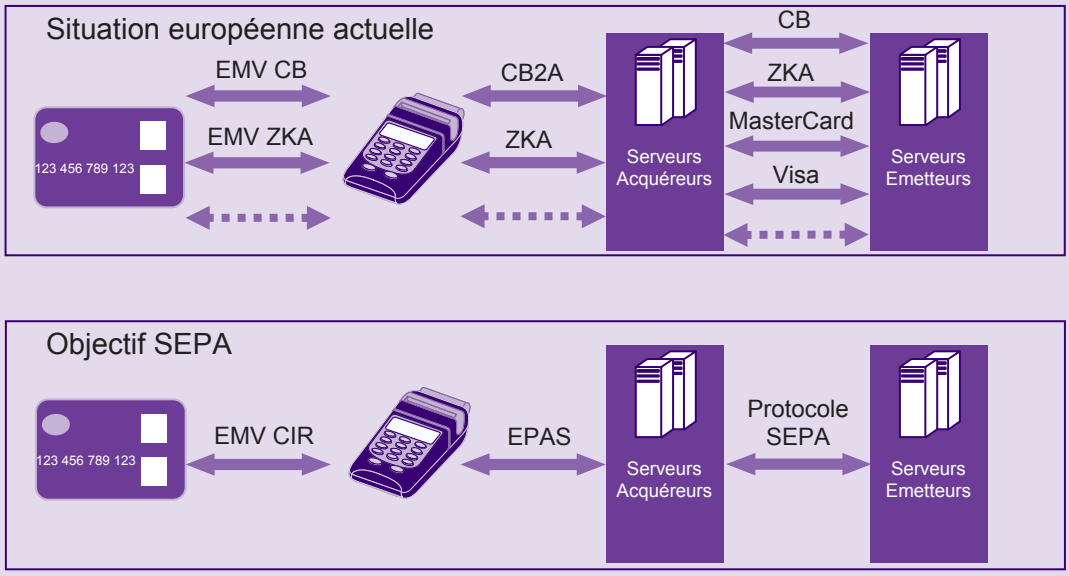
17 Association française de normalisation

de cartes et de terminaux disposeront d'une plus grande facilité pour distribuer leurs produits sur un marché étendu à l'Europe.

Encadré 6 : Evolution des standards techniques avec l'émergence de SEPA

La situation européenne actuelle est marquée par un cloisonnement des quelque trente systèmes de carte de type « interbancaire » nationaux. Les paiements par carte transfrontaliers reposent donc pour l'instant principalement sur les réseaux internationaux, tel Visa ou Mastercard. Il en résulte que chaque système de paiement par carte dispose aujourd'hui de ses propres spécifications pour les échanges informatiques 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.

Les travaux de standardisation européens doivent conduire à l'adoption de spécifications communes sur l'ensemble de ces phases du cycle de paiement par carte. Cet effort d'harmonisation devrait par exemple conduire à retenir un seul mode de mise en œuvre du standard EMV pour le dialogue entre la carte et le terminal, ce qui n'est pas le cas aujourd'hui.



Les choix de l'EPC en matière de standardisation

En complément des préconisations qui figuraient déjà dans le SCF[18], notamment pour l'emploi systématique du standard EMV, l'EPC a identifié un besoin de standardisation sur les trois domaines d'interaction (ou « interfaces ») composant l'ensemble du cycle de paiement par carte :

– entre la **carte et le terminal** ;

– entre le **terminal de paiement et le serveur de l'acquéreur** ;

– entre les **serveurs** des **acquéreurs** de transactions et ceux des **émetteurs** de cartes.

L'EPC s'appuie en réalité pour l'essentiel sur des initiatives conduites indépendamment de lui par différents groupes de travail constitués par des banques, des systèmes de carte ou des industriels. Ces travaux visent en priorité les transactions de paiement de proximité. L'EPC a conclu des accords avec ces groupes de travail en vue d'envisager le moment venu la généralisation de leurs spécifications sous forme de standards.

[18] Cf. version 2 – mars 2006

L'EPC conditionne l'adoption de ces spécifications au respect de trois exigences :

– que ces spécifications répondent aux besoins exprimés par l'EPC et soient libres de droits[19] ;

– qu'elles soient compatibles avec les standards déjà existants au niveau mondial ;

– qu'il soit possible de maintenir et de développer les standards.

La standardisation de l'interface carte - terminal

Pour répondre à l'un des objectifs majeurs d'interopérabilité de SEPA, qui est que toute carte émise dans tout pays de l'espace SEPA puisse être techniquement acceptée sur l'ensemble des terminaux de cette zone, il est nécessaire de standardiser l'interface entre la carte et le terminal. De plus, cette préoccupation se double d'un besoin de compatibilité avec les standards internationaux existants, pour permettre l'acceptation des cartes des réseaux européens en dehors de l'espace SEPA.

Dès 2005, l'EPC a retenu pour cette interface les spécifications techniques EMV, produites par le consortium EMVCo, (« Europay, Mastercard, Visa » - EMV, dont est également membre le réseau japonais JCB). Ce choix assure ainsi que les cartes émises par les systèmes de carte interbancaire européens seront des cartes à puce avec code confidentiel, situation équivalente en matière de sécurité à ce qui existe en France depuis 1992, ce dont l'Observatoire a déjà eu l'occasion de se féliciter.

En complément du choix d'EMV, l'EPC a affiché son intérêt pour prolonger les travaux de standardisation par des spécifications portant à la fois sur les cartes et sur les terminaux, en s'appuyant sur les propositions d'initiatives extérieures.

Pour les cartes :

– Définition de choix communs d'implémentation d'EMV : la norme EMV autorise plusieurs niveaux d'implémentation. Les modalités de mise en œuvre varient actuellement d'un système de carte à un autre, ce qui peut affecter l'interopérabilité de ces systèmes. C'est la raison pour laquelle il est nécessaire de compléter la standardisation en ce domaine en réalisant un choix dans les différentes options offertes, c'est-à-dire en définissant les règles propres à l'application de paiement installée sur le terminal (contrôle ou non du code, etc.) et au réseau de l'émetteur (plafond d'autorisation, etc.). Tel est l'objet des travaux du groupe CIR–TWG[20] (« Common Implementation Recommendations »), qui a défini des spécifications communes pour le paiement en mode EMV (CPA - « Common Payment Application »). Les caractéristiques de sécurité des cartes françaises « CB » (authentification dynamique, contrôle du code confidentiel) sont compatibles avec ce projet de standard.

Pour les terminaux :

– Harmonisation du déroulement de la transaction sur le terminal : l'EPC préconise d'élaborer un modèle unique de déroulement de transaction, commun à tous les terminaux SEPA, pour garantir que les fonctions de paiement sont toutes prises en compte de manière homogène. Cela réduit également les incidents techniques et les coûts de développement et de certification.

---

19 tout au moins que les conditions d'accès et d'usage, tant financières que contractuelles, ne constituent pas un obstacle ou une quelconque barrière pour les développeurs et utilisateurs.

20 CIR-TWG est un groupe de travail constitué par le groupement des utilisateurs européens d'EMV.

Le groupe CIR a rédigé une première version de la spécification fonctionnelle décrivant la cinématique de transaction (FAST). Si cette standardisation, en cours de rédaction, était adoptée par l'EPC, cela permettrait ainsi d'effectuer les contrôles sécuritaires réalisés actuellement avec les cartes françaises (authentification dynamique, contrôle du code, gestion de plafonds, etc.).

– Harmonisation de l'affichage des informations au porteur : le standard EMV ne définissant pas l'interface entre le porteur et le terminal, le groupe CIR a inclus dans son projet de spécification FAST des règles d'affichage communes (détection du pays d'origine de la carte…) et des messages uniformisés. Une éventuelle standardisation de l'affichage n'a pas de vocation directe à l'amélioration de la sécurité, même si elle contribue à l'aisance et à la vigilance du porteur.

– Spécification des composants matériels et logiciels d'un terminal ou d'un automate de paiement : le groupe ERIDANE[21] élabore actuellement des spécifications relatives aux différents composants des matériels d'acceptation (claviers, écrans, lecteurs, logiciels…). Ce standard permettra de disposer de composants homogènes, indépendamment de la marque du terminal. La production de ces matériels devrait donc être facilitée. Cette spécification a peu d'impact sur la sécurité du terminal, même si certaines extensions envisagées par ERIDANE pourraient prévoir des dispositifs sécurisés pour la connexion des terminaux et automates à des réseaux ouverts. L'EPC ne s'est pas encore prononcé sur son application.

Par ailleurs, l'EPC est également susceptible de retenir les principes édictés par les organismes de standardisation créés à l'initiative des réseaux internationaux. Ceux-ci élaborent en effet également une normalisation de certains équipements, afin de mieux garantir la sécurité des paiements par carte. L'organisme PCI SSC (« Payment Card Industry - Security Standards Council »), fondé par American Express, Discover Financial Services, JCB International, Mastercard Worldwide et Visa Inc, définit des standards de sécurité pour l'industrie de la carte. L'EPC siège désormais à titre consultatif auprès des organismes EMVCo et PCI SSC. Les principales recommandations de PCI SSC concernent la protection des données de cartes et du code confidentiel dans les terminaux, les automates ou les bases de données des commerçants. Compte tenu de l'origine américaine de la plupart des réseaux fondateurs de PCI SSC qui utilisent le mode piste, certaines de ces recommandations ciblent ce type de transaction. Les mesures de sécurité demandées aux commerçants sont par définition moins adaptées à des marchés pour lesquels les paiements par carte sont fondés sur l'utilisation de la puce et du code confidentiel, comme c'est le cas en France, puisque les diligences à prendre ne correspondent pas à tous les types de fraude visant les cartes à puce[22]. Si ces normes n'étaient pas adaptées aux spécificités du marché européen, l'impact de leur adoption serait élevé pour les commerçants et les émetteurs français, qui ont depuis quinze ans organisé leur sécurité en fonction de l'utilisation de cartes à puce[23].

La standardisation de l'interface terminal - acquéreur

L'objectif de SEPA de permettre aux commerçants de choisir librement au meilleur coût la prestation d'un acquéreur appelle également à un renforcement de la standardisation dans le domaine terminal – acquéreur (autorisation, acquisition, gestion du terminal, etc.).

21 ERIDANE rassemble des systèmes de paiement par carte européens, des fabricants de terminaux et des commerçants.

22 Cf. Rapport annuel 2005 de l'Observatoire § 3.2 p. 31

23 Cf. Rapport annuel 2006 de l'Observatoire p. 37

Il existe actuellement de nombreux protocoles pour la connexion (autorisation et remise) des terminaux aux serveurs des acquéreurs, qui, bien que fondés sur la norme internationale ISO 8583[24], ne sont pas compatibles entre eux.

Les systèmes de carte français utilisent par exemple le protocole « CB2A » élaboré par le Groupement des Cartes Bancaires. L'EPC envisage l'élaboration d'un protocole unifié qui permettrait d'utiliser le même terminal pour l'acceptation de cartes émises par des systèmes différents. Il ne se prononce toutefois ni sur l'obligation de prescrire une telle spécification, ni sur le niveau de description technique nécessaire. Le consortium EPAS (« Electronic Protocol Application Software »)[25] vise à définir un protocole de communication unique. Les orientations techniques majeures dans ce domaine n'ont pas encore été retenues. Ce protocole pourrait être fondé soit sur la norme internationale actuelle (ISO 8583), soit sur une nouvelle norme (ISO 20022[26]), dont la mise en œuvre est déjà prévue pour d'autres maillons de la chaîne de transaction par carte (acquéreur / émetteur) et pour d'autres moyens de paiement (virements et prélèvements SEPA). Il ne visera pas la protection des données échangées sur des réseaux ouverts, qui ne peut être assurée que par des mesures de sécurité spécifiques (ex : infrastructures de gestion de clés cryptographiques).

La standardisation pour les échanges entre acquéreurs et émetteurs

Les établissements acquéreurs doivent pouvoir joindre les établissements émetteurs, d'abord pour effectuer les demandes d'autorisation des transactions, puis pour initier les opérations de compensation et de règlement. Les infrastructures techniques permettant de transporter des autorisations et des fichiers de transactions entre les acquéreurs et les émetteurs sont souvent étroitement liées au système de carte. Dans le cas de transactions impliquant des acteurs extérieurs au système, celui-ci peut transmettre des transactions vers les réseaux concernés (cas des porteurs étrangers en France) ou, à l'inverse, réacheminer les transactions des porteurs français effectuées chez des commerçants à l'étranger. Dans leur très grande majorité, ces systèmes de carte nationaux et internationaux ont spécifié leur propre protocole de communication sur la base de la norme ISO 8583. Toutefois, des différences d'implémentation de ces protocoles par ces infrastructures requièrent que celles-ci mettent en œuvre des passerelles de conversion pour réaliser leurs échanges.

Pour favoriser la concurrence, l'EPC a fixé comme principe que les infrastructures d'acquisition devront dorénavant être séparées du système de paiement par carte proprement dit. De la sorte, un acquéreur ou un émetteur doit pouvoir choisir librement ses infrastructures d'autorisation et de compensation, sans être obligé de choisir ceux proposés par les systèmes de carte nationaux et internationaux auxquels il adhère[27].

La standardisation des échanges serait une contribution importante pour l'atteinte de cet objectif, mais l'EPC considère qu'il n'est pas obligatoire de créer un nouveau standard à court terme. En effet, il indique pouvoir continuer à s'appuyer sur les standards existants (Visa, Mastercard, etc., fondés sur la norme ISO 8583) qui sont en tout état de cause nécessaires pour traiter les transactions internationales.

Pour faire évoluer cette situation à plus long terme, l'EPC a toutefois entamé en avril 2007 certains travaux préparatoires, portant sur la définition de son expression de besoins et

24 Spécifications d'échange de messages de transactions financières initiées par carte.

25 EPAS regroupe des systèmes de carte, des commerçants et des industriels.

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

27 C'est le concept « d'unbundling » du SCF.

sur l'identification et la description des données à transporter (en se référant au format de celles-ci défini par les normes EMV et UNIFI). Il réalise aussi un inventaire des différents protocoles utilisés, l'évaluation de leurs différences et de la possibilité d'en réduire le nombre. Il est donc pour l'instant difficile de juger des effets que pourrait avoir un futur standard sur la sécurité de ces échanges. Il faut toutefois noter que l'utilisation d'un tel standard permettrait de limiter les difficultés de conversion liées aux différences d'implémentation de la norme ISO 8583.

Par ailleurs, le projet d'alliance de certains systèmes nationaux, appelé « EAPS – European Alliance of Payment Schemes », prévoit également de développer un nouveau standard d'échange entre acquéreurs et émetteurs, en s'appuyant sur la norme ISO 8583.

La certification

La certification de la conformité des cartes et des terminaux, à la fois aux besoins fonctionnels et aux exigences de sécurité définis par les systèmes de paiement par carte, dépend pour l'instant de procédures nationales, voire des systèmes eux-mêmes[28]. Il en résulte que les niveaux d'exigences de sécurité peuvent varier selon les différents systèmes de paiement par carte, et que les industriels qui doivent faire certifier leurs produits sont soumis à des démarches répétitives et coûteuses.

Pour faciliter la convergence en la matière, le SCF édicte un certain nombre de principes :

– les systèmes de paiement par carte ne devront plus exercer eux-mêmes cette activité de certification, tant fonctionnelle que sécuritaire, mais devront recourir à des organismes indépendants. Une telle mesure est de nature à faciliter une certification unique pour les matériels, en vue de leur utilisation ensuite par différents systèmes de paiement par carte ;

– l'utilisation de méthodes d'évaluation sécuritaire offrant la possibilité d'une reconnaissance mutuelle entre pays et systèmes de paiement par carte (du type « Critères communs »)[29] est souhaitée.

Toutefois, le SCF ne prescrit rien pour unifier les exigences de sécurité ni pour harmoniser les procédures de certification et permettre ainsi une reconnaissance mutuelle de celles-ci par chaque système de carte. L'harmonisation de ces exigences de sécurité et procédures de certification sécuritaire est pourtant un enjeu majeur pour garantir que le SEPA n'aboutisse pas à un abaissement du niveau de sécurité des cartes et des terminaux. L'Observatoire a déjà exprimé ses attentes sur ce point dans son rapport 2005.

L'EPC étudie les travaux du groupe CAS (« Common Approval Scheme »)[30], qui définit :

– des exigences de sécurité du terminal ou de l'automate de paiement : celles-ci couvrent l'ensemble des composants de ces matériels, c'est-à-dire non seulement le clavier (PED – « PIN Entry Device ») sur lequel est saisi le code confidentiel, mais aussi le lecteur de piste et les composants logiciels gérant les données de la carte. Pour le clavier, l'EPC semble privilégier les spécifications PCI PED V2.0, élaborées par PCI SSC, dont le niveau apparaît équivalent à celles préparées par CAS. Toutefois, les exigences prévues par PCI PED couvrent également le lecteur de piste et pourraient s'avérer coûteuses pour les systèmes de carte européens qui n'utilisent pas la piste ;

---

28 Cf. Rapport annuel 2005 de l'Observatoire – encadré 6, p. 30

29 Cf. Rapport annuel 2005 de l'Observatoire – encadré 12, p. 45

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

– une méthodologie commune d'évaluation : CAS recommande l'adoption de la méthodologie des « Critères communs », utilisée aujourd'hui en France et en Allemagne pour les cartes et au Royaume Uni pour les terminaux. Cette préconisation permettrait de maintenir la qualité des procédures d'évaluation effectuées aujourd'hui dans ces pays et servirait de fondement à un système européen de reconnaissance mutuelle ;

– un schéma européen de certification fonctionnelle et sécuritaire de la carte et du terminal : il est en effet nécessaire de prévoir les modalités d'évaluation et de certification par des laboratoires et organismes spécialisés, ainsi qu'un dispositif assurant la reconnaissance mutuelle de ces certificats par les différents systèmes de paiement par carte opérant en Europe. L'Observatoire avait déjà souligné l'intérêt d'une telle démarche et soutenu une proposition d'amendement au projet de directive sur les services de paiement. Cet amendement n'ayant pas été retenu, il souscrit aux initiatives proposées par CAS et souhaite leur prise en compte par l'EPC.

Disponibilité des standards et déploiement des produits

L'EPC prévoit de rendre disponibles les différents standards pour fin 2008. Compte tenu des changements à opérer par l'ensemble des acteurs, il est difficile aujourd'hui de prévoir une échéance pour cette standardisation. La date de disponibilité des standards conditionne le début des travaux de développement, qui peuvent durer plusieurs mois (de 6 à 18 mois). Des tests d'interopérabilité devront ensuite être réalisés et dureront également plusieurs mois. Il n'y aura donc pas de produit entièrement conforme aux standards SEPA dans les délais prévus pour la mise en place du SCF (2008/2010).

Pour les terminaux de paiement, le rythme de déploiement des matériels conformes aux standards SEPA devra tenir compte du rythme de renouvellement, souvent assuré par les commerçants, des matériels déjà installés. Par exemple, en France, ces matériels, qui sont diffusés en très grand nombre (plus d'un million de terminaux), ont pour la plupart été remplacés récemment (à partir de 2002), avec une durée d'amortissement généralement supérieure à 7 ans. Dans l'attente de la migration du parc de terminaux à ce nouveau standard SEPA, les serveurs acquéreurs actuels pourront toutefois convertir les différents protocoles hérités des systèmes existants pour les transmettre dans les systèmes d'échange au format souhaité.

Les cartes françaises « CB » sont déjà au standard EMV. Les faire évoluer pour prendre en compte les préconisations préparées par le groupe CIR requerrait au minimum un délai de deux à trois ans, compte tenu de leur durée de validité qui conditionne leur renouvellement.

Malgré le retard pris dans l'élaboration d'un standard commun pour les infrastructures d'échange, la migration pourrait être effective dans des délais raisonnables, dans la mesure où le nombre de serveurs à modifier est restreint et où des applications de transcodage pourraient y suppléer.

Encadré 7 : 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	EMVCo	oui	disponible	Parc CB 100% EMV
Recommandations détaillées d'implémentation EMV	CIR	-	Fin 2008	
Domaine Terminal - Acquéreur				
Exigences fonctionnelles et sécuritaires	EPAS	oui	Fin 2008	A partir de 2009
Exigences de sécurité pour le terminal	CAS	oui	Fin 2008	A partir de 2009
Spécifications techniques détaillées	EPAS	-	Fin 2008	A partir de 2009
Architecture fonctionnelle des terminaux	ERIDANE	-	Fin 2008	A partir de 2009
Spécifications d'interfaces internes des terminaux	ERIDANE	-	Fin 2008	A partir de 2010
Domaine Acquéreur - Emetteur				
Exigences fonctionnelles	EPC A2IEG	oui	Fin 2008	A partir de 2009
Spécifications techniques détaillées	EPC A2IEG	-		
Domaine Certification				
Exigences sécuritaires communes	CAS	oui	Fin 2008	A partir de 2009
Méthodologie commune de certification sécuritaire	CAS	-	Fin 2008	A partir de 2009
Méthodologie commune de certification fonctionnelle	CAS	-	2008/2010	A partir de 2010

Conclusion

Permettre l'interopérabilité entre les différents systèmes de paiement en Europe constitue l'enjeu même du projet SEPA pour les cartes. Alors que chaque système existant aujourd'hui fonctionne déjà sur la base de matériels et de protocoles d'échange d'information standardisés, la standardisation commune aux différents systèmes reste embryonnaire et ne permet pas de fonder une réelle interopérabilité. L'ouverture européenne des systèmes de paiement par carte suppose donc une standardisation commune. Il importe que celle-ci contribue à un haut niveau de sécurité, au moins équivalent à celui pratiqué aujourd'hui en France.

Sur cette question, l'EPC examine des contributions de groupes d'experts sur la base desquelles il pourrait fonder les standards SEPA.

Les travaux de standardisation étant désormais bien identifiés, un calendrier général a pu être établi, qui indique les principales échéances pour la finalisation des standards et leur période d'implémentation.

Le dialogue avec les organismes internationaux de standardisation comme EMVCo et PCI SSC s'est également intensifié afin de permettre à l'EPC de faire connaître, à titre consultatif, les intérêts de ses membres.

Dans le prolongement des études qu'il avait déjà conduites en 2005, l'Observatoire rappelle l'importance de la prise en compte, lors de la définition des standards, d'un niveau élevé et homogène de sécurité des matériels et communications. Ces standards doivent en particulier être en adéquation avec l'analyse des risques des paiements par carte en Europe. Il soutient à ce titre les travaux destinés à promouvoir une méthodologie commune de certification de la sécurité des cartes et des terminaux, permettant de fonder une reconnaissance mutuelle, par les systèmes, des certifications délivrées par chacun d'eux. L'Observatoire considère en effet qu'il est indispensable que les acteurs européens disposent d'un schéma de certification propre à l'Europe et continuent à disposer de moyens et de compétences dans ce domaine.

Il souligne enfin le caractère stratégique de la gouvernance de ces standards pour la sécurité des paiements par carte en Europe, et considère que les systèmes européens doivent être acteurs de cette gouvernance.

3 | 2 La sécurité des nouveaux mécanismes d'initiation du paiement par carte (paiement par téléphone mobile, carte sans contact)

Le mode d'initiation du paiement par carte, c'est-à-dire la façon par laquelle est formulé l'ordre de paiement par carte, évolue, selon les avancées permises par le progrès technologique. Pour le paiement de proximité, il repose jusqu'à présent essentiellement sur la lecture d'une piste ou le dialogue entre une puce et le terminal ou l'automate de paiement. Dans les deux cas, la lecture des informations de la carte suppose le « contact » de la carte avec le terminal. La forme du support plastique de la carte, qui a été très tôt normalisée au niveau mondial, a permis d'assurer l'interopérabilité entre les terminaux et les cartes des différents émetteurs. L'apparition en France à la fin des années 1980 des cartes à puce contenant une application de paiement n'a pas entraîné de modification de la forme du support. Il fallait conserver la compatibilité avec les terminaux existants, tant pour des questions de coûts que d'interopérabilité avec la piste qui restait majoritairement utilisée. Le support ne changeant pas, le mode d'initiation du paiement a alors seulement évolué du fait du changement de mode de dialogue entre la carte et le terminal ou l'automate, celui-ci ne se faisant plus par une lecture de la piste magnétique mais par un dialogue avec la puce.

Certaines innovations technologiques apparues ces dernières années ont amené les acteurs du paiement à imaginer de nouveaux usages qui sont susceptibles de faire davantage évoluer le mode d'initiation du paiement par carte. Il devient notamment possible de faire exécuter, indépendamment de l'utilisation du support plastique habituel, les fonctions de paiement inscrites traditionnellement dans la puce électronique de la carte. En parallèle, l'émergence des technologies dites « sans contact » permet de s'affranchir d'une insertion de la carte dans un terminal. La combinaison de ces évolutions récentes conduit à voir apparaître, d'une part, des cartes sans contact[31], et, d'autre part, de nouveaux supports tels que le téléphone mobile, permettant de loger la puce comportant l'application logicielle de paiement et dialoguant également avec des terminaux en mode sans contact.

L'Observatoire, dans le prolongement de son étude de 2004 sur les cartes sans contact, s'est intéressé aux conditions de sécurité de ces deux nouveaux modes d'initiation, sur la base d'expérimentations actuellement en cours en France. Les cartes prépayées, examinées dans le cadre des travaux de suivi des politiques de sécurité des émetteurs et des accepteurs, ne sont pas couvertes par cette étude.

Caractéristiques des nouveaux modes d'initiation du paiement par carte

Deux grandes familles de nouveaux mécanismes d'initiation sont expérimentées en France :

– les solutions de cartes de paiement au format habituel (norme ISO 7816-1), équipées à la fois d'une puce exécutant l'application de paiement et d'un dispositif permettant d'établir une communication sans contact avec un terminal de paiement. Ce dispositif se compose

[31] Les premières cartes sans contact qui sont apparues, principalement sur le marché américain, transmettaient une copie des données de la piste. Les tests réalisés en France sont effectués sur des cartes à puce, ce qui explique que cette étude n'évoque que les cas de cartes à puce sans contact.

d'un microprocesseur et d'une antenne permettant d'émettre des communications selon le protocole NFC (« Near Field Communication »). Il est prévu pour fonctionner à très faible distance, obligeant ainsi la carte à être rapprochée du terminal de paiement (moins de 10 cm environ) ;

– les solutions de paiement utilisant un téléphone mobile, associant, d'une part, une application logicielle de paiement inscrite dans une puce et, d'autre part, un dispositif de communication sans contact NFC.

Dans les deux cas, le mode de communication sans contact répond à la norme ISO 14443, qui permet d'échanger des données entre une puce et un lecteur sans contact, le terminal ou l'automate de paiement, situé à quelques centimètres.

Initiation du paiement par carte sans contact

Les cartes sans contact qui commencent à être testées en France sont fondées sur des spécifications élaborées par Visa et MasterCard. Tout en étant prévues pour dialoguer en mode sans contact, ces cartes peuvent toutefois toujours dialoguer avec le terminal de paiement en mode contact (cartes dites duales). L'initiation de la transaction est bien entendu modifiée par l'utilisation du sans contact, de même d'ailleurs que la suite du traitement, pour laquelle il existe quelques adaptations par rapport à une transaction EMV classique.

Le mode sans contact permet d'initier le paiement plus rapidement, ce qui peut être adapté à certaines situations commerciales pour lesquelles l'exécution rapide de la transaction est cruciale. Le dialogue de la carte avec le terminal par le protocole NFC est réalisé en moins d'une seconde. La carte n'a pas à être introduite dans le lecteur, celui-ci traite la transaction hors ligne (pour éviter le délai requis par l'appel vers le serveur de la banque acquéreur ou émetteur). Par souci d'ergonomie, compte tenu du délai très court de présentation de la carte au terminal, il n'est pas non plus prévu de vérification de code confidentiel ni de confirmation de l'ordre de paiement par le porteur. La simple présentation de la carte à proximité du lecteur suffit à déclencher le paiement. Toutefois, par sécurité, le mode sans contact n'est possible que pour un montant maximal limité, de l'ordre de 20 à 30 euros selon les choix faits par les banques émetteur et acquéreur. De même, dès lors qu'un certain nombre de transactions sans contact a été effectué, ou dès lors que celles-ci atteignent un certain montant cumulé, la transaction doit s'effectuer en mode contact. La remise à zéro des montants cumulés nécessite alors la vérification du code PIN et/ou une demande d'autorisation, pour permettre à nouveau un fonctionnement sans contact.

Initiation du paiement par téléphone mobile en mode sans contact

Dans le domaine de la téléphonie mobile, de nombreux acteurs internationaux étudient différentes options possibles pour permettre le paiement sans contact au moyen d'un téléphone mobile. Parmi celles-ci, on peut distinguer aujourd'hui au moins deux modèles techniques qui ont commencé à être testés en France :

– un premier modèle consiste à inscrire l'application de paiement de la banque du porteur dans la puce SIM (« Subscriber Identity Module ») gérée par l'opérateur téléphonique[32]. C'est alors ce microprocesseur qui exécute les opérations permettant d'initier le paiement. Le téléphone est par ailleurs équipé d'un dispositif NFC pour réaliser la communication avec le terminal de paiement ;

[32] Les standards définis par « Global Platform » pour les puces SIM prévoient que celles-ci comportent différentes unités isolées, les « Security Domains », permettant d'y inscrire des applications logicielles distinctes.

– un second modèle consiste à loger l'application de paiement dans une puce dédiée, le « Secure Element », qui initie la transaction de paiement, contrôle les communications NFC et contient des certificats numériques. Cette architecture permet de développer des services indépendamment des infrastructures des opérateurs de télécommunication, c'est-à-dire sans faire intervenir la puce SIM ni les services associés de téléphonie[33].

On remarque que dans ces deux cas, l'application de paiement est hébergée sur un composant électronique qui n'est plus nécessairement émis par des banques, même si celles-ci en conservent la maîtrise sécuritaire. Cette application est, en effet, incluse dans un espace sécurisé réservé à la banque émettrice, pour lequel cette dernière fixe des exigences spécifiques. L'application de paiement peut être soit pré-chargée en personnalisation, soit téléchargée de manière sécurisée via le réseau de téléphonie mobile. Il est ensuite possible d'activer, suspendre, désactiver ou mettre à jour l'application à distance.

Avec le téléphone mobile, le mode d'initiation du paiement est par définition en mode sans contact. Ce n'est pas le réseau de téléphonie qui est utilisé. Le dispositif de communication NFC dont est équipé le téléphone permet le dialogue entre l'application de paiement et le terminal sans contact, de la même façon que pour les cartes sans contact. L'application de paiement peut permettre de régler tous les montants, avec une possibilité de transaction sans saisie de code ni validation du client en dessous d'un certain montant. Le règlement est débité du compte bancaire auquel est associée l'application de paiement. Après son enregistrement sur le terminal, la transaction est ensuite transmise au serveur de la banque acquéreur comme n'importe quelle transaction par carte.

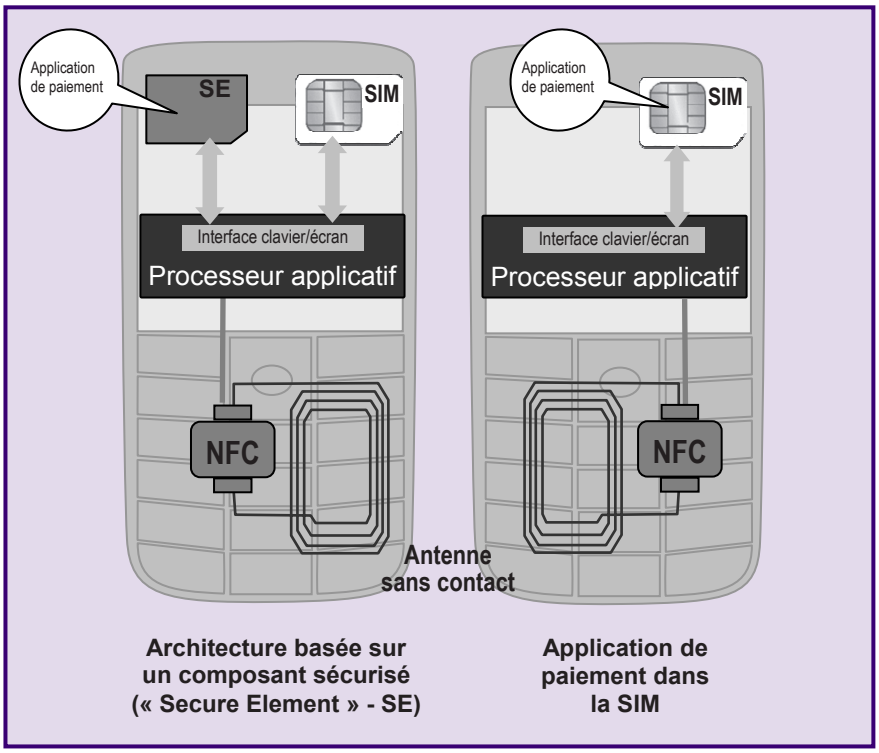


Illustration graphique de deux modèles techniques
de localisation de l'application de paiement
dans le téléphone mobile

[33] On notera qu'il pourrait également y avoir un troisième cas dans lequel serait inscrit dans le téléphone mobile, non pas une application logicielle de paiement du type de celles utilisées pour les cartes, mais un simple dispositif d'authentification permettant d'accéder à distance à une application de paiement. Ce cas n'est pas étudié ici et s'apparente davantage à des solutions d'ordre de paiement électronique à distance comme dans la vente en ligne.

D'autres solutions sont également à l'étude mais ne font pas l'objet d'expérimentations en France. Il existe ainsi, par exemple, des projets consistant à raccorder le processeur gérant l'application de paiement au port d'extension de mémoire dont sont désormais dotés les téléphones de dernière génération. Fonctionnant ainsi comme un module indépendant du téléphone mobile, selon le même principe qu'une carte d'extension de mémoire, ce processeur peut être utilisé sur le téléphone choisi par l'utilisateur, ce qui lui offre plus de souplesse pour le choix de son équipement (technologie « SecureMMC »)[34].

Impacts en matière de sécurité

Par rapport au paiement par carte avec contact, les modes d'initiation sans contact, qu'ils soient par carte ou par mobile, présentent des particularités :

– la communication entre le terminal de paiement et la carte ou le téléphone mobile se fait par ondes radio ;

– le mode d'authentification du porteur est modifié. Par exemple, dans certains cas (petits montants), le code PIN peut ne plus être demandé et le porteur ne valide pas l'ordre de paiement ;

– la puce contenant les données bancaires peut ne plus être, dans le cas du mobile, une puce bancaire.

Il en résulte que la protection de ces paiements présente des particularités par rapport aux paiements par carte en mode contact, et que cela peut appeler la mise en œuvre de nouveaux mécanismes de sécurité. Les dispositions légales destinées à protéger le porteur contestant avoir effectué un paiement pourraient également trouver à s'appliquer compte tenu de la modification du mode d'initiation du paiement.

Mesures de sécurité requises pour les modes d'initiation sans contact

Protection contre l'écoute des informations échangées

Dans les solutions testées en France, les informations susceptibles d'être échangées entre la carte et le terminal sont le numéro de la carte (le PAN)[35], le montant de la transaction et les données d'authentification de la carte. Ces informations sont sensibles voire confidentielles ; elles requièrent donc une protection contre leur capture et leur réutilisation à des fins frauduleuses. C'est pourquoi un certain nombre de mesures sont prises dans ces expérimentations.

Pour éviter la réutilisation des données capturées, la carte ou l'application de paiement du téléphone mobile sont authentifiées de façon dynamique à chaque transaction. De plus, les solutions sur téléphone mobile utilisent un PAN dédié au mode sans contact (PAN distinct du PAN de la carte de paiement, certificat numérique), qui ne serait donc pas réutilisable dans d'autres modes de paiement s'il était intercepté.

---

34 « Secure MultiMediaCardTM », technologie dérivée des spécifications MMC (« MultiMediaCardTM »), cartes mémoires disponibles en plusieurs formats standardisés, et particulièrement courantes comme unités de stockage multimédia pour l'équipement électronique mobile.

35 « Primary Account Number » : données qui identifient l'émetteur et le compte du porteur de la carte.

Dans les applications actuelles de paiement par carte sans contact, le choix a été fait de ne pas présenter le code PIN[36]. Sur téléphone mobile, il est saisi directement sur le clavier du téléphone et n'est pas transmis au terminal.

Compte tenu des spécifications actuelles des réseaux internationaux Visa et Mastercard, les nom et prénom du porteur peuvent être transmis en mode sans contact de façon non protégée, ce qui pose un problème de protection de ces données. En revanche, les expérimentations menées en France dans le domaine du paiement par téléphone mobile évitent un tel risque puisque ces informations ne sont pas gérées.

Activation de l'application de paiement à l'insu du porteur

L'utilisation d'une interface sans contact modifie les enjeux en termes de protection du contenu de la carte, car il devient possible d'établir un dialogue avec la carte – donc d'obtenir des informations sur celle-ci, voire de déclencher une opération de paiement (« télé-pickpocketing ») – sans le consentement du porteur.

Il est par conséquent primordial de faire en sorte que la carte ne délivre aucune information directement utilisable par un fraudeur. Normalement, la limitation de distance du protocole sans contact réduit ce risque, car il est extrêmement difficile d'activer et d'aller lire avec un terminal frauduleux une carte sans contact au delà d'une très courte distance.

Mais pour prévenir tout risque, notamment par relais de la communication sur un équipement distant utilisé par un fraudeur, il est souhaitable de faire en sorte que le terminal détecte un rallongement anormal du délai de transaction, comme cela est susceptible de se produire en cas de relais. L'apport de ce type de contre-mesure reste toutefois à évaluer, surtout avec l'amélioration permanente des technologies. Diverses protections consistant à rendre la carte inopérante sans une action de son propriétaire mériteraient également d'être étudiées (étui de protection, bouton d'activation…).

Dans le cas du téléphone mobile, l'application de paiement est activée soit par le porteur avant d'approcher son téléphone pour effectuer le paiement, soit par le terminal avec validation par le porteur par frappe de code ou non. Afin de protéger l'intégrité de l'application de paiement du téléphone mobile, les promoteurs de ce type de solution ont en outre choisi de n'autoriser l'envoi d'une nouvelle application au « Secure Element » ou à la puce SIM du téléphone portable que chiffrée et signée par la banque et transmise par l'opérateur via un canal sécurisé (par transmission de SMS).

Vol du support

En l'absence de saisie du code PIN et de vérification en ligne de la validité de la carte, il devient possible d'utiliser une carte volée pour des achats de petit montant. Les systèmes de paiement par carte et les banques ont choisi de limiter les risques introduits par ce nouvel usage au travers d'une gestion du risque sophistiquée, fondée sur des compteurs qui, lorsqu'ils atteignent un certain seuil, imposent la bascule en mode contact. La réinitialisation des compteurs suppose alors une authentification du porteur et une autorisation en ligne. Les événements comptés sont par exemple le nombre d'opérations et le cumul des transactions réalisées sans contrôle. L'utilisation de ces compteurs permet donc de limiter le préjudice financier en cas de vol d'une carte ou d'un téléphone mobile sans contact. Ceci suppose toutefois que ces

[36] Il s'agit d'un choix de conception et non d'une impossibilité technique. D'autres applications sans contact en cours de spécification prévoient de transmettre le code PIN chiffré entre le terminal et la carte.

compteurs soient bien protégés contre les manipulations, ce qui doit être pris en compte dès la conception des composants et validé par leur évaluation sécuritaire.

Le paiement par mobile sans contact offre également des possibilités de gestion du risque de nature équivalente, imposant par exemple une demande d'autorisation et/ou une validation du porteur lorsque certains seuils sont dépassés, afin d'autoriser à nouveau le paiement hors ligne. Au niveau organisationnel, le téléphone mobile offre en outre un environnement à certains égards plus avantageux que celui des cartes de paiement. Notamment en cas de vol, l'opérateur de télécommunication peut déclencher le blocage de l'application si celle-ci est sur la puce SIM. Au besoin, l'application de paiement et les plafonds de transaction peuvent être modifiés rapidement grâce à la technologie OTA (« Over The Air »), qui permet la mise à jour à distance de l'application de paiement. Toutefois, cette contre-mesure ne fonctionne pas avec un utilisateur qui configurerait son téléphone pour qu'il ne se connecte pas avec l'opérateur (mode de sélection manuel du réseau ou déconnexion de l'antenne).

Résistance de l'application de paiement aux attaques

Afin d'assurer la sécurité des transactions, il est nécessaire que celles-ci s'exécutent au sein d'un environnement sécurisé. Cette sécurité, tant logique que physique, concerne d'une part le module fonctionnel qui contient l'application de paiement, et d'autre part le téléphone lui-même.

Les autorités bancaires demandent actuellement que les cartes de paiement fassent l'objet d'une certification sécuritaire, ce qui n'est pas encore le cas des puces utilisées pour le paiement par mobile (SIM ou « Secure Element »). Or, l'utilisation du téléphone mobile pour initier des opérations de paiement par carte amène à se poser la question du contrôle de l'accès aux données bancaires, surtout lorsque l'application de paiement est située dans la puce SIM, propriété de l'opérateur téléphonique. Le module fonctionnel responsable de la sécurité de l'application de paiement embarquée doit être évalué avec un niveau d'assurance adapté à cet environnement spécifique.

Le niveau de sécurité doit pouvoir évoluer, pour satisfaire les besoins de ces nouvelles fonctionnalités. Plusieurs solutions sont actuellement envisagées pour atteindre, dans les téléphones mobiles, un niveau de sécurité adapté à une application de paiement. Ainsi, les standards établis par « Global Platform » pour les puces SIM ont été conçus pour cloisonner de manière sécurisée les applications et leurs données. La banque émettrice sera alors la seule à pouvoir accéder à son application, l'opérateur ne faisant que fournir le canal sécurisé permettant cet accès.

Un téléphone mobile constitue un environnement bien plus complexe qu'une carte à puce ou qu'un terminal de paiement. Il est le résultat d'un assemblage de briques technologiques développées indépendamment par plusieurs fournisseurs. La sécurité n'a pas été jusqu'à présent une priorité majeure dans la conception des téléphones : les fonctionnalités et le temps de mise sur le marché ont été ces dernières années des préoccupations beaucoup plus importantes. Les téléphones mobiles sont par exemple exposés à des risques de transmission de logiciels malveillants (capture de données, simulation d'application de paiement à des fins de « phishing », etc.) pouvant être propagés par des canaux comme Bluetooth, Internet, WiFi. D'autre part, l'ajout de fonctionnalités et les nouveaux usages du mobile vont exposer de manière accrue le téléphone aux phénomènes de vol, de fraude et de malveillance.

Conclusion et recommandations de l'Observatoire

L'évolution des technologies permet aujourd'hui aux émetteurs de cartes de paiement d'étudier des solutions innovantes pour réaliser des paiements de proximité. Ainsi, la technologie du sans contact modifie le mode d'initiation du paiement par carte en permettant un dialogue avec le terminal ou l'automate d'acceptation sans introduction de la carte. La même technologie, combinée au fait que l'application de paiement peut désormais être inscrite dans une puce d'un téléphone mobile, permet d'utiliser celui-ci pour initier le paiement par carte.

Ces nouveaux modes d'initiation répondent à des situations de paiement marquées par le souci de rapidité des transactions et apportent ainsi une nouvelle facilité pour les porteurs comme pour les commerçants.

Sur la base des expériences conduites actuellement en France pour ces deux types de solution, l'Observatoire s'est attaché à mesurer les changements que celles-ci présentaient en termes de sécurité par rapport aux cartes à puce fonctionnant aujourd'hui uniquement en mode contact.

Les changements apportés au mode d'initiation du paiement exposent les nouvelles solutions de carte sans contact et de paiement sans contact par téléphone mobile à des risques spécifiques. En particulier, l'échange des données de la transaction par ondes radio avec le terminal de paiement et l'absence d'authentification du porteur et de validation de la transaction en dessous de certains montants requièrent la mise en œuvre de mesures de protection appropriées. Afin d'éviter le risque d'activation ou de détournement de l'application de paiement à l'insu du porteur (« télé-pickpocketing »), l'Observatoire recommande en particulier d'étudier la possibilité de mettre en place des mesures permettant, lorsque cela est nécessaire, de s'assurer du consentement du porteur, par exemple par la mise à disposition de moyens simples pour activer et désactiver ces nouveaux modes d'initiation, ou pour valider toute transaction.

Les solutions introduites actuellement en France sont exclusivement des expérimentations. Des mesures de sécurité sont déjà mises en œuvre et pourront être complétées dans la mesure où les spécifications et les développements ne sont pas encore stabilisés. Aussi est-il important que les banques et les opérateurs de téléphonie mobile, ainsi que leurs prestataires techniques, poursuivent les analyses de risque et les études sécuritaires actuellement en cours afin de définir, avant tout déploiement à grande échelle, des mesures destinées à couvrir les risques spécifiques liés aux nouveaux mécanismes d'initiation et à maintenir un niveau de risque acceptable et comparable à celui observé pour les autres types de cartes de paiement. L'Observatoire recommande en conséquence que ces mesures de réduction de risque fassent l'objet d'une évaluation par un tiers indépendant et contrôlé, rôle joué aujourd'hui par le Schéma national de certification[37].

Pour les cartes sans contact, l'Observatoire note que la certification sécuritaire de ces nouveaux mécanismes par les autorités de certification intervenant actuellement pour les cartes à puce fonctionnant en mode contact ne pose pas de difficulté. Pour les téléphones mobiles, dont le mode de fonctionnement est notablement différent, l'Observatoire recommande que la certification sécuritaire de ces mécanismes soit réalisée en tenant compte des spécificités de leurs architectures.

[37] Cf. Rapport annuel 2005 de l'Observatoire, encadré p. 30

L'Observatoire continuera à exercer une veille technologique sur ces solutions nouvelles afin de tenir compte de la finalisation de leurs spécifications et de leurs développements par les professionnels.

3 | 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 quatre 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 a commencé partout en Europe, avec une progression correcte dans la plupart des pays, globalement en ligne avec l'engagement des banques européennes au sein de l'EPC d'avoir achevé cette migration fin décembre 2010. L'Observatoire s'inquiète cependant des disparités persistantes dans la progression de la migration, qui sont susceptibles de laisser perdurer une fraude transfrontalière européenne significative.

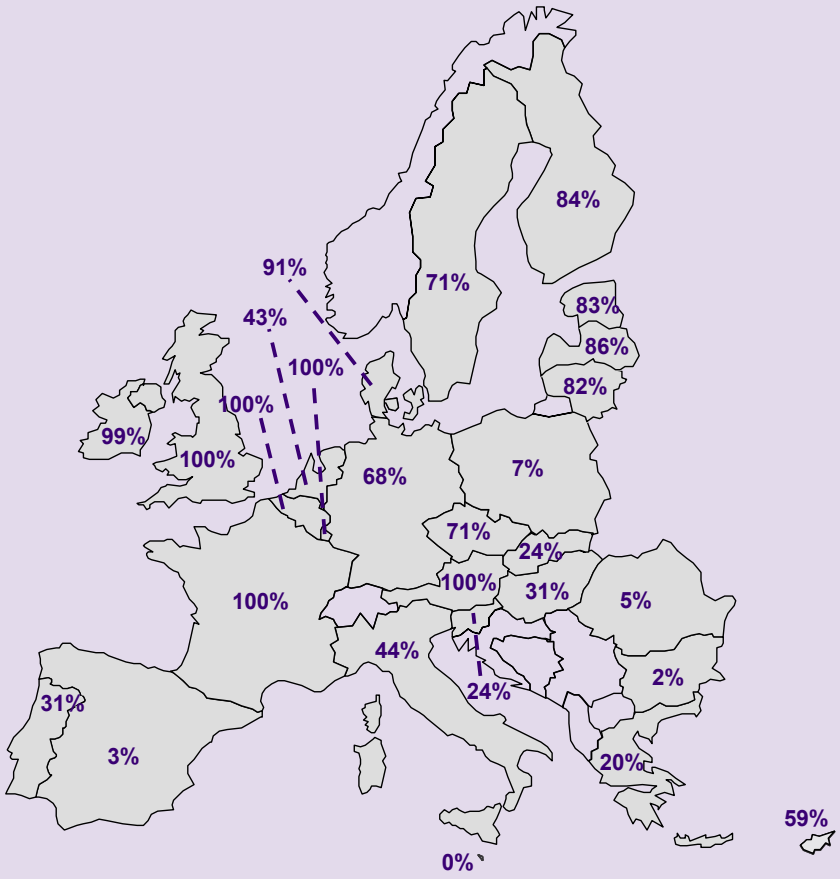
État de la migration en France

En France, la migration au standard EMV est pratiquement terminée. Fin mars 2008, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes CB, 98 % des terminaux et automates, et 100 % des distributeurs automatiques de billets étaient conformes aux spécifications EMV. Les 2 % restants de terminaux et automates, peu utilisés, seront migrés lors de leur remplacement normal.

État de la migration en Europe

Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2008, 61,6 % des cartes interbancaires circulant au sein des 27 États membres de l'Union européenne sont maintenant conformes à la spécification EMV (+ 8 points par rapport à mars 2007). 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 plusieurs grands pays soit est à peine débutée (Espagne, Pologne), soit reste peu avancée.

Encadré 8 – Déploiement des cartes EMV en Europe



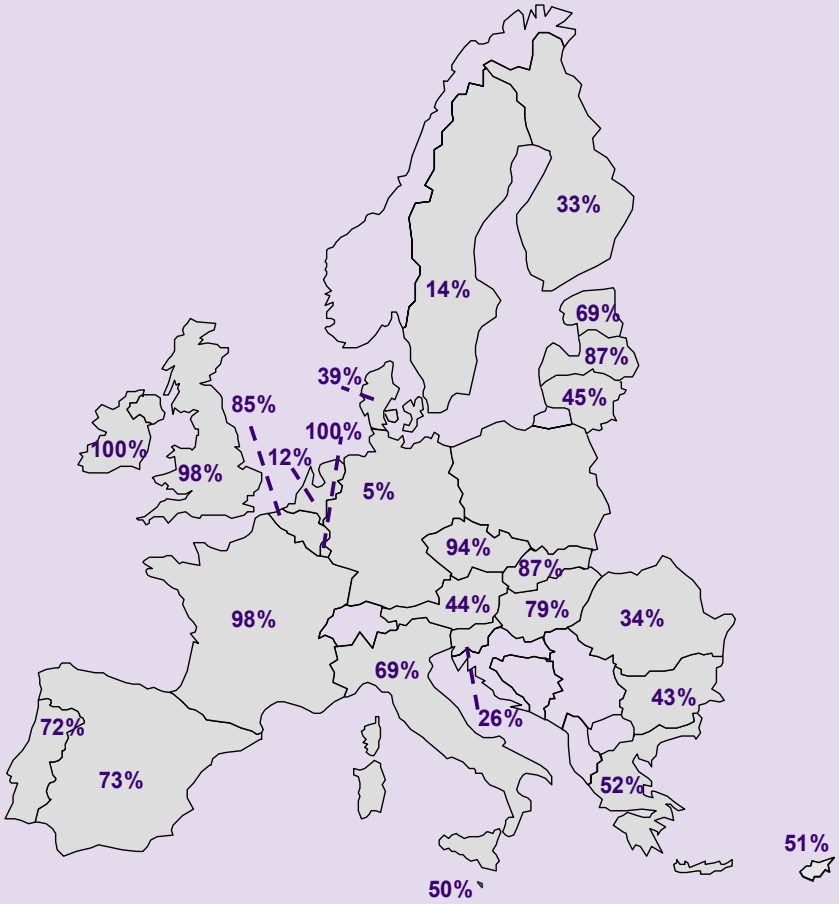
Source : European Payments Council – mars 2008

Par rapport à l'an dernier, on constate une progression générale de la migration des cartes au standard EMV. Toutefois, plusieurs pays débutent à peine leur migration, comme l'Espagne, la Bulgarie, la Roumanie et la Pologne.

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

Concernant l'acquisition, à fin mars 2008 la migration vers EMV progresse encore sensiblement : 66,9 % des terminaux de paiement (voir Encadré 9) et 83,2 % des distributeurs automatiques de billets (voir Encadré 10) sont conformes à EMV (soit une progression de respectivement + 15 points et + 17 points par rapport à mars 2007). La situation reste très contrastée pays par pays, tant en taux d'équipement qu'en progression d'une année sur l'autre.

Encadré 9 – Déploiement des terminaux et automates EMV en Europe



Source : European Payments Council – mars 2008

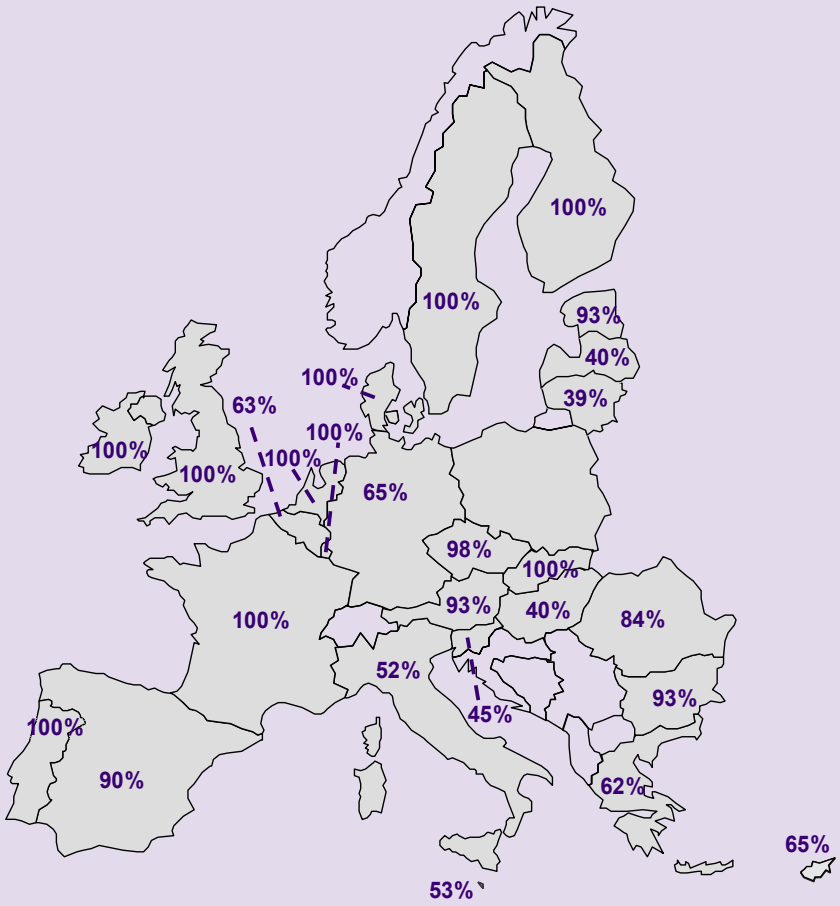
La tendance observée pour les terminaux et automates est à l'inverse de celle constatée pour le déploiement des cartes : la migration des terminaux est globalement plus rapide dans les pays du Sud de l'Europe, qui sont les régions les plus touristiques et donc les plus susceptibles d'enregistrer des volumes élevés de transactions transfrontalières.

La situation évolue toujours très peu en Allemagne, en Suède et aux Pays-Bas par rapport à mars 2007, ces pays restant à un faible niveau d'équipement. L'Autriche et le Danemark, où la migration était à peine entamée l'an dernier, ont en revanche rattrapé leur retard.

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

Les chiffres de la Pologne ne sont pas connus de façon fiable à ce jour.

Encadré 10 – Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2008

La progression de la migration des distributeurs de billets est plus homogène dans les différents pays européens et les taux de migration sont globalement plus élevés que pour les cartes et les terminaux. Il subsiste toutefois quelques disparités. Les pays en cours de migration de leur parc de distributeurs automatiques de billets au standard EMV ont probablement choisi de migrer en priorité les automates utilisés par les touristes et visiteurs étrangers. L'Allemagne et l'Italie restent en deçà des niveaux de déploiement des autres grands pays mais ont pratiquement doublé leur niveau d'équipement par rapport à mars 2007.

Les chiffres de la Pologne ne sont pas connus de façon fiable à ce jour.

4 | IMPACT DE LA DIRECTIVE SUR LES SERVICES DE PAIEMENT SUR LES RÈGLES APPLICABLES AUX CARTES DE PAIEMENT EN FRANCE

Dans son étude de 2005 sur la sécurité des cartes dans le cadre de l'harmonisation européenne, l'Observatoire s'était félicité de l'élaboration d'une directive sur les services de paiement permettant la mise en place d'un cadre juridique commun pour les paiements en Europe. Il avait porté une attention particulière à plusieurs points de la proposition de directive : la création du nouveau statut d'« établissement de paiement » à côté du statut bancaire ; la définition de l'irrévocabilité du paiement ; les allégements réglementaires prévus pour les paiements considérés comme de faible montant.

La directive sur les services de paiement a été adoptée le 13 novembre 2007[38] et doit être transposée dans les droits nationaux des États membres avant le 1er novembre 2009. Ce nouveau texte refonde largement le droit existant. Dans le domaine des cartes de paiement, la directive fait suite aux efforts d'harmonisation européenne qui avaient déjà abouti à des recommandations, notamment en matière de « paiement électronique ». Plus récemment, deux directives[39] avaient permis d'établir des règles communes auxquelles les dispositions de la directive sur les services de paiement vont se substituer.

Les objectifs du nouveau texte européen sont ambitieux et l'Observatoire a souhaité mesurer l'importance des changements qu'il induira en droit français. Le marché des paiements, donc celui des cartes, va ainsi s'ouvrir à de nouveaux acteurs non bancaires, les établissements de paiement (I). La directive conduira également à une harmonisation des droits nationaux des États membres en posant des règles communes pour l'ensemble des services de paiement, ce qui constitue une approche différente de celle privilégiée en droit français (II). Par ailleurs, les obligations d'information de la clientèle devront évoluer (III), mais aussi les règles d'irrévocabilité et de contestation, ce qui modifiera l'équilibre des droits entre les porteurs et les accepteurs (IV).

4|1 L'ouverture du marché des cartes à de nouveaux acteurs non bancaires

La directive sur les services de paiement couvre comme le droit français actuel l'ensemble des activités d'émission et de gestion de cartes de paiement. Elle favorisera néanmoins une forte évolution du marché en permettant l'émergence de nouveaux prestataires non bancaires, les établissements de paiement.

---

38 Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.

39 La directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrat à distance et la directive 2002/65/CE concernant la commercialisation à distance des services financiers auprès des consommateurs.

Un champ d'application très comparable au droit français actuel

La directive inclut dans son champ plusieurs services de paiement couvrant l'ensemble des activités d'émission et de gestion de cartes de paiement : l'émission de cartes et l'acquisition des données liées aux opérations de paiement effectuées par carte, les opérations de paiement, qu'elles soient réalisées ou non à partir d'un compte ou d'une ligne de crédit et, enfin, les retraits d'espèces. Le droit français actuel incluait de la même façon depuis 1984 l'ensemble de ces activités dans le champ des activités bancaires de mise à la disposition du public et de gestion de moyen de paiement.

La directive exclut de son champ certains instruments de paiement (dont les cartes) dits à « utilisation limitée ». L'article 3(k) de la directive exclut ainsi « les services fondés sur des instruments qui ne peuvent être utilisés, pour l'acquisition de biens ou de services, que dans les locaux utilisés par l'émetteur ou, dans le cadre d'un accord commercial avec l'émetteur, à l'intérieur d'un réseau limité de prestataires de services ou pour un éventail limité de biens ou de services ». Ces dispositions sont proches de l'actuel article L. 511-7 I, 5° du Code monétaire et financier. Mais des travaux sont actuellement menés pour évaluer si la directive suppose de modifier les modalités d'application de cet article.

Les établissements de paiement, nouvelle catégorie de prestataire de services de paiement aux côtés des établissements de crédit

Contrairement au droit français actuel, la directive ne réserve pas aux seuls établissements de crédit la prestation de services de paiement mais permet à de nouveaux acteurs, les établissements de paiement, de s'y engager. Ceux-ci pourront donc fournir l'ensemble des services de paiement définis par la directive. A titre accessoire de certaines prestations de service de paiement, ils pourront également octroyer des crédits, de manière limitée et harmonisée pour les opérations transfrontalières, et dans le respect des obligations nationales au plan domestique. Le texte établit des obligations statutaires allégées pour l'exercice des activités de ces nouveaux prestataires. Certaines de ces obligations varient selon les services de paiement effectués. Ainsi, les établissements de paiement devront être dotés d'un capital initial de 125 000 euros pour s'engager dans la prestation de services de paiement par carte et devront disposer de fonds propres. L'Observatoire avait eu l'occasion en 2005 de se prononcer en faveur de la meilleure protection possible des fonds confiés par les utilisateurs aux établissements de paiement. De ce point de vue, la directive oblige uniquement les établissements de paiement à protéger les fonds reçus des utilisateurs lorsqu'ils exerceront d'autres activités en plus de leur activité de prestation de services de paiement. Mais il est intéressant de noter que la transposition pourra prévoir que cette obligation de protection s'applique même si l'établissement se spécialise dans la prestation de services de paiement en n'exerçant que cette seule activité. Cet agrément ouvrira la possibilité aux établissements de paiement d'exercer leur activité dans n'importe quel autre État membre, par le mécanisme de la reconnaissance mutuelle européenne.

Dans un but de développement de la concurrence, la directive prévoit de plus que les établissements de paiement doivent pouvoir avoir accès aux systèmes de paiement, ce qui inclut certains systèmes de paiement par carte. Les règles régissant l'accès à ces systèmes de paiement doivent ainsi être « objectives, non discriminatoires et proportionnées ». L'Observatoire avait considéré en 2005 que cet accès pourrait constituer un facteur de risque si les établissements de paiement ne présentaient pas de garanties financières suffisantes. Il convient cependant de noter que les dispositions de la directive précisent que ces règles ne doivent pas entraver l'accès aux systèmes « dans une mesure excédant ce qui est nécessaire pour prévenir certains risques spécifiques tels que le risque de règlement, le risque opérationnel et le risque d'entreprise et protéger la stabilité financière et opérationnelle des systèmes de

paiement ». Les systèmes de carte de type « interbancaire » devront ainsi permettre l'accès à tout prestataire de services de paiement qui en fait la demande ou, à tout le moins, ne pas restreindre l'accès à leur système pour des motifs qui ne seraient pas liés objectivement à la sécurité de celui-ci. En revanche, les systèmes de type « privatif » n'ont pas cette obligation, le législateur européen ayant considéré que le mode de fonctionnement de ces systèmes ne requérait pas le libre accès à leur système.

L'ambition du texte européen de favoriser la concurrence dans le domaine des services de paiement est indissociable de la nécessaire harmonisation des règles régissant l'exercice de la profession, mais également des règles applicables aux opérations de paiement. Cette harmonisation aura un double impact en droit français : elle conduira à un renforcement du cadre législatif et réglementaire relatif aux paiements et favorisera une approche nouvelle de cette activité, fondée sur un souci de neutralité technologique.

4|2 Une approche nouvelle de la réglementation applicable aux paiements

Un cadre législatif et réglementaire renforcé

Alors que le droit français des paiements repose actuellement largement sur des règles professionnelles et peu sur des dispositions législatives et réglementaires, la transposition de la directive conduira à fixer dans la loi ou le règlement un plus grand nombre de règles.

Ainsi, la partie législative du Code monétaire et financier ne comporte aujourd'hui que six articles concernant les cartes de paiement (auxquels il faut ajouter les dispositions relatives aux infractions). Ces dispositions visent essentiellement à favoriser l'utilisation de ce moyen de paiement en garantissant une bonne protection aux porteurs. Outre une définition de la carte de paiement et l'affirmation du principe d'irrévocabilité de l'ordre de paiement donné au moyen d'une carte, le Code monétaire et financier précise le niveau de responsabilité du titulaire de la carte en cas de perte, de vol ou d'utilisation frauduleuse à distance. Il fixe également le délai légal pendant lequel le titulaire d'une carte peut faire une réclamation. Pour le reste, ce sont des règles professionnelles contractuelles qui précisent les conditions d'utilisation des cartes de paiement.

La directive sur les services de paiement établit un cadre beaucoup plus complet en précisant les obligations d'information et les règles applicables aux opérations de paiement en matière de consentement, de révocation, de contestation et d'exécution (respectivement titres III et IV de la directive). Ces dispositions seront transposées en droit français, pour certaines dans le domaine législatif, pour d'autres dans le domaine réglementaire.

Ces règles seront communes à tous les utilisateurs de services de paiement de l'Union européenne. En effet, la directive sur les services de paiement est une directive de pleine harmonisation, même si elle comporte un certain nombre de dispositions pour lesquelles différentes options sont laissées à l'appréciation des autorités nationales et laisse la place à quelques adaptations contractuelles. De plus, la communauté française a fait part à plusieurs reprises de sa préoccupation que les transpositions nationales convergent vers des interprétations communes. Ceci fera donc l'objet d'une vigilance particulière lors des travaux de transposition.

Un socle commun à tous les services de paiement mais qui prévoit quelques distinctions selon le mode d'initiation des opérations ou les instruments utilisés

La transposition de la directive en droit français conduira à ne plus faire apparaître de dispositions applicables par type de moyen de paiement. En effet, la directive sur les services de paiement ne s'appuie pas, contrairement au droit français, sur la notion de moyen de paiement. Elle définit des règles pour un ensemble de « services de paiement », cette notion se rapprochant de celle d'opérations de « mise à disposition ou de gestion de moyens de paiement » existant dans le droit français actuel. Les opérations relatives aux cartes de paiement seront donc soumises au socle de règles commun aux services de paiement. Conformément au souhait du législateur européen, cette approche permettra une neutralité technologique des règles applicables aux paiements quelles que soient les techniques utilisées et leur évolution dans le temps, tout en tenant compte des spécificités des services concernés.

Pour l'application de certaines dispositions, comme en matière de révocation des ordres, de contestation des paiements et d'exécution des opérations, la directive distingue ainsi les services de paiement en fonction de leur mode d'initiation. Elle désigne notamment les paiements par carte sous le vocable « d'opérations initiées via le bénéficiaire », expression qui pourra faire l'objet d'adaptation au moment de la transposition pour plus de lisibilité. Les autres types d'opération sont également désignés de manière générique par les expressions suivantes : « opérations initiées par le payeur » dans le cas des virements, « opérations initiées par le bénéficiaire » dans le cas des prélèvements.

Pour préciser certaines dispositions, la directive s'appuie également, dans un nombre limité d'articles, sur la notion d'instrument de paiement ou plus précisément sur la notion d'instrument de paiement équipé d'un « dispositif de sécurité personnalisé », c'est-à-dire permettant d'authentifier le payeur. Ces articles visent essentiellement les transactions effectuées par carte, par téléphone portable si l'application de paiement est assortie d'un dispositif de sécurité personnalisé, ainsi que celles effectuées depuis des sites de banque en ligne.

Enfin, la directive prévoit un régime dérogatoire pour les instruments de paiement « relatifs à des montants faibles ». L'Observatoire avait fait part en 2005 de sa préoccupation concernant ce régime, compte tenu que le montant alors envisagé par la Commission européenne aurait pu conduire à une application de ce régime à une grande partie des opérations de paiement par carte. Dans la lignée de ses propositions initiales, la directive prévoit au final un allégement réglementaire pour ces instruments, notamment en matière d'obligation d'information et de contestation. Le dispositif finalement retenu ne s'applique toutefois qu'à des instruments dont le montant maximal de transaction ne peut, par contrat, dépasser 30 euros.

4|3 Harmonisation des obligations d'information

Organisées autour de l'élaboration d'un même contrat-cadre pour tous les services de paiement, y compris ceux fournis à partir d'une carte de paiement, les informations que le prestataire de services de paiement doit fournir à son client sont énumérées par la directive. Celle-ci prévoit également la possibilité pour un commerçant de moduler ses tarifs en fonction du moyen de paiement utilisé par son client.

Pour les contrats porteur et accepteur

La directive harmonise les obligations d'information à la charge des prestataires à la fois pour les opérations de paiement isolées et pour les opérations relevant d'un « contrat-cadre ». Les opérations de paiement par carte relèvent de ce deuxième cas : en effet, l'émission d'une carte se fait sur la base d'un contrat entre l'émetteur et le porteur qui régit à la fois les modalités de délivrance de la carte et ses modalités d'utilisation, l'acquisition des opérations se fait également sur la base d'un contrat entre l'acquéreur et l'accepteur. La directive précise les mentions à faire figurer dans ces contrats-cadres. Il s'agit d'informations sur le prestataire de services de paiement (nom et coordonnées), sur l'utilisation du service de paiement (forme et procédure du consentement, délai d'exécution, possibilité de convenir de limites de dépenses pour l'utilisation d'un instrument de paiement), sur les frais (y compris taux d'intérêt et taux de change), sur la communication (fréquence), sur les mesures de protection et les mesures correctives (mesure à prendre pour préserver la sécurité d'un instrument, possibilité de blocage de l'instrument, responsabilité du prestataire et du payeur, conditions de remboursement...), sur la modification et la résiliation d'un contrat (durée du contrat, droit de résiliation) et sur les recours possibles.

La directive encadre également les modalités de modification et de résiliation de ces contrats porteurs ou accepteurs, ce qui constitue une nouveauté pour les contrats carte. En ce qui concerne la modification des conditions contractuelles, ces dispositions se situent cependant largement dans la lignée de ce qui existe aujourd'hui en matière de conventions de compte. La directive prévoit ainsi que toute modification doit être proposée par le prestataire de services de paiement au plus tard deux mois avant la date proposée pour son entrée en vigueur. Sauf refus explicite de l'utilisateur avant la date d'entrée en vigueur, la modification est réputée acceptée. Dans le cas où l'utilisateur n'accepterait pas la modification, il a le droit de résilier son contrat immédiatement et sans frais, avant la date d'entrée en vigueur de la modification.

En matière de résiliation, la directive encadre en revanche davantage les pratiques et propose un cadre un peu plus favorable aux utilisateurs de services de paiement que celui actuellement en vigueur en France. Un contrat-cadre peut ainsi être résilié à tout moment par le client à moins que les parties ne soient convenues d'un délai de préavis, celui-ci ne pouvant excéder un mois. Cette résiliation n'emporte pas de frais si le contrat-cadre a été conclu pour une durée déterminée supérieure à 12 mois ou s'il a été conclu pour une durée indéterminée. Dans les autres cas, les frais de résiliation doivent être adaptés et en rapport avec les coûts.

Application de frais ou de déductions pour l'usage des moyens de paiement scripturaux

La directive prévoit un dispositif inspiré des pratiques anglo-saxonnes en fixant un principe de liberté pour le commerçant de pratiquer une facturation particulière, à la hausse ou à la baisse, en fonction du moyen de paiement scriptural utilisé. Cela signifie que, pour l'usage d'un moyen de paiement, le client pourra se voir offrir une réduction ou se voir appliquer des frais particuliers s'ajoutant au prix des biens ou services achetés. Les pratiques de réduction pour l'usage d'un moyen de paiement particulier sont déjà courantes en France, notamment pour les cartes de type « privatif » choisies par les commerçants. En revanche, l'application de frais, qui n'est pas interdite par le droit français actuel mais toutefois très peu répandue, serait nouvelle. Se pose donc la question de savoir quelle utilisation faire de la possibilité laissée par la directive aux États membres d'encadrer ou d'interdire l'application de frais spécifiques à l'usage d'un instrument de paiement. La transposition du texte en droit français devra tenir compte des risques que cette possibilité laissée aux commerçants peut créer en termes de modification de l'usage des différents moyens de paiement.

4 | 4 De nouvelles règles de révocation et de contestation

Si la directive sur les services de paiement pose un principe général d'irrévocabilité des ordres de paiement, elle offre des possibilités plus larges de contestation d'une opération de paiement. Déjà pratiquées par un certain nombre de pays, ces possibilités sont nouvelles en France, elles devront donc s'accompagner d'un effort d'information pour éviter d'éventuelles dérives.

Une irrévocabilité maintenue

L'Observatoire avait souligné en 2005 qu'il convenait de faire preuve de vigilance à l'égard de la définition de l'irrévocabilité prévue par la directive. En effet, le principe d'irrévocabilité est aujourd'hui un principe fondamental du paiement par carte, imposé en droit français par la loi (cf. article L. 132.2 du Code monétaire et financier : « l'ordre ou l'engagement de payer donné au moyen d'une carte de paiement est irrévocable »). Le paiement est ainsi considéré comme certain et irrévocable dès la saisie par le porteur de son code confidentiel. Le dispositif prévu au principal par la directive est proche du droit français actuel puisqu'il prévoit que, pour les « paiements initiés via le bénéficiaire » comme c'est le cas pour un paiement par carte, l'ordre de paiement ne doit plus pouvoir être révoqué une fois que le payeur a transmis au bénéficiaire son consentement à l'exécution de l'opération de paiement. Si les principes posés par la directive sont semblables à ceux du droit français actuel, les dérogations contractuelles prévues par le texte pourront permettre de s'en écarter, ce qui aboutirait à des situations hétérogènes pour les clients. Ces dérogations contractuelles ne sont toutefois possibles que si le porteur, son prestataire de services de paiement et le bénéficiaire en sont d'accord.

Des possibilités de contestation plus larges

La transposition de la directive élargira sensiblement les possibilités offertes actuellement par le droit français pour contester des paiements. La directive prévoit deux dispositifs, selon que le payeur n'a pas consenti au paiement ou qu'il en conteste seulement le montant.

Le premier dispositif concerne 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. En principe, le débiteur dispose d'un délai de 13 mois suivant la date de débit pour contester avoir autorisé une opération de paiement. Son prestataire devra alors rétablir le compte 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. Ce délai de contestation de 13 mois est beaucoup plus protecteur pour le porteur de carte que la règle appliquée actuellement en droit français : celle-ci fixe un délai de 70 jours à compter de la date de l'opération contestée, qui peut être prolongé contractuellement jusqu'à 120 jours. Nonobstant l'extension du délai de contestation à treize mois, et dans la ligne de la réglementation française actuelle, le porteur devra, lorsqu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer sans tarder son prestataire de services de paiement.

Une dérogation à ces règles de remboursement est cependant prévue par la directive pour les instruments équipés d'un dispositif de sécurité personnalisé, donc notamment pour les cartes de paiement. Le payeur pourra dans ce cas supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé ou, « si le payeur n'est pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, consécutive au détournement d'un instrument de paiement ». Ceci s'entend sauf agissement frauduleux ou négligence grave du titulaire et avant

la mise en opposition de la carte. Cette dernière formulation retenue dans la directive est ambiguë et pourrait aboutir à s'écarter du droit français actuel qui ne retient l'engagement de la responsabilité du porteur à concurrence de 150 euros que pour les cas de vol ou de perte. Il conviendra donc lors des travaux de transposition de porter une attention particulière à ce point, afin d'assurer le maintien du haut niveau de protection accordé à l'heure actuelle aux porteurs de cartes en cas de paiement non autorisé effectué frauduleusement à distance, sans utilisation physique de la carte ou en cas de contrefaçon.

Le deuxième cas de contestation ouvert par la directive aux porteurs concerne les opérations ayant fait l'objet d'une autorisation générale de la part du payeur, mais sans que le montant précis de l'opération n'ait été indiqué au moment de l'autorisation. Ce dispositif s'applique notamment aux paiements par carte, par exemple lors de réservations d'hôtel ou de voitures. Ainsi, lorsque le payeur a donné son consentement à une opération de paiement, il pourra, dans un délai de 8 semaines à compter de la date à laquelle les fonds ont été débités, demander un remboursement de cette opération dans le cas où le montant de l'opération finalement exécutée dépasserait le montant auquel le payeur pouvait raisonnablement s'attendre compte tenu de ses dépenses passées, des conditions prévues au contrat-cadre ou autres circonstances pertinentes. Dans un délai de 10 jours ouvrables suivant la réception de la demande de remboursement, le prestataire de services de paiement devra alors rembourser le montant total de l'opération de paiement, ou justifier son refus de rembourser en indiquant les organismes que le payeur peut saisir s'il n'accepte pas la justification donnée. Il s'agit d'une nouveauté par rapport au droit français qui permettra de couvrir des situations pour lesquelles il existe aujourd'hui un certain nombre de contentieux.

4|5 Conclusion

La transposition de la directive sur les services de paiement va sensiblement modifier la réglementation applicable aux paiements en France. Elle ouvre tout d'abord le marché des paiements à de nouveaux acteurs, les établissements de paiement, aux côtés des banques. Elle fournit également un cadre juridique beaucoup plus dense qui repose plus sur des dispositions législatives ou réglementaires que sur des règles contractuelles. Adoptant une approche globale, le législateur européen a cherché à ne pas différencier les services de paiement et a fondu les règles relatives aux cartes de paiement dans un ensemble qui se veut technologiquement neutre, tout en tenant compte des caractéristiques essentielles du paiement par carte. Il a établi la liste des informations dont doit pouvoir bénéficier tout utilisateur de services de paiement et donné un cadre à la possibilité pour un commerçant de moduler ses tarifs en fonction du mode de paiement de son client. Enfin, la directive, tout en confirmant le principe d'irrévocabilité d'un paiement, ouvre des possibilités plus larges de contestation.

D'ici le 1er novembre 2012, la Commission européenne devra réaliser un rapport sur la mise en œuvre de la directive qui permettra de mesurer l'impact qu'elle aura eu au niveau européen sur les modes d'utilisation des services de paiement et le niveau de compétitivité du marché des paiements.

ANNEXE A | MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

Le décret n° 2002-709 du 2 mai 2002 pris pour l'application de l'article L. 141-4 du Code monétaire et financier relatif à l'Observatoire de la sécurité des cartes de paiement a précisé les missions, la composition et les modalités de fonctionnement de l'Observatoire.

Cartes concernées

D'après l'article L. 132-1 du Code monétaire et financier, « constitue une carte de paiement toute carte émise par un établissement de crédit ou par une institution mentionnée à l'article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds ».

En conséquence, les compétences de l'Observatoire concernent les cartes émises par les établissements de crédit ou par une institution assimilée et dont les fonctions sont le retrait ou le transfert de fonds et ne couvrent pas les cartes monoprestataires bénéficiant d'une dérogation au monopole bancaire par l'article L. 511-7 I. 5 du Code monétaire et financier. Ces cartes, parfois appelées « cartes purement privatives », sont émises par un seul établissement et acceptées en paiement par lui-même ou par un nombre limité d'accepteurs ayant noué avec lui des liens de solidarité financière et commerciale.

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 d'établissements de crédit émetteurs et acquéreurs (cartes généralement qualifiées de « privatives ») ;

– un nombre élevé d'établissements de crédit émetteurs et acquéreurs (cartes généralement qualifiées « d'interbancaires »).

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 dépôt de fonds 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 permettant 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 ».

Attributions

Conformément à l'article L. 141-4 du Code monétaire et financier et au décret du 2 mai 2002 précités, 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.

En outre, le ministre chargé de l'économie et des finances peut saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

Composition

Le décret du 2 mai 2002 précité a déterminé 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 la Commission bancaire 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 B.

Les membres de l'Observatoire, autres que ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de la Commission bancaire, sont nommés pour trois ans. Leur mandat est renouvelable deux fois. Le président est désigné parmi ces membres par le ministre chargé de l'économie et des finances. Son mandat est de trois ans, renouvelable deux fois. Monsieur Christian NOYER, Gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément au décret du 2 mai 2002, 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 au début de chaque année au ministre chargé de l'économie et des finances, et transmis au Parlement.

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'économie et des finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail 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.

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat 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 B | LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

La composition actuelle de l'Observatoire a été définie par un arrêté du ministre de l'économie, des finances et de l'industrie du 20 avril 2006, complété par un arrêté du 22 juin 2006. Elle a été modifiée en 2007 par deux arrêtés en date du 27 juin et du 25 octobre 2007.

Liste des membres jusqu'au 27 juin 2007

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD
Député

Nicole BRICQ
Sénatrice

Représentant du secrétaire général de la Commission bancaire

Jean-Luc MENDA
Direction de la surveillance générale du système bancaire

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

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

Sur proposition du ministre de l'économie, des finances et de l'industrie :

- Le haut fonctionnaire de défense :
  Emmanuel SARTORIUS

- Le directeur général du Trésor et de la politique économique ou son représentant :
  Maya ATIG

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 :
  Jean-Pierre GERSKOUREZ
  Jean-Yves SAUSSOL

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Pauline FLAUSS
  Maxence DELORME

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 :
  Christian AGHROUM

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

Brigitte CHARLIER
Directrice de la Monétique - CEDICAM

Patrice COUFFIGNAL
Directeur - Europay France

Armand de MILLEVILLE
Vice président exécutif - American Express France

Jean-Marie DRAGON
Expert monétique - La Banque Postale

Bernard DUTREUIL
Directeur - Fédération bancaire française

Hervé DUCHARNE
Audit Manager et Études - Groupement Carte Bleue

Alain GOLDBERG
Directeur risques et conformité - Natixis Paiements

Dominique JOLIVET
Responsable du département maîtrise des risques et sécurité monétique - Caisse Nationale des Caisses d'Épargne

Cédric SARAZIN
Directeur Business et stratégie - Groupement des Cartes Bancaires

Gérard JOUVE
Directeur des Relations institutionnelles - CETELEM

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

Michèle DAUPHIN
Représentante conseillère technique - Familles de France

Valérie GERVAIS
Secrétaire générale - Association FO Consommateurs (AFOC)

Jean-Pierre JANIS
Conseil National des Associations Familiales Laïques (CNAFAL)

Christian HUARD
Secrétaire général - Association d'éducation et d'information du consommateur de l'Éducation nationale (ADEIC)

Frédérique PFRUNDER
Chargée de mission - Confédération du logement et du cadre de vie (CLCV)

Représentants des organisations professionnelles de commerçants

Richard BOUTET
Conseiller pour les moyens de paiement 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-Marc MOSCONI
Délégué général - MERCATEL

Philippe SOLIGNAC
Vice-président - Chambre de commerce et d'industrie de Paris/ACFCI

Guillaume VANOVERSCHELDE
Directeur administratif et financier - DECATHLON

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL
Executive Vice-President - Gemalto

Jacques STERN
Professeur – Ecole normale supérieure

Sophie VULLIET-TAVERNIER
Directeur des affaires juridiques - Commission nationale de l'informatique et des libertés (CNIL)

Liste des membres depuis le 27 juin 2007

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD
Député

Nicole BRICQ
Sénatrice

Représentant du secrétaire général de la Commission bancaire

Jean-Luc MENDA
Corinne DAUCHY
Direction de la surveillance générale du système bancaire

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

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

Sur proposition du ministre de l'économie, des finances et de l'emploi :

- Le haut fonctionnaire de défense :
  Emmanuel SARTORIUS

- Le directeur général du Trésor et de la politique économique ou son représentant :
  Maya ATIG
  Catherine JULIEN-HIEBEL

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 :
  Jean-Pierre GERSKOUREZ
  Jean-Yves SAUSSOL

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Pauline FLAUSS
  Maxence DELORME

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 :
  Christian AGHROUM

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

Brigitte CHARLIER
Directrice de la Monétique - CEDICAM

Patrice COUFFIGNAL
Directeur - Europay France

Armand de MILLEVILLE
Vice président exécutif - American Express France

Jean-Marie DRAGON
Expert monétique - La Banque Postale

Bernard DUTREUIL
Directeur - Fédération bancaire française

Alain GOLDBERG
Directeur risques et conformité - Natixis Paiements

Dominique JOLIVET
Responsable du département maîtrise des risques et sécurité monétique - Caisse Nationale des Caisses d'Épargne

François LANGLOIS
Directeur des Relations institutionnelles - CETELEM

Jean-Christophe LEGALLAND
Groupement Carte Bleue

Cédric SARAZIN
Directeur Business et stratégie - Groupement des Cartes Bancaires

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

Michèle DAUPHIN
Représentante conseillère technique - Familles de France

Valérie GERVAIS
Secrétaire générale - Association FO Consommateurs (AFOC)

Jean-Pierre JANIS
Conseil National des Associations Familiales Laïques (CNAFAL)

Christian HUARD
Secrétaire général - Association d'éducation et d'information du consommateur de l'Éducation nationale (ADEIC)

Frédérique PFRUNDER
Chargée de mission - Confédération du logement et du cadre de vie (CLCV)

Représentants des organisations professionnelles de commerçants

Philippe JOGUET[1]
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

Jacques STERN
Président du Conseil d'Administration - Ingenico
Président du Conseil d'Administration - Agence nationale de la recherche (ANR)

Sophie VULLIET-TAVERNIER
Directeur des affaires juridiques - Commission nationale de l'informatique et des libertés (CNIL)

[1] Nommé par arrêté en date du 27 octobre 2007

ANNEXE C | 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 150 membres du Groupement des Cartes Bancaires (« CB ») par l'intermédiaire de celui-ci ainsi que d'Europay France et du Groupement Carte Bleue pour les données internationales ;
- neuf émetteurs de cartes privatives : American Express, Banque Accord, Cetelem, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;
- les émetteurs du porte-monnaie électronique Moneo.

Les données collectées concernent également trois accepteurs de cartes de paiement, à savoir France Loisirs, Monoprix et la SNCF. L'Observatoire a également reçu des statistiques recueillies par la Fevad auprès d'un échantillon représentatif de ses membres et des statistiques recueillies par la FCD et par Mercatel pour la grande distribution et le commerce spécialisé.

Total des cartes en circulation en 2007 : 81,5 millions

- dont 55,7 millions de cartes de type « interbancaire » (« CB » et Moneo) ;
- et 25,7 millions de cartes de type « privatif ».

Cartes mises en opposition en 2007 : environ 460 000

Les transactions nationales sont celles qui mettent en jeu un porteur français et un commerçant accepteur français. Les transactions internationales sont de deux types : porteur français / accepteur étranger et porteur étranger / accepteur français.

Le marché des cartes de paiement en France

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
Cartes de type « interbancaire »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (en Md€)**	**Volume (millions)**	**Valeur (en Md€)**
Paiement de proximité et sur automate	5 606,80	250,66	112,35	8,55	140,41	13,03
Paiements à distance hors Internet	nd	11,80	7,04	0,90	5,80	1,57
Paiements à distance sur Internet	115,00	9,20	35,99	2,43	10,54	1,25
Retraits	1 337,51	93,12	37,06	4,39	29,11	5,01
Total	**7 059,31**	**364,79**	**192,44**	**16,28**	**185,86**	**20,86**
Cartes de type « privatif »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (en Md€)**	**Volume (millions)**	**Valeur (en Md€)**
Paiement de proximité et sur automate	208,04	22,91	9,03	1,54	16,52	2,87
Paiements à distance hors Internet	0,45	0,05	0,29	0,06	0,10	0,03
Paiements à distance sur Internet	1,29	0,18	0,16	0,03	0,48	0,07
Retraits	10,50	1,03	nd	nd	nd	nd
Total	**220,28**	**24,17**	**9,48**	**1,63**	**17,11**	**2,96**
Total général	**7 279,58**	**388,95**	**201,92**	**17,91**	**202,97**	**23,82**

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 »

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**540,3**	**38 006,0**	**159,4**	**29 127,0**	**343,9**	**59 267,6**[1]
Cartes perdues ou volées	474,9	34 046,7	80,0	8 336,2	105,8	10 070,6
Cartes non parvenues	5,4	302,7	1,2	304,4	6,7	489,8
Cartes altérées ou contrefaites	60,1	3 656,5	69,0	18 901,2	82,9	21 783,3
Numéro de carte usurpé	0,0	0,0	2,9	402,3	8,4	749,4
Autres	0,0	0,0	6,4	1 182,9	140,2	26 174,5
Paiements à distance hors Internet	**295,2**	**23 411,5**	**44,0**	**6 502,9**	**nd**	**nd**
Cartes perdues ou volées	50,0	2 549,4	14,8	2 541,2	nd	nd
Cartes non parvenues	0,3	18,7	0,1	16,3	nd	nd
Cartes altérées ou contrefaites	7,5	607,1	12,8	1 994,1	nd	nd
Numéro de carte usurpé	237,3	20 236,4	0,9	58,6	nd	nd
Autres	0,0	0,0	16,4	1 892,8	nd	nd
Paiements à distance sur Internet	**188,2**	**26 184,2**	**233,9**	**27 249,1**	**nd**	**nd**
Cartes perdues ou volées	11,2	1 010,9	69,1	8 148,6	nd	nd
Cartes non parvenues	0,1	14,6	0,2	18,1	nd	nd
Cartes altérées ou contrefaites	4,2	609,3	66,1	8 398,3	nd	nd
Numéro de carte usurpé	172,7	24 549,4	1,2	115,1	nd	nd
Autres	0,0	0,0	97,3	10 569,1	nd	nd
Retraits	**81,9**	**17 989,1**	**121,3**	**19 977,5**	**19,3**	**5 848,0**
Cartes perdues ou volées	79,6	17 601,4	12,0	1 969,2	3,4	713,2
Cartes non parvenues	0,5	107,1	0,1	26,7	0,1	19,4
Cartes altérées ou contrefaites	1,8	280,7	108,9	17 933,9	15,4	4 994,5
Numéro de carte usurpé	0,0	0,0	0,1	23,7	0,1	49,6
Autres	0,0	0,0	0,2	24,0	0,3	71,3
Total	**1 105,6**	**105 590,8**	**558,5**	**82 856,5**	**363,3**	**65 115,5**

Source : Observatoire de la sécurité des cartes de paiement

[1] Les émetteurs étrangers ne peuvent distinguer les paiements de proximité et sur automate des paiements à distance. Ainsi, seule la distinction paiement / retrait est pertinente. Les chiffres présentés ici pour la fraude « Émetteur étranger, Acquéreur français » sont donc les chiffres correspondant à la somme de tous les paiements (c'est-à-dire la somme des paiements à distance et des paiements de proximité et sur automate).

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**15,39**	**7 408,73**	**3,37**	**1 079,43**	**3,27**	**1 673,00**
Cartes perdues ou volées	6,60	1 655,52	0,75	232,93	1,14	620,37
Cartes non parvenues	3,08	652,37	0,32	139,10	0,01	7,58
Cartes altérées ou contrefaites	0,79	412,71	2,17	674,00	1,86	929,22
Numéro de carte usurpé	0,33	281,65	0,06	15,24	0,15	59,02
Autres	4,60	4 406,48	0,07	18,17	0,12	56,81
Paiements à distance hors Internet	**0,86**	**358,55**	**3,10**	**1 146,33**	**2,74**	**1 484,06**
Cartes perdues ou volées	0,15	22,41	0,06	36,92	0,13	34,45
Cartes non parvenues	0,06	13,85	0,06	19,49	0,00	0,48
Cartes altérées ou contrefaites	0,05	1,80	0,11	32,31	0,29	194,61
Numéro de carte usurpé	0,52	299,71	2,83	1 048,14	2,27	1 243,92
Autres	0,07	20,79	0,03	9,48	0,06	10,61
Paiements à distance sur Internet	**0,30**	**186,11**	**0,78**	**194,50**	**1,23**	**421,09**
Cartes perdues ou volées	0,08	57,58	0,00	1,81	0,04	6,53
Cartes non parvenues	0,03	19,53	0,00	0,65	0,00	0,14
Cartes altérées ou contrefaites	0,01	0,12	0,01	3,26	0,07	13,52
Numéro de carte usurpé	0,17	105,00	0,76	186,88	1,09	395,00
Autres	0,01	3,88	0,01	1,91	0,04	5,89
Retraits	**3,60**	**1 004,91**	**0,00**	**1,00**	**0,00**	**2,50**
Cartes perdues ou volées	3,13	800,82	0,00	1,00	0,00	0,00
Cartes non parvenues	0,36	160,47	0,00	0,00	0,00	0,00
Cartes altérées ou contrefaites	0,00	0,16	0,00	0,00	0,00	2,50
Numéro de carte usurpé	0,00	18,02	0,00	0,00	0,00	0,00
Autres	0,10	25,44	0,00	0,00	0,00	0,00
Total	**20,14**	**8 958,31**	**7,24**	**2 421,26**	**7,24**	**3 580,64**

Source : Observatoire de la sécurité des cartes de paiement

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 4 juillet 2008
Dépôt légal 3ème trimestre 2008
ISSN 1767-6665

RAPPORT ANNUEL
2007

L'Observatoire de la sécurité des cartes de paiement est un forum chargé de promouvoir le dialogue et les échanges d'informations entre l'ensemble des acteurs intéressés, en France, par la sécurité et le bon fonctionnement des systèmes de paiement par carte. Il réunit deux parlementaires, des représentants des administrations concernées, des émetteurs de cartes et des associations de commerçants et de consommateurs.

Créé par la loi sur la sécurité quotidienne de novembre 2001, l'Observatoire exerce un suivi des mesures de sécurisation entreprises par les émetteurs et les commerçants, établit des statistiques de fraude harmonisées et assure une mission de veille technologique.

Le présent rapport constitue le rapport d'activité annuel de l'Observatoire. Conformément à l'article L.141-4 du Code monétaire et financier, il est remis au ministre chargé de l'économie et des finances et transmis au Parlement.

Ce rapport a été préparé à la

BANQUE DE FRANCE
EUROSYSTÈME

BdF - 29413 - Ateliers SIMA - 180717 - 6-08

Edition 2008
ISSN 1767-6665