2006 RAPPORT ANNUEL

DE L'OBSERVATOIRE DE LA SÉCURITÉ DES CARTES DE PAIEMENT

bservatoire
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 2006
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

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 précité, 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 une étude relative à la protection des données de cartes de paiement dans la filière de personnalisation en France (1ère partie), puis une présentation des statistiques de fraude pour 2006 (2ème partie) et une synthèse des travaux conduits en matière de veille technologique (3ème partie). Enfin, le rapport comprend une étude portant sur la perception par les porteurs de la sécurité des cartes de paiement, qui a été réalisée sur la base d'un sondage conduit par l'institut CSA (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 cartes 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 LA PROTECTION DES DONNEES DE CARTES DE PAIEMENT DANS LA FILIERE DE PERSONNALISATION

1.1 Introduction

Dans le cadre de sa mission de suivi des politiques de sécurité mises en œuvre par les émetteurs et les accepteurs, l'Observatoire avait conduit en 2005 une étude sur la protection des données de cartes dans la filière acquisition. En 2006, il a complété cette étude par une analyse des mesures de sécurité prises par les émetteurs et leurs sous-traitants industriels lors des opérations dites de « personnalisation » des cartes.

La personnalisation consiste à enregistrer sur des cartes produites par les industriels et encore à ce stade inutilisables, des informations qui vont permettre leur utilisation par les porteurs. Il s'agit à la fois des données d'authentification propres à l'émetteur et des informations d'identification et d'authentification du titulaire (nom, numéro de carte, PIN, date de validité, etc.). La réalisation des différentes opérations nécessaires à la personnalisation requiert donc d'importantes précautions pour que les données qui sont inscrites sur la carte, notamment les données personnelles du porteur, ne puissent être détournées ou modifiées à des fins frauduleuses.

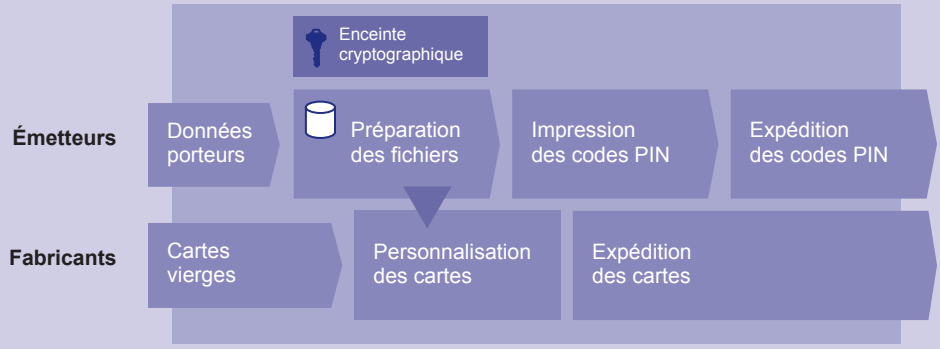
Afin d'être enregistrées sur les cartes, ces informations sensibles sont reçues et stockées sur différents matériels (réseaux informatiques, ordinateurs, machines-outils, supports divers). L'Observatoire s'est donc attaché à identifier non seulement les données devant être protégées, mais également ces différents matériels servant à les enregistrer sur les cartes, afin d'apprécier de façon globale la pertinence et l'efficacité des mesures de sécurité mises en œuvre tout au long du processus de personnalisation.

Pour ce faire, l'Observatoire a recueilli les informations utiles, sur la base d'un questionnaire adressé aux représentants des émetteurs[3] ainsi que des personnalisateurs de cartes, via leur association, l'AFPC (l'Association des Fabricants et Personnalisateurs de Cartes).

L'étude a uniquement concerné les activités comprises dans le périmètre des ateliers de personnalisation de cartes, à l'exclusion des opérations réalisées par les émetteurs (gestion des porteurs) et au sein des usines de fabrication des supports pour cartes (voir Encadré 1).

[3] Banque Accord, American Express, BMS, Cofinoga, Cedicam, Cetelem, CNCE, Diners, Finaref, Groupement des Cartes Bancaires « CB », La Banque Postale, Natixis

Encadré 1 – Périmètre de l'étude



Périmètre étudié : **Ateliers de personnalisation**

1 | 2 Descriptif de la personnalisation

Les émetteurs soit font réaliser par leurs propres services les opérations de personnalisation, soit recourent à des prestataires spécialisés, désignés sous l'expression « ateliers de personnalisation » ou « personnalisateurs ». Ceux-ci sont tenus vis-à-vis des émetteurs par des obligations strictes concernant la sécurité des opérations. De manière générale, les mesures de sécurité couvrent l'ensemble des informations et matériels exposés au risque de détournement ou d'altération à des fins frauduleuses. La forte sensibilité des opérations de personnalisation requiert en effet un encadrement et un contrôle très stricts par les émetteurs et leurs prestataires.

Les ateliers de personnalisation

Les ateliers de personnalisation français opèrent généralement pour différents secteurs utilisateurs de cartes à puce ou à piste (téléphonie, commerce, banque, etc.) et pour des clients de différents pays. Le marché des cartes de paiement françaises qui est pris en charge par les prestataires représente environ 60 millions de cartes, dont 85 % comportent une puce. La moitié de ces 60 millions de cartes sont utilisées avec un code confidentiel, ce qui requiert généralement l'envoi d'un courrier spécifique (dit « *mailer* ») au porteur pour le lui transmettre.

Ces ateliers assurent l'activité de personnalisation des cartes de paiement de type « interbancaire » et de type « privatif ». Ils appartiennent soit à des groupes bancaires, soit à des groupes industriels de monétique, soit à des prestataires indépendants spécialisés.

La complexité des activités exercées par les personnalisateurs est élevée en raison de la variété des quantités de cartes à traiter (d'une à quelques centaines de milliers de cartes), des procédés industriels à mettre en œuvre et des exigences de sécurité requises par la sensibilité des opérations. Elle implique en conséquence une organisation des opérations de grande qualité.

Encadré 2 – Les différentes phases de la personnalisation

La personnalisation se déroule en plusieurs phases :

1. **Réception, contrôle et stockage des cartes vierges**

   Les cartes sont le plus souvent fabriquées dans des usines séparées des ateliers de personnalisation. Lorsqu'elle est reçue par l'atelier, la carte est dite « vierge » : elle comporte seulement le visuel de l'émetteur et, si elle en dispose, la puce dédiée aux applications de paiement.

2. **Réception des données des porteurs en provenance des émetteurs et préparation du fichier de personnalisation**

   A la réception des données relatives aux porteurs, le prestataire réalise différents traitements informatiques préparatoires à la personnalisation. Des clés secrètes propres à l'émetteur et destinées à authentifier la carte sont calculées dans des enceintes cryptographiques sécurisées (« boîtes noires ») à partir des clés « maîtres » de l'émetteur. L'ensemble des données propres aux porteurs et à l'émetteur est constitué sous forme d'un fichier informatique. Un fichier est préparé pour chaque visuel de carte, afin de simplifier la gestion des lots de cartes vierges par les opérateurs. L'enregistrement des données sur la carte peut alors démarrer.

3. **L'individualisation de la carte par la machine de personnalisation**

   En fonction du type de carte, la personnalisation peut comporter différentes opérations : l'enregistrement des données dans la puce, et/ou sur la piste magnétique, l'embossage du nom du porteur et du numéro de carte et la gravure du code spécifique pour la vente à distance (« CVx2 »). La plupart des machines, pilotées par informatique, permettent de réaliser ces différentes opérations en une seule fois.

4. **Façonnage et mise sous pli**

   Cette ultime étape est en général réalisée manuellement, le personnel contrôlant la conformité visuelle de la carte et préparant sa mise sous pli, le cas échéant en y joignant des documents d'accompagnement. La mise sous pli peut également être automatisée. Les cartes sont alors prêtes à être expédiées, ce qui peut se faire soit directement et individuellement aux porteurs, soit d'abord de façon groupée en agence ou aux centres de répartition des émetteurs, charge à ceux-ci de faire la mise à disposition des porteurs.

5. **Envoi du Code confidentiel (PIN)**

   Dans le cas de cartes de paiement fonctionnant avec un code confidentiel, l'atelier (parfois l'émetteur) réalise le calcul, l'impression dans un courrier sécurisé (*mailer*) et l'envoi du code PIN au porteur.

Les données traitées et produites dans le processus de personnalisation

Les données transmises par l'émetteur comportent les éléments d'identification du porteur (nom, adresse d'envoi) et de la carte (numéro de carte, type de carte), ainsi que les différentes modalités d'usage de cette carte (retrait et/ou paiement, autorisation systématique, plafonds de paiement et de retrait, etc.). Dans certains cas, l'émetteur peut aussi choisir lui-même le code confidentiel à attribuer à une carte, mais celui-ci est généralement généré par le personnalisateur.

Ces différentes données sont également associées à des informations de gestion administrative (mode de distribution de la carte, adresse, conditionnement souhaité, etc.).

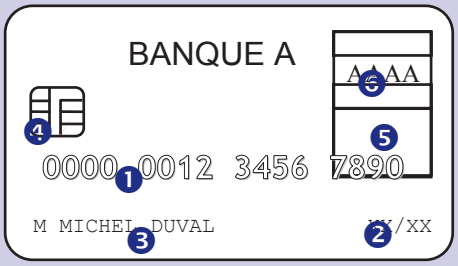
Le personnalisateur complète les données fournies par l'émetteur en y associant :

– des données secrètes (code confidentiel, clés et cryptogrammes) calculées avec, d'une part, les données transmises par les émetteurs pour chaque lot à produire et, d'autre part, des clés secrètes propres à chacun de ceux-ci transmises préalablement. Pour assurer leur

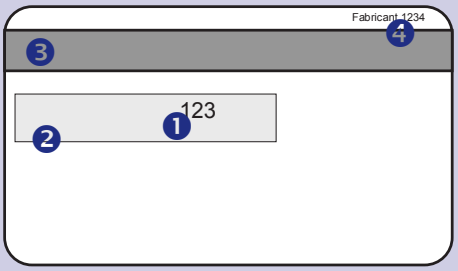
protection contre toute tentative d'intrusion ou de copie dans les locaux du personnalisateur, les clés secrètes de l'émetteur sont stockées dans des enceintes cryptographiques (« boîtes noires ») ;

– des données de gestion administrative de la production (numéro de lot de cartes vierges, éléments de traçabilité, etc.).

Encadré 3 – Les éléments d'une carte de type « interbancaire »



1. Numéro de la carte. Les caractères sont « embossés», c'est-à-dire imprimés en relief
2. Date d'expiration
3. Nom du porteur
4. Microprocesseur ou micromodule
5. Hologramme (emplacement variable)
6. Marque du réseau (emplacement variable)



1. Code CVx2 utilisé pour la vente à distance. Il est calculé et gravé lors de la phase de personnalisation
2. Panneau de signature comportant des impressions propres à chaque réseau de carte
3. La bande magnétique est composée de 3 pistes ISO (1, 2, et 3), qui sont encodées lors de la personnalisation
4. Référence de l'industriel ayant fabriqué le corps de carte en plastique et inséré la puce

1|3 La sécurité de la personnalisation

Les informations et les produits intervenant dans les différentes étapes de la personnalisation constituent des éléments sensibles qui, s'ils étaient détournés ou copiés, pourraient être utilisés pour réaliser des paiements frauduleux.

Selon les spécialistes interrogés, les principales mesures de sécurité à mettre en œuvre doivent viser à protéger les données utilisées pour la personnalisation des cartes contre le détournement, et ce, pendant toutes les phases de la personnalisation : stockage, production et expédition. Ces spécialistes considèrent également qu'il est nécessaire de se prémunir contre le vol de cartes vierges ou personnalisées, ainsi que des mailers associés, dans les processus de production et d'expédition.

Les émetteurs requièrent ainsi des personnalisateurs l'application de politiques de sécurité strictes portant sur les domaines suivants.

Le choix et l'agrément des ateliers de personnalisation

L'activité des ateliers de personnalisation est soumise à des exigences de sécurité très fortes de la part des réseaux de cartes et des émetteurs. Le Groupement des Cartes Bancaires « CB », de même que Visa et Mastercard, imposent à ces ateliers des cahiers des charges très stricts servant de fondement à la délivrance de leur agrément. Ces cahiers des charges comportent un ensemble d'exigences en termes de sécurité (physique et logique) et d'organisation dont le respect est audité régulièrement par des experts indépendants, mandatés par les réseaux de cartes et les établissements de crédit. Les émetteurs de cartes de type « privatif » choisissent le plus souvent des ateliers déjà agréés par le Groupement des Cartes Bancaires « CB », Visa ou Mastercard, lorsqu'ils ne personnalisent pas eux-mêmes leurs cartes.

Les établissements de crédit ont également l'obligation de faire rapport annuellement aux autorités de tutelle sur la maîtrise, par eux-mêmes ainsi que par leurs prestataires, des risques portant sur leurs activités essentielles.

Les ateliers de personnalisation

Un ensemble de dispositions de sécurité, visant à protéger les biens sensibles lors de leur manipulation, est imposé aux ateliers de personnalisation. La sécurité physique des ateliers s'appuie sur un contrôle des accès physiques (sas unipersonnels, etc.), la surveillance permanente et généralisée des locaux (vidéosurveillance, gardiennage) et le stockage des cartes dans des coffres. L'accès logique aux systèmes d'information doit être contrôlé et réservé au seul personnel habilité. Enfin, les enceintes cryptographiques confiées aux prestataires par les émetteurs, et contenant leurs clés cryptographiques racines sont exploitées dans des locaux bénéficiant d'une sécurité renforcée.

Ces mesures de sécurité physique et logique apparaissent associées à un ensemble de « bonnes pratiques » organisationnelles. Ainsi, un responsable sécurité, indépendant de la production, est généralement chargé de vérifier l'application des procédures. De même, les différentes fonctions dans les ateliers sont séparées physiquement : l'impression des codes confidentiels est assurée dans des ateliers différents et à l'aide de personnel différent de ceux qui personnalisent les cartes. Les différentes catégories de personnel n'ont accès qu'aux locaux et aux informations strictement nécessaires à leur activité. Un double comptage des éléments utilisés ou produits est organisé à toutes les étapes de la personnalisation. Dans la plupart des ateliers, un suivi de production informatisé permet à tout moment de consolider et d'auditer tous les événements concernant un lot de cartes. Ces contrôles peuvent aussi viser à s'assurer de la bonne synchronisation des opérations de personnalisation (association des données du porteur avec la carte de son émetteur).

Les données et les fichiers

La phase de personnalisation nécessite l'utilisation de données et de fichiers très sensibles. Pour en assurer la protection, les ateliers mettent en œuvre les pratiques suivantes :

– utilisation de plateformes informatiques dédiées pour le transfert sécurisé des fichiers entre l'émetteur et le personnalisateur ;

– chiffrement et scellement des fichiers de données durant leur transport ;

– délivrance d'un accusé de réception logique, permettant de valider les envois et les réceptions ;

– chiffrement des fichiers de données en phase d'exploitation dans l'atelier et lors de l'archivage des éventuels fichiers d'historique ;

– enregistrement et audit par le service sécurité de tous les événements, en particulier l'accès aux fichiers sensibles.

Les enceintes cryptographiques et les clés

Les enceintes cryptographiques comportant les clés des émetteurs nécessaires au calcul des données de personnalisation sont soumises à une surveillance particulière, notamment durant les phases de maintenance. Le chargement des clés cryptographiques dans les boîtes noires fait ainsi l'objet de procédures très strictes sous le contrôle de personnes indépendantes de l'atelier. Ces « boîtes noires » disposent de plus de mécanismes d'autoprotection contre les attaques logiques et physiques.

Les cartes

Les exigences de sécurité prévoient le transport sous haute protection des cartes vierges entre les sites industriels. Dès leur arrivée, elles sont comptées puis stockées dans des coffres. L'accès à ces coffres est strictement réservé à du personnel habilité. Les quantités de cartes à personnaliser sont transmises au personnel de l'atelier au fur et à mesure des besoins. Les rebuts et les consommables pouvant comporter des données de cartes (ruban encreur, etc.) sont comptés et détruits. Chaque lot de cartes fait l'objet d'une réconciliation complète à chaque étape de la personnalisation, permettant de tracer toutes les cartes produites ou mises au rebut. Les cartes rebutées sont systématiquement détruites.

Les expéditions des cartes personnalisées

Les cartes personnalisées sont soit directement expédiées aux porteurs par courrier, souvent en recommandé, soit expédiées par lot dans les centres de répartition des émetteurs. Dans ce cadre, le traitement des courriers non parvenus aux destinataires (NPAI) fait normalement l'objet de traitements particuliers visant à limiter les détournements possibles.

Le courrier transmettant le code confidentiel ne permet pas de lire celui-ci par transparence et ne peut être ouvert sans laisser des traces irréversibles. Ce courrier est envoyé de façon à éviter toute possibilité qu'une personne malveillante ne soit en possession à la fois de la carte et du code.

En complément, plusieurs émetteurs mettent le numéro de carte en opposition dès sa création, puis activent la carte à la première utilisation par le porteur (par exemple dans un DAB), ou par une procédure préalable d'activation à distance (par exemple après appel téléphonique).

1|4 Conclusion

L'activité de personnalisation des cartes est un processus dont la sécurité est cruciale. Il s'agit en effet de l'étape de production lors de laquelle se concentrent à la fois les cartes elles-mêmes et des données sensibles, telles que les informations identifiant et authentifiant la carte et le porteur.

Le risque de vol, de copie ou de détournement de ces différents éléments, présents en quantités industrielles à ce stade de la fabrication des cartes, requiert des exigences de sécurité élevées, à la fois en matière de protection physique et logique.

Les réponses à l'enquête conduite par l'Observatoire montrent que les émetteurs et les systèmes de cartes imposent aux prestataires habituellement en charge de cette activité de telles exigences ; ils les agréent sur cette base pour créer leurs cartes et contrôlent très régulièrement la bonne application de ces mesures de sécurité. Le professionnalisme réputé des personnalisateurs français témoigne des précautions prises par l'ensemble de ces prestataires. Ceux-ci innovent également en permanence pour compléter si besoin est par des « bonnes pratiques » les exigences de sécurité des émetteurs.

Les émetteurs et représentants des personnalisateurs consultés n'ont pas reporté d'incident ayant affecté la sécurité de leurs opérations de personnalisation.

2 | STATISTIQUES DE FRAUDE POUR 2006

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[4]. Une synthèse des statistiques pour 2006 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 4 – 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 ». L'échantillon s'est, en 2006, enrichi d'un nouvel émetteur, Franfinance.

Les données fournies à l'Observatoire par les émetteurs portent ainsi sur :

– 346,4 milliards d'euros de transactions réalisées en France et à l'étranger à l'aide de 53,6 millions de cartes de type « interbancaire » émises en France (dont un peu moins de 1 million de porte-monnaie électroniques),
– 26,1 milliards d'euros de transactions réalisées (principalement en France) avec 25 millions de cartes de type « privatif »[5],
– et 22,58 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, par l'intermédiaire de BMS (Billettique Monétique Services).

Commerçants

Les données collectées concernent six accepteurs de cartes de paiement, à savoir Carrefour, Décathlon, le groupe Casino, France Loisirs, Monoprix et la SNCF. Cette collecte s'est également enrichie pour 2006 de statistiques recueillies par la Fédération du e-commerce et de la vente à distance (FEVAD) auprès d'un échantillon représentatif de 29 entreprises de vente à distance.

---

4 Cf. rapport 2003, partie 3.

5 La baisse du nombre de cartes de ce type entre 2005 et 2006 (27,2 millions de cartes de type « privatif » étaient en circulation fin 2005) s'explique par la mise en application de la loi 2005-67 du 28 janvier 2005 *tendant à conforter la confiance et la protection du consommateur*, dite « loi Chatel », qui impose la résiliation de plein droit des contrats de crédit renouvelables non utilisés pendant une période de trois années consécutives. Certains émetteurs de cartes de type « privatif » ont été amenés à invalider les cartes associées aux contrats visés par la nouvelle loi.

2|1 Vue d'ensemble

Le montant total des paiements et des retraits frauduleux enregistrés dans les systèmes français est estimé en 2006 à 252,6 millions d'euros, contre 235,9 millions d'euros en 2005. La fraude, orientée à la baisse entre 2003 et 2005 (voir Tableau 1), est donc en légère augmentation (+ 6,6 %). Le montant moyen d'une transaction frauduleuse est également en légère augmentation, à 117 euros contre 111 euros en 2005.

Toutefois, dans un contexte de croissance soutenue du volume et de la valeur des transactions par carte (cf. annexe C), cette augmentation du montant de la fraude est sans impact sur le taux global de fraude, qui reste stable. Celui-ci s'établit en 2006 comme en 2005 à 0,064 %, contre 0,070 % en 2004.

Le montant de la fraude émetteur – c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France – s'élève en 2006 à 186,1 millions d'euros, en augmentation par rapport à 2005 (161,9 millions d'euros). Rapporté au montant des transactions, le taux de fraude émetteur s'établit en 2005 à 0,050 %, un taux légèrement supérieur à celui de 2005 (0,046 %), mais équivalent à celui de 2004 (0,049 %).

Le montant 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 – s'élève en 2006 à 176,2 millions d'euros, contre 171,8 millions d'euros en 2005. Rapporté au montant des transactions, le taux de fraude acquéreur s'établit cependant en légère baisse, à 0,047 % (contre 0,048 % en 2005).

L'annexe C du présent rapport regroupe des tableaux détaillés des volumes et valeurs de transactions et des volumes et valeurs de fraude, par types de cartes, zones géographiques, types de transactions et origines de fraude.

2|2 Répartition de la fraude par type de carte

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

	2002	2003	2004	2005	2006
Cartes de type « interbancaire »	232,1 (0,082 %)	259,2 (0,086 %)	224,1 (0,069 %)	218,8 (0,064 %)	**237,0 (0,065 %)**
Cartes de type « privatif »	13,1 (0,078 %)	14,4 (0,082 %)	17,5 (0,082 %)	17,1 (0,067 %)	**15,6 (0,052 %)**
Total	245,2 (0,082 %)	273,6 (0,086 %)	241,6 (0,070 %)	235,9 (0,064 %)	**252,6 (0,064 %)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 1 – **Montants et taux de fraude**

Pour les cartes de type « interbancaire », le montant total de la fraude est en légère augmentation en 2006 à 237 millions d'euros (contre 218,8 millions d'euros en 2005). Rapporté au montant des transactions, le taux de fraude n'évolue pas de manière significative, puisqu'il s'établit à 0,065 % en 2006 contre 0,064 % en 2005.

Pour ce type de carte, les taux de fraude émetteur et acquéreur sont respectivement de 0,050 % et de 0,047 % (contre 0,046 % et 0,048 % en 2005). La valeur moyenne d'une transaction frauduleuse est de 112 euros contre 110 euros en 2005.

Pour les cartes de type « privatif », le montant total de la fraude s'élève en 2006 à 15,6 millions d'euros, soit un taux de fraude de 0,052 %, en baisse sensible par rapport à 2005 (0,067 %). Les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,045 % et à 0,046 % (contre 0,049 % et à 0,061 % en 2005). La valeur moyenne d'une transaction frauduleuse s'établit à 430 euros en 2006[6].

2|3 Répartition de la fraude par zone géographique

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

	2002	2003	2004	2005	2006
Transactions nationales	**89,5 (0,033 %)**	**88,3 (0,031 %)**	**103,9 (0,033 %)**	**97,8 (0,029 %)**	**109,6 (0,031 %)**
Transactions internationales	**155,7 (0,531 %)**	**185,3 (0,648 %)**	**137,7 (0,417 %)**	**138,1 (0,408 %)**	**143,0 (0,362 %)**
Dont émetteur français et acquéreur étranger	51,9 (0,558 %)	79,3 (0,690 %)	55,2 (0,463 %)	64,1 (0,458 %)	76,4 (0,453 %)
Dont émetteur étranger et acquéreur français	103,8 (0,519 %)	106 (0,620 %)	82,5 (0,391 %)	74,1 (0,373 %)	66,5 (0,295 %)
Total	**245,2 (0,082 %)**	**273,7 (0,086 %)**	**241,6 (0,070 %)**	**235,9 (0,064 %)**	**252,6 (0,064 %)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 2 – **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 : 60 % de la fraude porte 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 (+ 6,29 %), le taux de fraude de celles-ci n'augmente que très légèrement en passant à 0,031 % en 2006 (0,029 % en 2005) et demeure à un niveau très faible.

La fraude sur les transactions internationales augmente pour sa part en 2006 en montant mais diminue en taux. Cette tendance générale recouvre néanmoins une double évolution :

– d'une part, la fraude liée aux transactions des porteurs étrangers en France est en baisse, tant en montant (66,5 millions d'euros en 2006 contre 74,1 millions d'euros en 2005) qu'en taux (0,295 % en 2006 contre 0,373 % en 2005). 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 ;

– d'autre part, la fraude liée aux transactions des porteurs français à l'étranger augmente en montant (76,4 millions d'euros en 2006 contre 64,1 millions d'euros en 2005), mais diminue légèrement en taux (0,453 % en 2006 contre 0,458 % en 2005).

[6] L'augmentation significative de cet indicateur par rapport à celui publié pour les années précédentes (188 euros en 2005), s'explique par l'amélioration de l'outil statistique de plusieurs émetteurs de cartes de type « privatif ».

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.

En ce qui concerne les transactions nationales (voir Tableau 3), on observe que :

– 70 % des paiements frauduleux recensés par l'Observatoire pour 2006 ont été réalisés dans le cadre de paiements de proximité et sur automate, et de retraits. Cette proportion est tendanciellement en baisse : elle était de 76 % en 2005 et de 83 % en 2004 ;

– le taux de fraude sur les paiements de proximité et sur automate est très inférieur à celui sur les paiements à distance. En 2006, ce taux s'est établi à 0,024 %, contre 0,199 % pour les paiements à distance. En outre, ce taux est tendanciellement en baisse : il se montait à 0,025 % en 2005 et 0,029 % en 2004 ;

– la fraude sur les paiements à distance s'élève en 2006 à 33,2 millions d'euros, en forte augmentation par rapport à 2005 (23,6 millions d'euros). Toutefois, dans un contexte de croissance très dynamique du volume et de la valeur de ces paiements (+ 38,9 % entre 2005 et 2006), cela se traduit par une augmentation très modeste du taux de fraude sur ce type de paiement (0,199 % en 2006 contre 0,196 % en 2005) ;

– la fraude sur les retraits, après avoir diminué entre 2004 et 2005, connaît un léger rebond en 2006 (17,4 millions d'euros en 2006 contre 15,0 millions d'euros en 2005).

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

** Pour tous types de cartes* *Source : Observatoire de la sécurité des cartes de paiement*

▲ Tableau 3 – **Répartition de la fraude nationale par types de transaction**

Les efforts engagés par l'Observatoire pour affiner son système d'information statistique lui permettent de disposer pour 2006 d'indicateurs sur les taux de fraude pour les différents modes de paiement à distance réalisés avec tout type de carte. On observe ainsi que le taux de fraude sur les paiements à distance par Internet est légèrement plus élevé que celui observé sur les paiements à distance par d'autres canaux (courrier, téléphone). Par ailleurs, selon les estimations de la FEVAD[7] qui confirment ce constat, le taux de fraude semble varier selon les

[7] Selon une étude réalisée auprès d'un échantillon d'entreprises et de sites de commerce électronique adhérents à la FEVAD et représentatifs des principaux secteurs du commerce électronique et de la vente à distance.

secteurs d'activité et serait plus important dans le cadre de la vente de services que dans celle de produits.

Toutefois, le niveau des taux de fraude des paiements à distance mesuré par la FEVAD sur son échantillon est inférieur à celui calculé par l'Observatoire[8]. Cet écart suggère que le taux de fraude est moins élevé chez les spécialistes du commerce électronique, ce qui pourrait s'expliquer par la mise en œuvre par ces derniers de mesures de sécurité spécifiques à ce type de transactions.

Dans ce contexte, l'Observatoire souhaite rappeler 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[9].

En ce qui concerne les transactions internationales (voir Tableau 4), l'Observatoire ne dispose d'une décomposition fine de la fraude par type de transactions que pour la seule année 2006, et 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 (0,288 % contre 0,840 %) ;

– 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 (0,898 % contre 0,684 %).

	Montant de la fraude en millions d'euros **(Taux de fraude)**
Émetteur français – Acquéreur étranger	**2006**
Paiements	**54,0 (0,421 %)**
- dont paiements de proximité et sur automate	28,1 (0,288 %)
- dont paiements à distance	26,0 (0,840 %)
- dont par courrier / téléphone	5,7 (0,684 %)
- dont sur Internet	20,3 (0,898 %)
Retraits	**22,4 (0,555 %)**
Total	**76,4 (0,453 %)**
Émetteur étranger – Acquéreur français	**2006**
Paiements	**61,5 (0,344 %)**
Retraits	**5,0 (0,107 %)**
Total	**66,5 (0,295 %)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 4 – **Répartition de la fraude internationale par types de transaction**

8 La FEVAD estime la fraude sur les transactions nationales à distance pour les cartes de type « interbancaire » à 0,130 %.

9 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.

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 ;

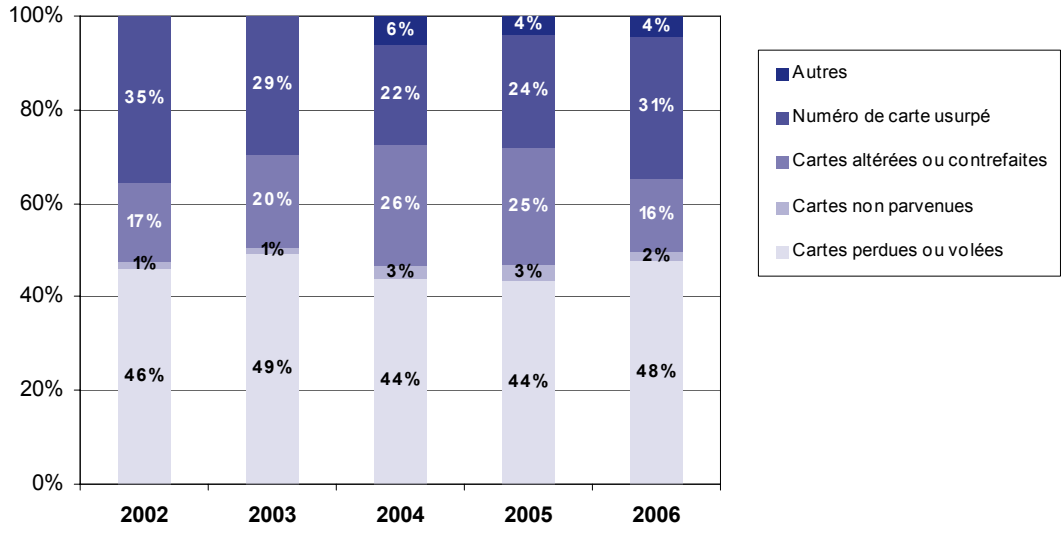
– carte non parvenue : la carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;

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

En augmentation en 2006, l'origine de fraude de loin la plus importante reste celle liée aux pertes et vols de cartes, avec près de 48 % des paiements nationaux frauduleux. La contrefaçon de cartes, encore à l'origine de 16 % des paiements nationaux frauduleux, diminue fortement en 2006. En revanche, la fraude par usurpation de numéro de carte, utilisée pour les paiements à distance, qui est à l'origine d'un peu plus de 31 % des paiements frauduleux, a progressé en 2005 et 2006, après trois années de baisse. Enfin, on observe une stabilisation 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 %).

2006	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	52,5	47,9 %	50,0	49,8 %	2,5	27,5 %
Carte non parvenue	1,8	1,6 %	0,7	0,7 %	1,1	11,7 %
Carte altérée ou contrefaite	17,4	15,9 %	17,1	17,0 %	0,3	3,1 %
Numéro usurpé	33,5	30,5 %	32,7	32,5 %	0,8	8,3 %
Autres	4,4	4,1 %	-	-	4,4	49,4 %
Total	**109,6**	**100 %**	**100,5**	**100 %**	**9,1**	**100 %**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 6 – **Répartition de la fraude nationale selon son origine et par type de carte**

Encadré 5 – Faits marquants de l'année vus par les forces de police et de gendarmerie

L'année 2006 a été marquée par une augmentation générale des cas recensés par les forces de police et de gendarmerie en matière de fraude relative aux cartes de paiement.

En matière de contrefaçon, 53 755 faits ont été relevés, 3 496 individus ont été mis en cause, motivant 1 642 mesures de garde à vue.

Les attaques de distributeurs de billets ont fortement augmenté : 515 faits de ce type ont été recensés en 2006, contre 200 en 2005 et 80 en 2004. De nombreuses enquêtes ont été diligentées en 2006 sur l'ensemble du territoire national pour de telles attaques. Parmi celles-ci on peut distinguer :

- l'interpellation de trois responsables d'un réseau de piratage de distributeurs automatiques de billets. Cette affaire a permis de mettre fin aux activités de trois malfaiteurs, tous connus du grand banditisme, spécialisés dans ce type d'activité, en liaison avec des individus d'origine roumaine basés aux Pays-Bas ;
- l'enquête relative au piratage d'une vingtaine de terminaux de paiement électroniques de chaînes de restaurant, ayant occasionné un préjudice de plus de 2 millions d'euros et la compromission de 3 000 cartes de paiement. Cinq individus ont été interpellés en Espagne dans le cadre de cette affaire, ainsi que trois autres en France.

L'année 2006 a aussi vu un renforcement de la coopération des autorités répressives nationales avec leurs homologues des pays de l'Est de l'Europe, du fait du caractère transfrontalier de ce type de délinquance et de l'origine des groupes criminels mis en cause. Cette coopération sera amenée à être pérennisée dans les années à venir.

3 | VEILLE TECHNOLOGIQUE

Dans le cadre de sa mission de veille technologique, l'Observatoire a mené, en 2006, deux études concernant, d'une part, l'impact de l'utilisation de réseaux ouverts dans l'environnement des cartes de paiement et, d'autre part, les automates de paiement et de retrait. Pour chacun de ces deux thèmes, l'Observatoire a analysé les enjeux en matière de sécurité et formulé un ensemble de recommandations. Par ailleurs, l'Observatoire a mis à jour les informations rassemblées les années précédentes sur la migration des différents pays européens au standard EMV pour les cartes et les terminaux.

3|1 Utilisation de réseaux ouverts dans l'environnement des cartes de paiement

Jusqu'à récemment, les risques associés aux réseaux utilisés pour les transactions par carte de paiement restaient en grande partie maîtrisés, d'abord du fait que ces réseaux étaient administrés par l'opérateur historique, ensuite parce que les technologies employées étaient mieux connues des constructeurs d'équipements que des éventuels attaquants, enfin parce que les connexions réalisées étaient très ponctuelles, n'intervenant que lors des télécollectes et des demandes d'autorisation. L'utilisation de technologies de type X.25[10] garantissait en outre, même en cas d'interconnexion fortuite avec d'autres réseaux comme Internet, un certain cloisonnement sans même recourir à des dispositifs de filtrage[11].

L'émergence de nouvelles technologies de télécommunication, couramment désignées comme des « réseaux ouverts », est en passe de modifier profondément le niveau de menace auquel devront faire face les futurs systèmes de paiement. La généralisation d'IP (*Internet Protocol*), le protocole de communication standard sur lequel est basé Internet, et les nouvelles offres de service des opérateurs de télécommunication, conduisent inexorablement à utiliser des réseaux mutualisés, transportant de multiples flux (données, voix). Pour les systèmes de paiement par carte, l'arrivée de technologies comme l'ADSL[12] et le GPRS[13] a apporté des avantages pour le raccordement des matériels d'acceptation : être connecté en permanence et à haute vitesse, ce qui permet de disposer de fonctionnalités nouvelles (téléchargement de mises à jour plus fréquentes, demandes d'autorisation rapides, etc.), à un coût forfaitaire et raisonnable, permettant de surcroît plusieurs connexions sur une seule ligne.

L'interconnexion facilitée par cette généralisation est source de menaces qui, sans être nouvelles, prennent une autre dimension du fait de la très grande diffusion des technologies de télécommunication les plus récentes. Là où chaque équipementier monétique ou réseau

---

10 X.25 est un protocole de communication normalisé en 1976 par le CCITT et notamment utilisé en France par Transpac.

11 Élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

12 *Asymmetric Digital Subscriber Line*. Évolution de l'utilisation des lignes téléphoniques usuelles permettant, notamment, d'utiliser la ligne pour établir une connexion Internet haut débit permanente, tout en ne gênant pas son utilisation simultanée pour de la téléphonie classique.

13 Le *General Packet Radio Service* ou GPRS est une norme pour la téléphonie mobile dérivée du GSM, permettant un débit de données plus élevé. On le qualifie souvent de 2,5G. Le G est l'abréviation de génération et le 2,5 indique que c'est une technologie à mi-chemin entre le GSM (2e génération) et l'UMTS (3e génération).

développait son propre système de communication X.25, les développements sur IP se fondent pour la plupart sur des outils logiciels externes et facilement accessibles, si bien que le niveau de compétence est désormais inversé : la connaissance des protocoles de communication n'est plus réservée aux fournisseurs de terminaux de paiement. À ceci s'ajoute le fait que les réseaux sont beaucoup plus facilement accessibles, du fait notamment de la multiplication des technologies sans fil, et offrent des points d'accès très diffus et internationaux. Ils présentent des niveaux de sécurité hétérogènes, dépendant du bon vouloir de chaque opérateur, là où un opérateur unique offrait un niveau homogène. Enfin, la connexion permanente à un réseau est synonyme d'une durée d'exposition plus grande aux attaques.

Après une description des différents acteurs du système de paiement par carte concernés, sont présentées ci-après une analyse de l'impact en termes de risque de l'utilisation de réseaux ouverts, les mesures de sécurité mises en œuvre, puis les recommandations de l'Observatoire.

Les acteurs et les réseaux impliqués

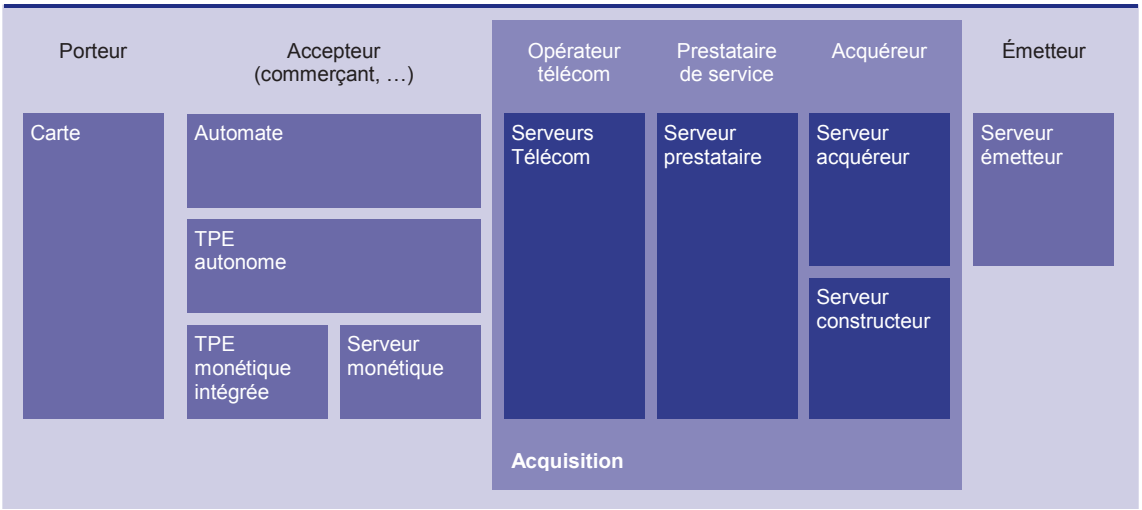
Un système de paiement par carte voit transiter différents flux :

– les flux opérationnels, liés à la gestion des transactions, avec :

  - la phase de transaction, qui correspond à l'initiation, la validation et la transmission de l'ordre de paiement. Elle fait intervenir le porteur et sa carte, l'accepteur et son système d'acceptation. La validation d'un paiement par carte nécessite la mise en œuvre de plusieurs fonctions comme l'authentification du porteur, le contrôle d'authenticité de la carte et l'autorisation de la transaction qui peut être réalisée soit hors ligne (sans interrogation de l'émetteur de la carte), soit en ligne. Les paiements réalisés sont stockés dans le terminal d'acceptation du commerçant ; ils sont ensuite transmis à l'établissement acquéreur (télécollecte) ;
  - la phase de règlement, qui permet d'achever le paiement par l'échange et le règlement de l'ordre de paiement entre les intermédiaires financiers du porteur et de l'accepteur ;

– les flux de maintenance des systèmes d'acceptation (téléparamétrage, téléchargement), qui impliquent aussi les constructeurs des équipements d'acceptation.

Encadré 6 – Acteurs et réseaux



Entre acquéreurs et émetteurs, les échanges transitent sur des réseaux bancaires très contrôlés. Dans le cas des cartes bancaires « CB », ce réseau s'appelle l'e-RSB (Réseau de

Services aux Banques). Bien que basé sur des technologies IP, il est totalement privé, sans interconnexion avec Internet.

En revanche, la liaison accepteur – acquéreur est un domaine où les offres de télécommunications se multiplient, notamment avec l'ADSL et le GPRS. Chez l'accepteur, les liaisons caisses – concentrateur et terminal – base sont également susceptibles de migrer vers des technologies plus exposées (technologies sans fil Wifi[14], Bluetooth[15], DECT[16], réseau local en IP…).

Impact de l'utilisation de réseaux ouverts

L'utilisation de réseaux ouverts peut introduire des risques accrus en termes de disponibilité, de confidentialité des données échangées, de détournement des fonctions du système, ou de piratage des équipements.

Pour maîtriser ces risques, l'utilisation de protocoles sécurisés devient indispensable pour protéger les échanges entre les différents acteurs du système de paiement. Mais l'intégrité logique des équipements est également cruciale pour éviter les intrusions.

Sécurité des échanges

Les liaisons entre les différents équipements du système de paiement par carte voient circuler des données sensibles, dont l'interception ou la manipulation doivent être prévenues. Il convient donc de protéger ces données par des mécanismes fournissant confidentialité, intégrité et authentification.

Ces services de sécurité n'étant pas intégralement gérés par le protocole d'échange monétique, ils doivent pouvoir s'appuyer sur des mécanismes fournis par les protocoles de communication associés aux nouveaux réseaux. La communication entre le système d'acceptation et le serveur d'acquisition de l'acquéreur ou de son prestataire de service doit être authentifiée et protégée en intégrité et en confidentialité par des algorithmes de chiffrement fort. Il en va de même pour les réseaux de communication entre un concentrateur du système d'acceptation et les différents points de vente ou caisses internes.

Avec l'utilisation de technologies rendant les réseaux de communication utilisés plus accessibles, le contrôle des flux autorisés sur le réseau devient également indispensable. Des mécanismes interdisant toute communication autre que celles légitimes et nécessaires au bon fonctionnement du système, s'imposent donc. Parmi ces mécanismes, on trouve principalement le filtrage, avec des équipements tels que les gardes-barrières (*firewall*) et les routeurs filtrants, qui contrôlent les échanges en un point de passage obligatoire. Une technique complémentaire est le cloisonnement, qui consiste à concevoir l'architecture du réseau sous forme de différentes zones de sécurité distinctes, les échanges entre zones étant contrôlés, limitant ainsi les possibilités d'un attaquant ayant accès à l'une des zones.

---

[14] Le Wifi est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11 (ISO/CEI 8802-11).

[15] Le Bluetooth est une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et leurs périphériques (imprimantes, scanners…).

[16] *Digital Enhanced Cordless Telephone* est une norme de téléphonie sans-fil numérique.

L'utilisation de ces techniques permet également de faire obstacle aux attaques contre la disponibilité du système par saturation des équipements. De ce fait, les seules attaques restant possibles ne pourront provenir que d'équipements identifiés, qui pourront donc facilement être désactivés.

Encadré 7 – Protocole sécurisé

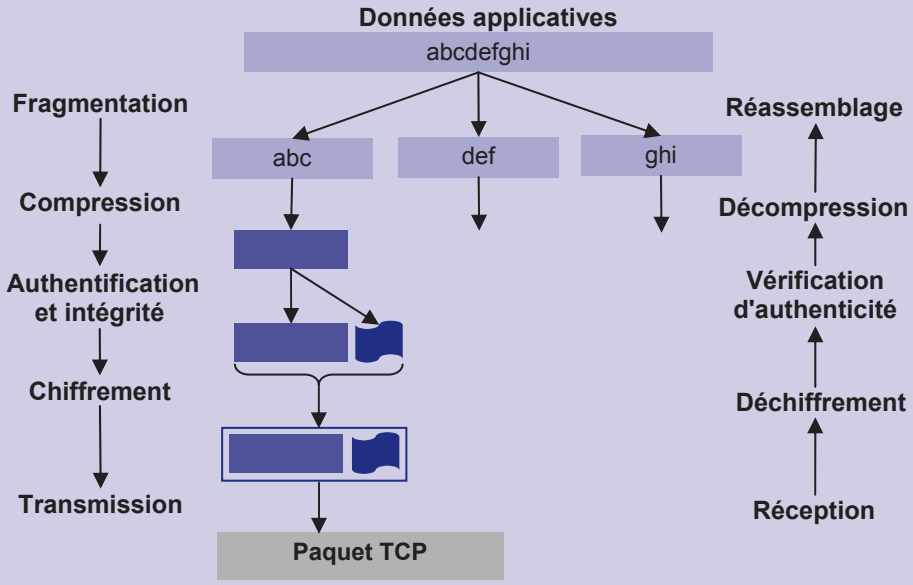
Un protocole sécurisé fournit un ensemble de services de protection des données : confidentialité, intégrité et authentification.

Confidentialité – Service de sécurité qui consiste à s'assurer que seules les personnes autorisées peuvent prendre connaissance d'un ensemble de données. Le mécanisme qui permet d'obtenir ce service est généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique.

Intégrité – Service de sécurité qui consiste à s'assurer que seules les personnes autorisées pourront modifier un ensemble de données. Dans le cadre de communications, ce service consiste à permettre la détection de l'altération des données durant le transfert.

Authentification – Service de sécurité qui consiste à s'assurer que les données reçues ont bien été émises par l'émetteur déclaré.

Voici, à titre d'exemple, la façon dont le protocole SSL (Secure Socket Layer) protège les données issues des applications, avant de les transmettre au protocole de communication TCP :



Sécurité des équipements

Si un attaquant peut viser les flux de données échangés, il peut aussi chercher à accéder frauduleusement à un des équipements composant le système de paiement. Il aura alors la possibilité, non seulement de collecter des données sensibles, mais également de tenter de détourner le système à son avantage. L'attaquant peut aussi chercher à faire obstacle à la disponibilité du système.

Ces attaques logiques, par le biais du réseau de télécommunication, seront à prendre de plus en plus en compte avec l'évolution des technologies.

Aussi, la résistance des terminaux de paiement et des serveurs à ces attaques doit-elle être recherchée, spécifiée et contrôlée, de façon soit à y résister, soit à les signaler, soit à les contrecarrer. Elle passe par un durcissement de la sécurité des systèmes d'exploitation des équipements, par un contrôle d'accès avec authentification des interlocuteurs, et par une surveillance des actions menées sur ces équipements, notamment pour ce qui concerne les opérations de maintenance. Sur les systèmes d'acceptation, cela se traduit en particulier par un renforcement des mécanismes de contrôle des opérations de téléparamétrage ou de téléchargement.

Encadré 8 – Durcissement de la sécurité des systèmes

Le durcissement de la sécurité d'un système vise à optimiser sa sécurité compte tenu de son contexte d'utilisation. En effet, les équipements sont généralement fournis par leurs fabricants munis d'un ensemble de fonctionnalités et d'une configuration par défaut qui se veulent adaptés à la majorité des utilisateurs, mais peuvent présenter des faiblesses sur le plan de la sécurité.

Le durcissement du système passe donc par la suppression ou la désactivation des composants logiciels et fonctionnalités inutilisées, qui pourraient faciliter le travail d'un attaquant ou présenter des failles de sécurité.

La configuration par défaut, généralement minimale sur le plan de la sécurité, doit également être adaptée pour n'autoriser que le strict nécessaire. Il convient aussi de modifier les éventuels mots de passe par défaut.

Pour améliorer encore la sécurité de l'équipement, il est souvent possible d'activer des mécanismes de sécurité ou des contrôles supplémentaires, ou d'ajouter des outils permettant une surveillance accrue du système.

De plus, on associe généralement au durcissement une mise à jour avec les derniers correctifs de sécurité, suivie d'une vérification par des outils de contrôle.

État des lieux des mesures de sécurité mises en œuvre

Pour tenir compte de l'impact de l'utilisation de réseaux ouverts, les acteurs des systèmes de paiement par carte doivent donc mettre en œuvre des mesures destinées à circonscrire les risques qui découlent de cette utilisation.

Ainsi, le Groupement des Cartes Bancaires « CB » a-t-il défini dès 2004 des *« Exigences sécuritaires liées aux communications avec les systèmes d'acceptation paiement »*. Ces exigences concernent la traçabilité de la maintenance, l'intégrité des systèmes monétiques, la protection des liens internes et externes à l'accepteur, la restriction des communications, le durcissement des systèmes d'exploitation et l'authentification des serveurs. Elles sont destinées à assurer la sécurité des flux et des équipements monétiques en termes d'intégrité, de confidentialité et de disponibilité dans le cadre de l'utilisation de réseaux ouverts. Elles s'imposent depuis décembre 2005 aux différents acteurs du domaine « CB » : acquéreurs, accepteurs, opérateurs de services et de télécommunications, constructeurs.

Concernant les cartes de type « privatif », l'adoption de mesures de sécurisation des transactions est le plus souvent du ressort de chaque émetteur. Les systèmes privatifs actuels, du fait de leur caractère fermé, et donc contrôlé, sont pour le moment moins concernés par l'utilisation de réseaux ouverts. Cependant, même s'ils utilisent leurs propres applicatifs et leurs propres réseaux d'échange, les systèmes privatifs partagent des équipements avec le système « CB », notamment le matériel d'acceptation des accepteurs, ces derniers disposant généralement d'un seul terminal multi-applicatifs. Les émetteurs des cartes de type « privatif » pourraient ainsi profiter de la réutilisation de mesures de sécurité développées par les constructeurs pour « CB ».

Les mesures mises en œuvre aujourd'hui par les émetteurs français résultent de leurs propres analyses et ne découlent pas d'initiatives européennes ou internationales. En effet, les seules mesures existantes ne couvrent que partiellement la question, puisque les exigences *« Payment Card Industry (PCI) Data Security Standard »* du PCI Security Standards Council, qui incluent notamment une exigence de chiffrement des échanges sur les réseaux ouverts, ne concernent que la protection des données de carte. Cependant, l'initiative européenne du groupe *Common Approval Scheme* (CAS) vise actuellement à élaborer des exigences de sécurité portant sur la protection des terminaux et de leurs échanges via tous types de réseaux, notamment ouverts. Dès lors que ces exigences seraient rendues obligatoires aux systèmes de cartes européens par le Conseil européen des paiements (European Payments Council - EPC), il existerait un niveau de protection des échanges de données équivalent à ce qui est mis en œuvre aujourd'hui en France.

Recommandations

L'Observatoire encourage vivement tous les acteurs français concernés à se conformer aux *« Exigences sécuritaires liées aux communications avec les systèmes d'acceptation paiement »* définies par le Groupement des Cartes Bancaires « CB ».

En effet, l'application de ces exigences récentes doit suivre au plus près le rythme de renouvellement des équipements, notamment du fait, à moyen terme, du remplacement du protocole X.25 par le protocole IP. Le respect d'exigences de sécurité est donc nécessaire pour répondre aux attaques rendues possibles par l'utilisation croissante de réseaux ouverts. Ce document commun offrirait le bénéfice d'uniformiser les mesures de sécurité pour l'ensemble du système et de protéger efficacement la totalité des acteurs.

Si l'impact de l'utilisation de réseaux ouverts sur les systèmes de paiement par carte est correctement pris en compte en France, on constate en revanche une absence de normes en la matière au niveau européen. Or, avec la mise en œuvre de SEPA, les réseaux vont s'étendre au-delà des frontières. Dans ce cadre, l'Observatoire considère qu'il sera indispensable d'adopter des règles communes, de niveau au moins équivalent aux exigences françaises. Il serait souhaitable que les travaux de coordination de l'EPC en matière de standards comportent également des exigences de sécurité, telles que celles formulées par le groupe *Common Approval Scheme*.

3|2 La sécurité des automates de paiement et de retrait

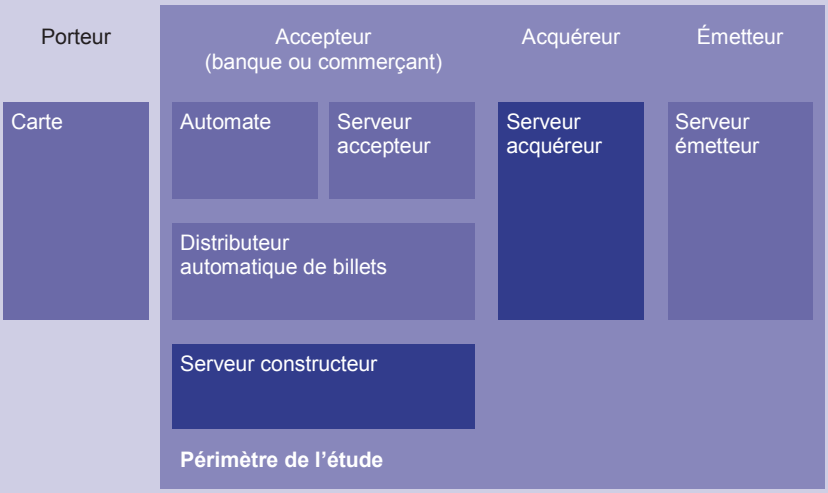
Champ de l'étude

Dans le cadre de sa mission de veille technologique, l'Observatoire a étudié en 2005 la sécurité des terminaux de paiements autonomes. Il a poursuivi en 2006 son analyse de la sécurité des systèmes d'acceptation en étudiant les dispositions spécifiques prises pour la protection des automates de paiement (ex. : distributeurs automatiques de carburants) et de retrait (distributeurs automatiques de billets - DAB).

Il existe aujourd'hui en France quelques 180 000 automates de ces deux types (cf. infra Tableau 7), et leur sécurité est un enjeu important. Ils peuvent en effet être, du fait de leur isolement, une cible privilégiée des fraudeurs pour récupérer des données de carte utiles à la réalisation de transactions frauduleuses. Ces automates acceptent généralement les cartes de type « interbancaire », ainsi que, dans la plupart des cas, certaines cartes de type « privatif ».

L'Observatoire a étudié les mesures ou dispositifs de sécurité mis en œuvre sur les automates les plus répandus, y compris pour les opérations réalisées entre ces matériels et les serveurs monétiques auxquels ils sont reliés (cf. Encadré 9, ci-dessous).

Encadré 9 – Champ de l'étude



Après un bref descriptif du mode de fonctionnement des automates, sont présentés les risques auxquels ils sont exposés et les enjeux de leur sécurité. Sont ensuite présentées les mesures de protection mises en œuvre et les perspectives d'évolution en ce domaine. En dernière partie, l'Observatoire formule, sur la base de cette analyse, des recommandations.

Mode de fonctionnement des automates

Les **automates** permettent aux porteurs de cartes un usage de celles-ci 7 jours sur 7 et 24h sur 24 et sont, si l'on excepte les publiphones, de plus en plus largement déployés en France. En plus des cartes de type « interbancaire » qui fonctionnent en mode puce, ils acceptent fréquemment des cartes de type « privatif » ainsi que des cartes bancaires étrangères (sur la base de la lecture de la piste magnétique, s'il ne s'agit pas de cartes EMV).

Les **distributeurs automatiques de billets** (DAB) acceptent les cartes de type « interbancaire » et sont le plus généralement sous la responsabilité des banques. À ce titre, le Groupement des Cartes Bancaires « CB » définit les exigences de sécurité qui s'y appliquent. Pour ces cartes de type « interbancaire » EMV, les transactions mettent en jeu la puce de la carte et non sa piste magnétique. En France, à mi 2007, la totalité de ces automates acceptent les cartes à puce EMV. Ces cartes conservent toutefois une piste, notamment pour assurer leur interopérabilité à l'étranger. Cette piste magnétique des cartes EMV reste souvent utilisée pour l'ouverture des sas de protection des DAB qui ne sont pas en accès direct sur la voie publique. Pour toutes les cartes utilisées, le DAB effectue une demande d'autorisation auprès de l'émetteur, en transmettant, de la manière la plus sécurisée possible, les données lues sur la piste et le code confidentiel. À l'étranger, dans les pays n'ayant pas migré au standard EMV, les DAB traitent les cartes EMV comme des cartes à piste.

Les **automates de paiement**, qui sont installés par les commerçants pour répondre à des besoins de distribution automatique très ciblés (carburant, DVD, titres de transport, boissons…), acceptent les cartes de type « interbancaire » et de nombreuses cartes de type « privatif ». La

configuration de ces automates est très hétérogène, selon le type de produits ou de services distribués, l'ancienneté de l'automate ou les caractéristiques de certaines transactions (péages par exemple). Quand l'équipement est conforme au référentiel du Groupement des Cartes Bancaires « CB », la transaction est réalisée en mode EMV (puce et contrôle local du code confidentiel), avec éventuellement une demande d'autorisation. Lorsque l'automate continue à ne traiter que les pistes magnétiques, le contrôle du code confidentiel, qui est transmis chiffré au serveur de l'acquéreur, est le plus souvent réalisé en ligne avec la demande d'autorisation.

Les enjeux

Le nombre des automates de paiement et de retrait est en constante augmentation en France. A l'exception des publiphones, pour lesquels le nombre de ceux acceptant les paiements par carte a régressé ces dernières années en raison principalement du recul de l'usage de ces matériels au profit des téléphones portables, tous les secteurs pour lesquels des automates permettent l'usage de cartes de paiement sont en nette augmentation. Au total, les automates de paiement représentent 12 % du nombre de terminaux de paiement installés en France.

	Nombre d'automates **en 2000**	Nombre d'automates **en 2006**	**Écart** en %
Distributeur Automatique de Billets (DAB)	33 000	48 000	+45 %
Distributeur Automatique de Carburant (DAC)	10 000	18 000	+80 %
Distributeur de titres de transport	4 000	8 000	+100 %
Parking	3 000	4 000	+33 %
Biens et services (épicerie, photos, …)	4 000	6 000	+50 %
Distributeurs de DVD, forfaits ski, chambres d'hôtel, …	7 000	8 000	+14 %
Sous-Total (hors publiphones)	**61 000**	**92 000**	**+51 %**
Publiphones	220 000	90 000	-59 %
Total	**281 000**	**182 000**	**-35 %**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 7 – **Évolution du parc d'automates**

Évolution des risques

Selon la communauté bancaire, le nombre de cas de compromission d'automates dans le but de récupérer des données de cartes, aurait doublé entre 2005 et 2006 (500 automates, dont 450 DAB, soit 0,3 % du parc installé). Les forces de police sont intervenues à plusieurs reprises pour interpeller des fraudeurs et saisir leur matériel. Elles soulignent l'accroissement constant de la technicité de ces dispositifs frauduleux.

L'Observatoire ne dispose pas de données permettant de mesurer l'ampleur des transactions réalisées par cartes dont les données auraient été détournées lors de l'usage d'un automate de paiement ou de retrait. Il ne dispose pas non plus de chiffres de fraude spécifiquement réalisée sur des automates de paiements.

Il connaît en revanche, essentiellement pour les cartes de type « interbancaire », le montant de la fraude concernant les cartes françaises utilisées en retrait :

– sur les DAB français, qui exploitent des transactions en mode puce, cette fraude concerne presque exclusivement l'usage de cartes perdues ou volées. Elle représentait en 2006 un montant de 17,4 millions d'euros, soit 0,019 % du montant des retraits effectués en France par des cartes françaises ;

– sur les DAB étrangers, la fraude est réalisée à 80 % sur des transactions en mode piste et concerne principalement des cartes contrefaites. Elle représentait en 2006 un montant de 22,4 millions d'euros, soit 0,556 % du montant des retraits effectués à l'étranger par des cartes françaises.

Environ 80 % de la fraude sur DAB à l'étranger est réalisée en Europe, principalement en Italie (10 millions d'euros, soit 30 % du total de la fraude sur DAB à l'étranger). Compte tenu des mesures dites de transfert de responsabilité (*« liability shift »*), l'essentiel du montant de cette fraude est toutefois à la charge des banques italiennes.

Environ 40 000 cartes françaises ont subi en 2006 des transactions frauduleuses réalisées sur des DAB étrangers. Le coût du préjudice pour une carte fraudée utilisée sur un DAB est en moyenne de 600 euros, en trois transactions frauduleuses.

Objectifs des attaques

Les automates de paiement et de retrait font l'objet de deux types d'attaques malveillantes, ayant pour objectif :

– la récupération des données des cartes introduites par leur porteur légitime dans l'automate. Ces données permettent ensuite de réaliser des fausses cartes à pistes magnétiques. Certains dispositifs permettent la capture de la carte elle-même. Les fraudeurs cherchent aussi à récupérer en même temps le code confidentiel correspondant, pour utiliser la carte fraudée dans le plus grand nombre d'automates et de terminaux de paiement ;

– l'utilisation de fausses cartes, de cartes volées ou le détournement de fonctions de l'automate pour obtenir frauduleusement le bien ou le service distribué par l'automate.

Typologie des attaques

Les principales attaques réalisées sur les automates visent :

– à capturer la carte : un dispositif est ajouté sur la fente d'insertion de la carte et permet de bloquer celle-ci. Le porteur légitime croit à un dysfonctionnement de l'automate. Après son départ, le fraudeur peut récupérer la carte. Cette méthode suppose toutefois que le fraudeur ait pu visualiser la saisie par le porteur de son code confidentiel pour qu'il puisse ensuite faire usage de la carte ;

– à récupérer les données confidentielles de la carte, y compris le code du porteur : plusieurs dispositifs ont été observés, permettant soit de copier les données de la piste au moyen d'un lecteur de piste pirate installé sur l'automate, soit de copier les données d'identification

de la carte ainsi que le code confidentiel grâce à du matériel placé dans l'automate ou sur celui-ci ;

– à modifier les logiciels et paramètres de l'automate pour en prendre le contrôle ou modifier son fonctionnement : une telle attaque est très rare et repose par exemple sur l'emploi de logiciels malveillants. Dans un cas récemment observé à l'étranger, le fraudeur a réussi à utiliser le code d'administration de l'automate initialisé par le constructeur et que l'exploitant n'avait pas modifié. L'automate distribuait ainsi des coupures d'un montant supérieur à ceux demandés.

Les fraudes observées

Les transactions réalisées sur la base des pistes magnétiques n'offrent pas une protection aussi élevée que celles effectuées en utilisant la puce.

Les **cartes volées** avec leur code confidentiel, qu'elles fonctionnent en mode puce ou piste, peuvent, avant leur mise en opposition, permettre de réaliser des transactions de paiement ou de retrait en France ou à l'étranger. Même si certaines de ces transactions frauduleuses peuvent être réalisées sur la base de la piste ou pour des transactions en vente à distance, elles n'ont pas pour origine la compromission d'automate. En France, ces fraudes sont supportées par le porteur jusqu'à la mise en opposition de la carte, dans la limite du plafond fixé par la loi.

Les **fausses cartes**, associées au code confidentiel, sont utilisables avec leurs pistes magnétiques, dans les quelques cas suivants :

– les cartes françaises contrefaites sont utilisables par les fraudeurs, en paiement et en retrait, dans les pays où les dispositifs d'acceptation ne sont pas encore au standard EMV (en mode piste). Cette utilisation n'est néanmoins possible que jusqu'au moment de la mise en opposition de la carte puisque toutes ces transactions font, la plupart du temps, l'objet d'une demande d'autorisation à l'émetteur français. Dans tous les cas, ces fraudes ne sont pas à la charge des porteurs ;

– les cartes étrangères contrefaites, qu'elles comportent une puce ou non, sont par exception, utilisables en paiement en France sur certains types d'automates ne traitant que la piste magnétique. Les fraudes sont toutefois limitées compte tenu du plafonnement des montants au-delà desquels la demande d'autorisation est requise (souvent à partir du premier euro) et du contrôle de l'inscription de la carte dans la liste d'opposition chargée dans les automates. La migration en cours de ces automates à la norme EMV limitera ces possibilités de fraude aux seules cartes étrangères non équipées de puce ;

– les cartes étrangères non munies d'une puce (émises dans des pays n'ayant pas migré au standard EMV) permettent de réaliser des transactions de retrait en France et à l'étranger à condition que le fraudeur ait en sa possession le code confidentiel. Ces transactions avec des cartes étrangères font l'objet d'une demande d'autorisation, via les réseaux internationaux, et ne sont donc possibles qu'avant mise en opposition. Les éventuelles fraudes sont généralement supportées par les émetteurs étrangers.

Enfin, le numéro de carte (PAN) et la date de validité, qui figurent dans les données de pistes magnétiques, permettent aussi de réaliser des transactions en vente à distance. Ces fraudes ne sont possibles qu'avant la mise en opposition de la carte et uniquement lorsque le commerçant ne demande pas le code CVx2 gravé au dos de la carte (qui nécessiterait que le fraudeur ait eu la carte entre les mains). En France, la plupart des émetteurs de cartes de types « interbancaire » et « privatif » exigent ce code pour les transactions de paiement à distance (Voir Encadré 2, page 15 du rapport de 2005).

Les mesures de protection existantes

Compte tenu des scénarios d'attaque possibles, la protection des automates doit être envisagée selon les trois axes suivants :

– les contrôles réalisés pendant et après la transaction ;

– les protections contre des dispositifs pirates placés à l'extérieur et à l'intérieur de l'automate ;

– les défenses contre des dispositifs placés sur les lignes de communication ou l'usage de logiciels espions et malveillants.

Les contrôles réalisés pendant et après la transaction

Selon que la transaction est effectuée en mode puce EMV ou en mode piste, les protections réalisées ne sont pas exactement les mêmes. Le déploiement en Europe des cartes à puce EMV va considérablement limiter l'usage des pistes magnétiques et y réduire les fraudes liées à la récupération des données de la piste.

Le mécanisme de demande d'autorisation, éventuellement systématique pour certains types de transactions, la vérification des listes d'opposition, le contrôle du code confidentiel localement dans l'automate ou en ligne sur le serveur de l'émetteur, sont des mesures mises en œuvre très fréquemment pour prévenir l'utilisation frauduleuse de cartes sur automates. Pour plus d'efficacité, certaines mesures sont souvent ciblées géographiquement et tiennent compte du type d'automate à protéger.

Enfin, l'analyse a posteriori des fichiers de transactions et des fraudes permet de repérer les automates compromis, d'identifier les numéros de cartes volés, de déclencher des enquêtes et de constituer des statistiques utiles à la détection lors de l'autorisation de transactions risquées (se reporter au paragraphe « Systèmes de détection automatique de la fraude », page 38 du rapport de 2003 de l'Observatoire).

Les protections de l'automate contre les dispositifs disposés à l'intérieur de l'automate

La protection contre les dispositifs espions disposés à l'intérieur passe, tout d'abord, par une restriction des accès dans les automates. Ainsi, les constructeurs proposent du matériel robuste comportant des systèmes de fermeture efficaces parfois associés à des alarmes. Les accès à la fonction de vente de service (ou de distribution de billets) et à la fonction de paiement sont souvent enregistrés et fréquemment séparés. Cela permet de restreindre l'accès aux lecteurs de carte aux seuls exploitants habilités, et donc de limiter les possibilités d'installer des dispositifs de piratage. Un second niveau de protection est mis en œuvre pour la fonction de paiement elle-même, notamment par le chiffrement de bout en bout du code confidentiel, depuis le clavier jusqu'au système de traitement informatique de la transaction. Enfin, le clavier et l'électronique de commande sont sécurisés physiquement pour empêcher toute possibilité de récupérer le code et les données qui y transitent.

Les protections de l'automate contre les dispositifs placés à l'extérieur de l'automate

La façade de l'automate est adaptée pour le protéger contre la pose de dispositifs pirates externes. Dans certains automates, l'affichage de son image normale sur l'écran permet à

l'utilisateur d'identifier d'éventuelles modifications. L'apposition de caches protégeant contre l'observation de la saisie du code confidentiel et la vidéosurveillance des automates sont des mesures également de plus en plus généralisées.

Le Groupement des Cartes Bancaires « CB » impose depuis 2005 des exigences de sécurité, appelées *« AFAS – Anti Fishing Anti Skimming »* (anti-capture, anti-copie) pour les automates de paiement et de retrait. Celles-ci portent sur les modalités de maintenance, la protection de la façade et du code confidentiel. Ces exigences sont maintenant prises en compte dans le processus de fabrication des constructeurs qui réalisent des façades très élaborées et proposent des protections diverses. Depuis plusieurs mois, la conformité à ces exigences est un pré-requis à l'agrément des automates de paiement par le Groupement des Cartes Bancaires « CB ».

La protection des données sur les lignes de communication

Les automates de paiement acceptant les cartes « CB » sont soumis aux mêmes règles que celles applicables pour les terminaux de paiement électroniques. La partie précédente décrit en détail les principes retenus pour sécuriser ces échanges. Les automates de retrait sont reliés à des serveurs informatiques qui surveillent en temps réel et en permanence le fonctionnement de l'automate. L'ensemble des échanges est chiffré.

Les défenses contre l'espionnage des communications ou l'usage de logiciels malveillants

L'usage de plus en plus répandu de systèmes d'exploitation du marché (Windows, Linux) dans les ordinateurs de pilotage des automates génère de nouvelles vulnérabilités aux virus informatiques ou aux logiciels malveillants (chevaux de Troie). Les systèmes d'exploitation sont souvent « durcis » par le constructeur en limitant l'usage aux seules fonctions utiles et en empêchant l'installation de logiciels inconnus. Ils sont protégés selon les dernières prescriptions de protection des ordinateurs (pare-feu, etc.).

Lorsque les applications logicielles installées dans les automates peuvent être téléchargées, il est important que cette opération s'effectue en toute sécurité. C'est pourquoi ces applications logicielles sont souvent signées par le constructeur ou l'éditeur de logiciel en utilisant un mécanisme cryptographique, empêchant l'installation de logiciels qui ne seraient pas authentiques. Ces téléchargements peuvent également n'être réalisables que depuis des serveurs propres à chaque constructeur.

La communication auprès des utilisateurs

Ces dispositions sont complétées par une communication à destination :

- des porteurs, réalisée par les établissements bancaires, directement sur les automates de retrait (« frappez votre code à l'abri des regards indiscrets ; ne vous laissez pas distraire par un inconnu… »). Elle est souvent relayée par une information conduite par les associations de consommateurs. L'Observatoire propose cette année un ensemble de conseils de prudence pour l'utilisation des cartes (cf. chapitre 4) ;
- des exploitants des automates de retrait dans les agences bancaires (organisée par la Fédération Bancaire Française) et aux commerçants disposant d'automates de paiement (organisée pas les associations de commerçants), pour détecter toute anomalie en cours ou passée, sur la façade de l'automate.

Perspectives

Visa, Mastercard, JCB, sous leur label commun PCI, ont défini des exigences de sécurité spécifiques pour les automates (dites PCI-UPT pour *« Unattended Payment Terminal »*, automate de paiement), similaires à celles existant pour les terminaux de paiement (voir l'encadré 3, page 14 du rapport 2005 de l'Observatoire). Elles prescrivent des protections physiques et logiques de l'ensemble des composants électroniques intégrés dans l'automate (clavier, électronique de commande, écran …). Ces exigences résultent toutefois d'analyses de risques valant principalement pour les systèmes internationaux utilisant encore la carte à piste et peuvent paraître inutilement lourdes pour des matériels effectuant, comme en France, des transactions par carte à puce[17].

De plus, certains points de ce référentiel de sécurité restreignent les fonctionnalités de vente pour protéger la fonction de paiement. Par exemple, l'usage de l'écran est limité à la seule fonction de paiement, sans possibilité de réaliser un dialogue commercial avec le client. De même, dans certains cas, l'utilisation de cartes de type « privatif » serait rendu impossible limitant considérablement le chiffre d'affaires des automates. C'est pourquoi, les commerçants se sont opposés à la mise en œuvre de ces exigences tant que ces points n'auront pas été résolus par PCI. Les mesures du Groupement des Cartes Bancaires « CB », qui couvrent certains risques visés par PCI, ont vocation à être appliquées, dans l'attente d'une adaptation du référentiel PCI au contexte européen.

De son côté, le groupe européen *Common Approval Scheme* définit des exigences de sécurité, complémentaires à celles élaborées par les réseaux internationaux, pour les cartes, les terminaux de paiement et les automates. Il étudie les méthodes d'évaluation de ces matériels et construit un schéma de certification sécuritaire, basé sur une reconnaissance mutuelle des certificats émis dans les différents pays de la zone SEPA. Ces travaux sont reconnus par l'EPC, qui a en charge la coordination des diverses initiatives en matière de standards européens.

Recommandations

L'Observatoire prend note que, compte tenu du niveau élevé de protection des données enregistrées dans la puce, la lecture de la piste magnétique est la cible privilégiée des fraudeurs pour voler ces données. Toutefois, un grand nombre d'automates conservent un lecteur mixte de puce et de piste magnétique, soit pour permettre l'acceptation de cartes internationales ou de cartes de type « privatif », soit si ce n'est pas le cas, parce que cela résulte de la standardisation industrielle de leur fabrication.

Ainsi, pour certains automates de paiement ne nécessitant pas d'accepter les cartes à piste, l'Observatoire recommande à leurs fabricants, dès la conception de l'automate, de ne pas intégrer de lecteur de pistes magnétiques, souvent conservés pour des seules raisons de standardisation industrielle.

En effet, l'existence de ce lecteur de pistes expose inutilement les cartes à puce au risque de compromission de leurs données de piste lors de l'usage de ces automates. Ce choix de supprimer ou non un lecteur de pistes devra s'effectuer évidement en liaison étroite avec les émetteurs de cartes de type « privatif » pour ne pas risquer de réduire le service offert à leurs porteurs.

---

[17] Les transactions avec des cartes de type « privatif » françaises à pistes magnétiques, qui sont réalisées le plus souvent en ligne et dans un contexte très fermé (carte d'enseigne utilisée dans les magasins de l'enseigne) ne sont pas assujetties aux exigences « PCI ».

Par ailleurs, pour les automates requérant la double lecture puce et piste, l'usage de lecteurs séparés puce et piste, comme cela existe déjà pour les terminaux de paiement, pourrait permettre de déjouer les risques de compromission de la piste pendant une transaction avec la puce. Une telle mesure présenterait un intérêt tout particulièrement pour les automates présentant des risques importants de par leur type d'utilisation ou leur isolement géographique. L'Observatoire note cependant qu'une telle évolution représenterait un changement notable de la configuration des automates, avec des conséquences notamment en termes de coût de renouvellement et d'ergonomie d'utilisation par les clients. L'Observatoire estime en conséquence utile que les exploitants de ces automates étudient les conditions de faisabilité de cette mesure et vérifient que sa mise en place ne les expose pas à des fraudes de contournement d'une autre nature.

En parallèle, l'amélioration déjà engagée des dispositifs assurant une protection physique des automates, tels que ceux empêchant la pose de matériel de piratage ou permettant à l'utilisateur de vérifier l'aspect extérieur de l'automate (mesures AFAS), devrait être généralisée lors du renouvellement du matériel ou en cas de corruption de celui-ci par un fraudeur.

L'Observatoire attire l'attention des constructeurs sur la nécessité de systématiquement prendre en compte toutes ces menaces dès la conception de leurs automates, et en particulier celles portant atteinte à l'intégrité des logiciels embarqués.

L'Observatoire encourage par ailleurs les émetteurs et les commerçants à développer des campagnes de communication vis-à-vis des porteurs pour susciter leur attention lors des transactions sur automate. De même, le programme de communication mené par la Fédération Bancaire Française envers les exploitants des agences bancaires apparaît très utile pour identifier au plus tôt les automates compromis.

En tout état de cause, la problématique de la sécurité des automates requiert une convergence des efforts de standardisation sécuritaire à un niveau européen, impliquant toutes les parties prenantes : industriels, commerçants et banques. L'Observatoire se félicite de ces différentes initiatives et encourage les différentes parties prenantes à y participer activement et de façon coordonnée.

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 trois 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 continuent de montrer une situation inégale en Europe, certains pays, dont la France, étant proches d'achever leur migration, et d'autres restant très en retard. L'Observatoire s'inquiète à nouveau de ces disparités qui sont susceptibles de laisser perdurer une fraude transfrontalière européenne significative. À quelques mois de la mise en œuvre, début 2008, du projet SEPA pour les cartes, ces retards peuvent signifier que les adaptations ne seront pas toutes achevées en 2008, ce qui aura pour effet de faciliter la fraude sur les paiements transfrontaliers.

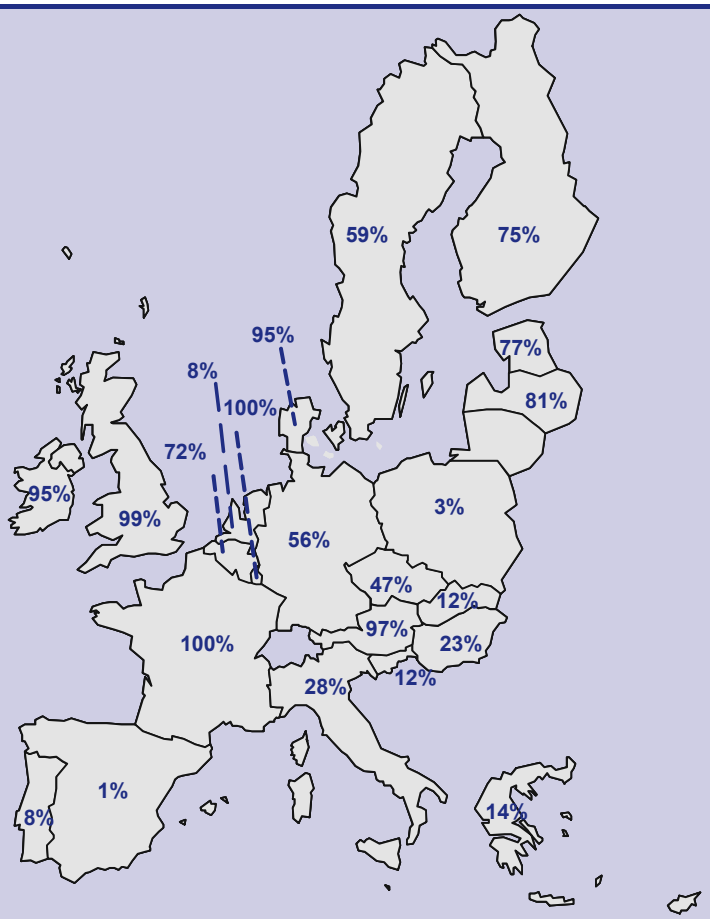
État de la migration en France

En France, la migration au standard EMV est pratiquement terminée. Fin mars 2007, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes CB, 95 % des terminaux et automates, et 100 % des distributeurs automatiques de billets étaient conformes aux spécifications EMV.

État de la migration en Europe

Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2007, 53,8 % des cartes interbancaires circulant en Europe (EU 27) sont maintenant conformes à la spécification EMV (+ 6 points). Pays par pays, la situation est nettement contrastée (voir Encadré 10). À quelques mois de l'échéance du projet SEPA, plusieurs grands pays ont soit à peine commencé leur migration (Espagne, Pologne, Portugal, Pays-Bas), soit peu avancé dans celle-ci, au point de ne vraisemblablement pas pouvoir équiper la totalité de leur parc en 2008 (Allemagne, Italie, Suède notamment).

Encadré 10 – Déploiement des cartes EMV en Europe



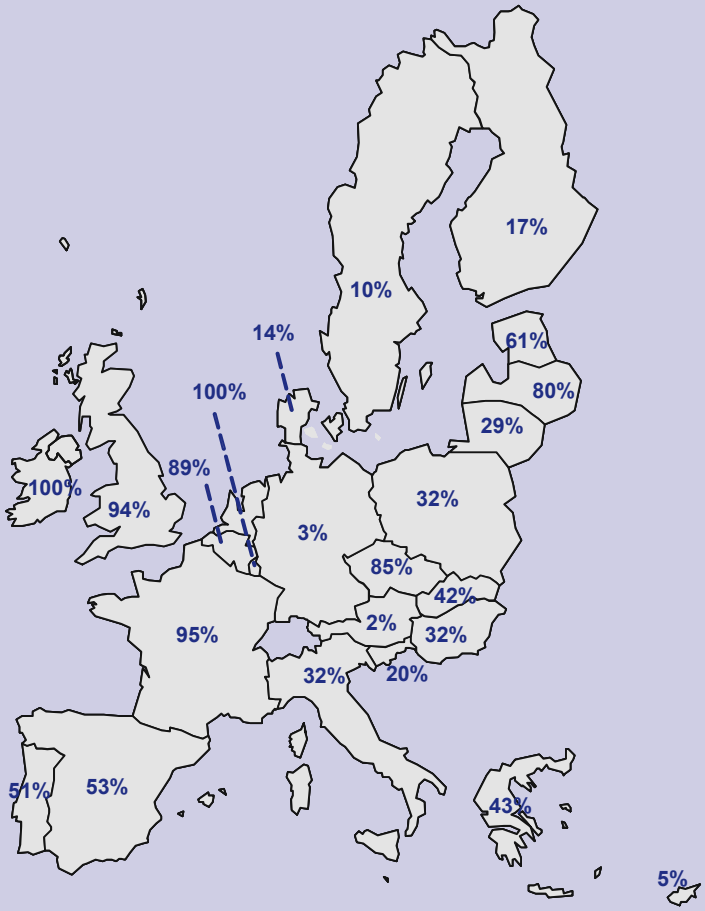
Source : European Payments Council – mars 2007

Comme en 2006, plusieurs grands pays débutent à peine leur migration de cartes, ceci est le cas par exemple pour l'Espagne, l'Italie et la Pologne.

L'Observatoire constate ainsi à nouveau un avancement supérieur du déploiement des cartes EMV dans les pays du Nord de l'Europe.

Concernant l'acquisition, à fin mars 2007 la migration vers EMV progresse sensiblement (+ 14 points) : 51,7 % des terminaux de paiement (voir Encadré 11) et 66,1 % des distributeurs automatiques de billets (voir Encadré 12) sont conformes à EMV. La situation reste très contrastée pays par pays tant en taux d'équipement qu'en progression d'une année sur l'autre. La situation évolue très peu en Allemagne et en Autriche par rapport à mars 2006, ces pays restant à un très faible niveau d'équipement. Toutefois, tous les pays ont entamé leur migration.

Encadré 11 – Déploiement des terminaux et automates EMV en Europe

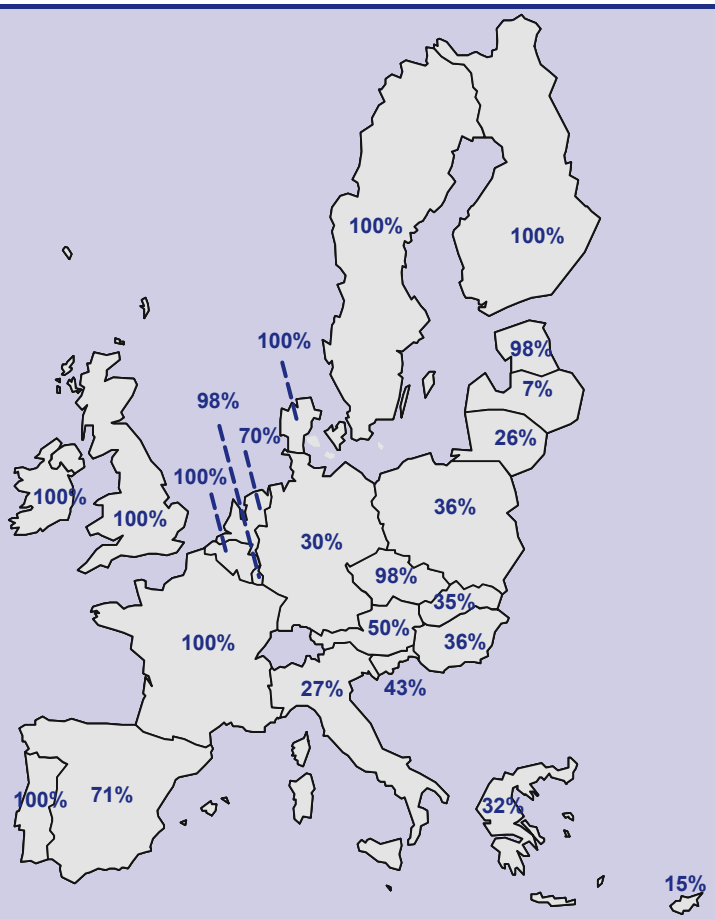


Source : European Payments Council – mars 2007

Cette répartition géographique met en évidence une tendance inverse à 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 plus élevés de transactions transfrontalières.

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.

Encadré 12 – Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2007

La progression de la migration des distributeurs de billets est plus homogène dans les différents pays européens, même s'il subsiste des disparités encore fortes. Les pays en cours de migration de leur parc de distributeurs automatiques de billets au standard EMV, ont probablement choisi en priorité de migrer les automates utilisés par les touristes et visiteurs étrangers. L'Allemagne et l'Italie restent toutefois en deçà des niveaux de déploiement des autres grands pays.

4 | PERCEPTION PAR LES PORTEURS DE LA SECURITE DES CARTES DE PAIEMENT

Les statistiques publiées par l'Observatoire permettent depuis plusieurs années de mesurer le niveau de la fraude sur les paiements par carte, son évolution, et d'apprécier les modes de paiement les plus exposés. L'Observatoire ne disposait toutefois pas jusqu'ici d'indications sur la perception par les porteurs de la sécurité des paiements par carte, ni sur son incidence sur les modalités d'utilisation des cartes de paiement.

C'est pourquoi, au début de 2007, l'Observatoire a fait procéder à un sondage auprès des porteurs de cartes de paiement français. L'enquête a été conduite par l'institut CSA auprès d'un échantillon représentatif de 1 005 personnes âgées de 18 à 74 ans résidant en France métropolitaine[18], contactées par téléphone du 5 au 6 février 2007.

Les résultats de ce sondage sont présentés ci-après. En confrontant ceux-ci aux statistiques dont il dispose, l'Observatoire s'est attaché à vérifier si les réponses des porteurs confirmaient les principales tendances observées dans les statistiques. Par ailleurs, l'analyse des résultats a montré la rémanence chez les porteurs de comportements risqués, ou parfois une méconnaissance des mécanismes d'opposition ou de contestation destinés à les protéger. C'est pourquoi l'Observatoire a élaboré, avec le soutien des différents collèges de représentants des consommateurs, des commerçants et des émetteurs qui le composent, une liste de conseils de prudence destinée au grand public.

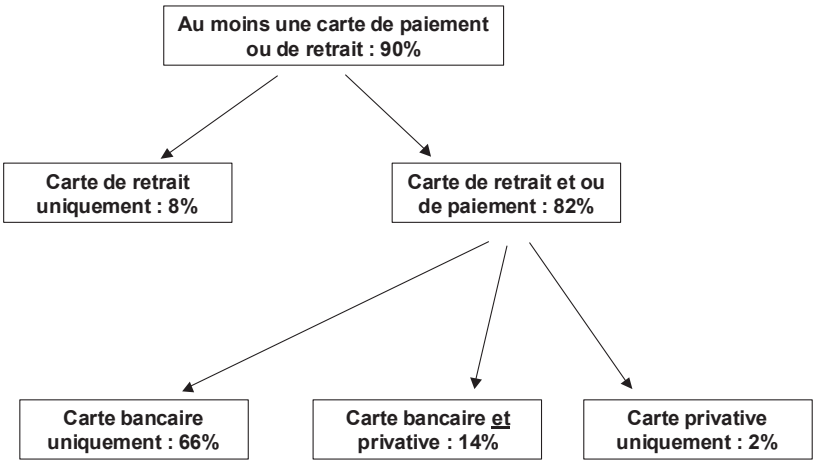
4|1 Le contexte de détention et d'usage des cartes de paiement

La détention des cartes de paiement

Une très large majorité des personnes interrogées, 9 personnes sur 10, détient aujourd'hui au moins une carte de paiement ou de retrait. Plus précisément, 8 % détiennent seulement une carte de retrait d'espèces, tandis que 80 % détiennent au moins une carte bancaire de paiement, et 16 % au moins une carte privative[19].

[18] L'échantillon a été construit selon la méthode des quotas qui portaient sur le sexe, l'âge, le statut professionnel et la profession des personnes interrogées, ainsi que sur la taille d'agglomération et la région d'habitation. Le sondage a été précédé d'une phase qualitative qui a consisté à réunir, à Paris et en province, plusieurs groupes de porteurs présentant chacun des comportements similaires en termes d'usages de leurs cartes.

[19] Il est à noter que pour les besoins de l'enquête, la typologie des cartes a été décomposée de manière différente de celle qu'emploie habituellement l'Observatoire. Les « cartes bancaires », de paiement ou de retrait, regroupent toutes les cartes de marque « CB », « Visa », « Mastercard », « American Express » ou « Diners », tandis que les « cartes privatives ou de magasin » sont celles émises par les organismes de crédit comme « Cetelem », « Cofinoga », « Sofinco », « Finaref », « Franfinance ». Cette dernière catégorie est parfois commercialisée au porteur directement par un commerçant et la carte reprend alors principalement ses éléments de visuel commercial.

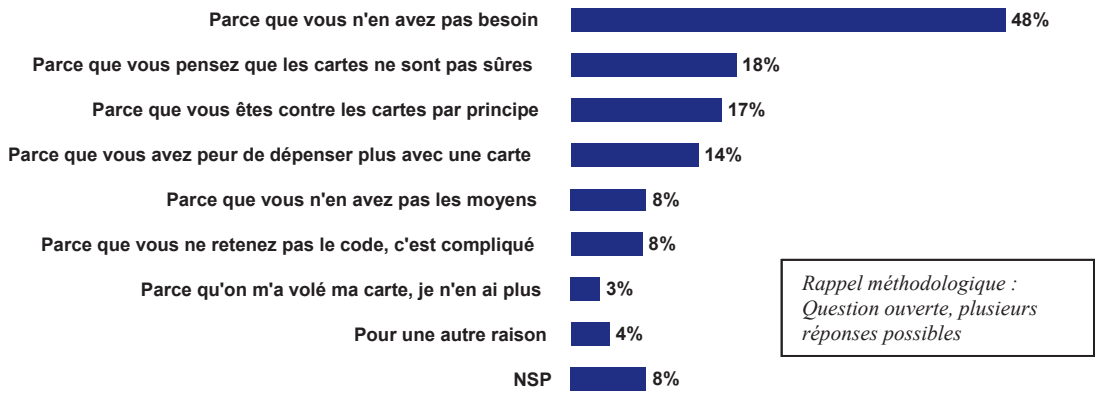


Les raisons qui motivent le choix de ne pas détenir certaines cartes sont multiples (voir graphique ci-après). La première raison citée est l'absence de besoin. Le manque de sécurité est cité en deuxième rang (18 %), mais cela signifie que seuls 2 % de la population totale âgée de 18 à 74 ans ne possèdent pas de carte parce qu'ils ont des craintes concernant la sécurité.

Les autres motifs mis en avant par les porteurs sont principalement leur refus de principe de détenir une carte et l'insuffisance de leurs moyens financiers (que ce soit parce qu'ils craignent de dépenser plus avec une carte ou à cause du coût de la carte elle-même).

Raisons de non détention de carte :

(base : non détenteurs de carte soit 10 % des personnes interrogées)



La segmentation des cartes perçue par les porteurs

Le marché français des cartes de paiement se caractérise par la disponibilité de nombreux types de cartes associés à différents usages et publics. L'étude qualitative, dont les résultats ont été confirmés par l'étude quantitative, a montré que les porteurs structurent l'offre de cartes de paiement en quatre grandes catégories décrites ci-après.

Les cartes « classiques quotidiennes » (taux d'équipement dans la population des 18-74 ans : 61 %)

Cette catégorie recouvre, dans la typologie habituellement utilisée par l'Observatoire, les cartes de type « interbancaire » les plus courantes. Les cartes « classiques quotidiennes » sont les

plus utilisées et les plus courantes dans tous les usages : paiements des achats courants, retraits d'argent, utilisation à l'étranger ou sur Internet.

Ces cartes sont parfaitement intégrées dans les habitudes de paiement et leur usage s'est banalisé, même si elles peuvent encore être parfois en concurrence avec le chèque, en particulier dans les catégories de population de plus faible niveau socioculturel.

Les cartes « sélectives »
(taux d'équipement dans la population des 18-74 ans : 17 %)

Cette catégorie rassemble des cartes de type « privatif » internationales au sens habituellement entendu par l'Observatoire (American Express ou Diners Club), mais aussi, pour certains porteurs, des cartes de type « interbancaire » de haut de gamme. Les porteurs hésitent sur le positionnement de ces dernières en raison de leur proximité avec les cartes « classiques quotidiennes », probablement en raison de leur large diffusion.

Les cartes « sélectives » bénéficient d'une image de « prestige », en particulier par les non-porteurs. Elles sont souvent associées par leurs porteurs à des usages plutôt exceptionnels ou circonstanciés (grosses dépenses, voyages, dépenses à forte symbolique sociale, etc.). Elles sont également perçues comme plus sûres que les autres cartes en raison des différents services et garanties associés à la carte, notamment l'assistance.

Les cartes « restrictives »
(taux d'équipement dans la population des 18-74 ans : 8 %)

Il s'agit des cartes à autorisation systématique et des cartes de retrait d'espèces. Elles sont assez peu valorisées et associées soit aux jeunes encore inexpérimentés dans la gestion de leur compte, soit aux populations à revenus modestes. En raison de la limitation de leur usage, elles sont perçues comme plus sûres que les cartes classiques.

Les cartes « de magasins »
(taux d'équipement dans la population des 18-74 ans : 18 %)

Il s'agit de toutes les autres cartes de type « privatif », émises par les établissements de crédit à la consommation, dont certaines sont parfois vues par les porteurs comme étant émises par des enseignes de la grande distribution. L'attrait de ces cartes réside donc directement dans la réserve de crédit consentie, même si selon les situations, l'action de fidélisation est également un facteur d'adhésion. Comme pour les cartes restrictives, l'usage restreint des cartes de magasin leur confère aux yeux des porteurs un sentiment de plus grande sécurité.

L'usage des cartes de paiement

Les porteurs interrogés montrent un grand attachement à leurs cartes, auxquelles ils associent très spontanément des attributs tels que la modernité et la facilité d'usage. Acceptées quasiment chez tous les commerçants et pour tout type de montant, les cartes sont adaptées à des situations de paiement très variées (achat, crédit, retrait) et sont utilisées très naturellement par leurs porteurs. Cet attachement est bien supérieur aux préoccupations éventuelles liées à la fraude.

Un usage généralisé en France

L'utilisation de la carte en France est aujourd'hui totalement banalisée pour une grande majorité de porteurs : près de 8 porteurs sur 10 déclarent utiliser leur carte souvent ou systématiquement pour payer leurs achats et une proportion comparable l'utilise chez un commerçant au moins une fois par semaine. Seule une petite minorité utilise sa carte moins d'une fois par mois.

Les plus gros utilisateurs sont des hommes, d'âge intermédiaire (45-54 ans), de catégorie socioprofessionnelle supérieure et de revenu élevé, habitant plutôt en milieu urbain. L'utilisation fréquente des cartes est par ailleurs fortement liée à un intérêt pour les nouvelles technologies.

La quasi-totalité des porteurs de cartes effectue également des retraits aux distributeurs ou guichets automatiques (95 %) et la moitié en effectue au moins un par semaine. En revanche, les comportements face aux automates de paiement (péage, distributeurs de billets de train, etc.) sont plus contrastés : si la proportion des porteurs qui paient avec leur carte sur automate est plus faible (environ trois porteurs sur quatre), la fréquence des paiements y est relativement importante parmi ceux qui les pratiquent (plus de 5 fois par mois).

Mais des réticences subsistent pour les paiements à distance et à l'étranger

Si l'usage de la carte pour les paiements à distance est naturel pour de nombreux porteurs (30 % d'entre eux paient avec leur carte par téléphone au moins 3 fois par an et 47 % des porteurs ayant accès à Internet paient en ligne à cette même fréquence), une part de la population reste réticente à l'utilisation de la carte pour payer à distance : 33 % des porteurs ne l'utilisent jamais pour payer par téléphone, par courrier ou sur Internet.

Concernant les paiements à l'étranger, alors que 51 % des détenteurs de carte internationale l'utilisent souvent ou systématiquement lors de leurs voyages, à la fois en paiement ou en retrait, 33 % ne l'utilisent pas pour des retraits à l'étranger et une proportion comparable ne l'utilise jamais pour payer, ou alors le moins souvent possible.

4|2 Les jugements portés sur la sécurité des cartes

Les cartes sont jugées plus sûres que les autres moyens de paiement

Parmi les différents moyens de paiement, la carte est celui qui apparaît aujourd'hui comme le plus sûr du point de vue des consommateurs, devant l'argent liquide, les virements ou prélèvements et le chèque.

Moyen de paiement jugé le plus sûr :

(Base : ensemble de la population française âgée de 18 à 74 ans)

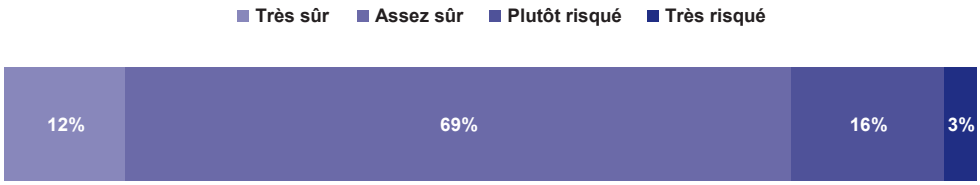
Ce classement diffère cependant sensiblement selon les segments de population : la carte est ainsi en tête parmi les 45-64 ans mais c'est l'argent liquide qui est jugé le plus sûr parmi les plus jeunes (18-24 ans), alors qu'à l'inverse les plus âgés (65 ans et plus) placent le chèque en tête.

Un moyen de paiement perçu comme sûr

La grande majorité des porteurs de carte considère que l'utilisation des cartes est aujourd'hui globalement sûre : 12 % considèrent qu'elle est « très sûre » et 68 % « assez sûre ». Seuls 19 % considèrent que l'utilisation des cartes est « risquée », dont 3 % « très risquée ». En outre, la sécurité des cartes est perçue par une très large proportion des porteurs soit comme constante (49 %) soit comme en amélioration (43 %).

Perception globale de la sécurité des cartes :

(Base : ensemble des porteurs de cartes âgés de 18 à 74 ans)



Par ailleurs, les questions de sécurité ne peuvent pas être considérées comme une entrave potentielle à l'utilisation des cartes, puisque 13 % seulement des porteurs déclarent être gênés dans leur utilisation en raison du risque qu'ils perçoivent.

Comme celles qui font le plus usage des cartes, les personnes les plus nombreuses à considérer l'utilisation des cartes comme sûre sont plutôt les hommes actifs, de catégories socioprofessionnelles supérieures et intéressés par les nouvelles technologies.

On notera en revanche des opinions plus mitigées quant à la sécurité des cartes chez les personnes plus âgées et/ou de milieu socioculturel plus modeste (65 ans ou plus, employés ou ouvriers, de niveau d'étude primaire ou technique et réfractaires aux nouvelles technologies).

Des craintes persistantes, notamment pour les paiements à distance et l'étranger

Il subsiste néanmoins un décalage entre l'opinion globale que les porteurs expriment au sujet de la sécurité des cartes et le sentiment ressenti en situation d'utilisation. En effet, la quasi-totalité des 12 % de porteurs qui considèrent que l'utilisation de la carte est « très sûre » estiment ne pas prendre du tout de risque quand ils l'utilisent. Mais seulement deux tiers des 68 % qui estiment l'utilisation des cartes seulement « assez sûre » font preuve d'une telle confiance lorsqu'ils l'utilisent.

A l'opposé, 29 % des porteurs qui pensent que, de manière générale, l'utilisation des cartes est risquée, déclarent ne pas avoir le sentiment de prendre de risque lorsqu'ils utilisent leur carte.

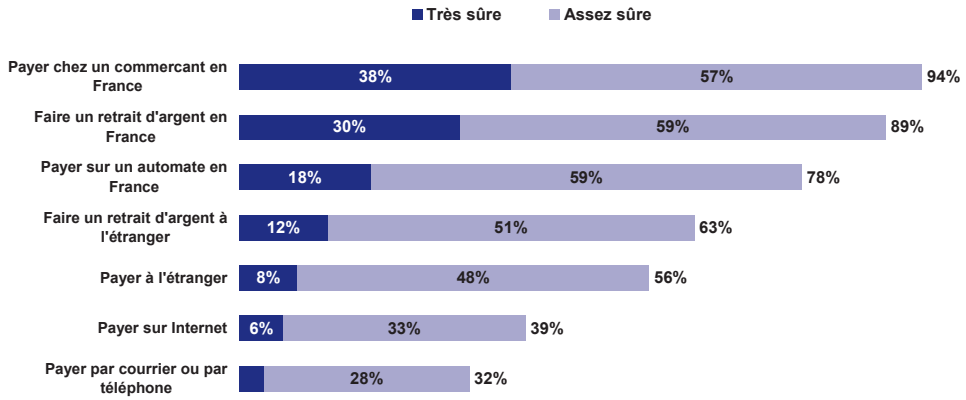
Dans tous les cas cependant, le sentiment d'insécurité demeure limité : seulement 2 % des porteurs déclarent avoir l'impression de prendre beaucoup de risques lorsqu'ils paient avec leur carte et 5 % lorsqu'ils effectuent des retraits.

On notera que ce sentiment est plus répandu parmi les femmes, les personnes les plus âgés et celles réfractaires aux nouvelles technologies.

La perception de la sécurité de l'utilisation des cartes varie néanmoins fortement selon les différents types d'utilisation.

Perception de la sécurité des cartes selon les situations :

(Base : ensemble des porteurs de cartes âgés de 18 à 74 ans)



Jugée sûre par la quasi-totalité des porteurs pour payer ou effectuer des retraits en France, voire très sûre pour environ un tiers d'entre eux, l'utilisation des cartes est jugée plus risquée à l'étranger et plus encore à distance (sur Internet, par téléphone ou par courrier).

Ainsi, près de 4 porteurs sur 10 considèrent que l'utilisation des cartes à l'étranger présente un risque. Cette proportion est de 6 sur 10 pour les paiements sur Internet et de 7 sur 10 pour les paiements par courrier ou par téléphone, qui sont ainsi les deux canaux de paiement par carte jugés les plus risqués.

Les paiements par téléphone ou par courrier se distinguent par ailleurs des autres types de paiement par le fait que même les porteurs qui payent par ces canaux considèrent qu'il s'agit d'un comportement risqué. Ce constat n'est pas valable pour les autres types de paiement, notamment sur Internet (71 % des payeurs en ligne considèrent que payer sur Internet est sûr) et à l'étranger (jugés sûrs par 76 % de ceux qui le pratiquent).

Certains porteurs indiquent faire parfois le choix de payer avec un autre moyen de paiement que leur carte lorsqu'ils considèrent qu'ils courent un risque : 43 % des utilisateurs l'ont déjà fait une fois, 31 % plusieurs fois. Dans les trois quarts des cas, il s'agissait de paiements à distance (Internet, courrier ou téléphone) ou à l'étranger. Le principal moyen de substitution est le chèque (dans près des deux tiers des cas) suivi par les espèces (dans un quart des cas).

4|3 La prise en considération des questions de sécurité : des réflexes intégrés mais une connaissance à améliorer en matière de droits et de conditions d'utilisation

Les établissements financiers et la Banque de France, premiers acteurs désignés pour améliorer la sécurité des cartes

Les deux types d'organismes qui, selon les utilisateurs de carte, devraient être chargés de l'amélioration de la sécurité des cartes, alors qu'ils ne sont pas considérés comme responsables des risques associés aux cartes de paiement, sont les établissements financiers (cités en premier ou en second par 66 % des personnes interrogées) et la Banque de France (citée en premier ou en second par 63 % des personnes interrogées). Viennent ensuite l'État (28 %), les services de police (18 %) puis, plus marginalement, les associations de consommateurs (11 %) et enfin, les commerçants (9 %).

Les porteurs ont tendance à considérer la fraude comme un phénomène global, touchant tout le monde, mais dont personne n'est directement responsable. Ils se sentent dès lors eux-mêmes fortement impliqués dans la sécurité de leur carte : les trois quarts d'entre eux estiment en effet avoir un rôle à jouer pour éviter d'être victime de fraude. Il est à noter que les plus impliqués sont ceux qui estiment par ailleurs que l'utilisation de leur carte est très sûre ou plutôt sûre.

Des réflexes de précaution bien intégrés

S'agissant de la sécurité des cartes, les mesures mises en place ou les précautions édictées par les établissements bancaires sont globalement connues et appréciées. Le discours des émetteurs sur les gestes de vigilance semble être acquis par les usagers : ils ne perçoivent plus de discours spécifique à ce sujet et déclarent en grande majorité se plier naturellement aux différentes recommandations[20].

Ces recommandations sont d'ailleurs jugées utiles (et même souvent indispensables) et la très grande majorité des utilisateurs de carte de paiement déclarent les appliquer à chaque paiement. Toutefois, encore 5 % des utilisateurs déclarent ne suivre aucune des préconisations des émetteurs.

Mais une information qui peut être améliorée

Qu'il s'agisse des moyens d'améliorer la sécurité des cartes ou des conditions d'utilisation des cartes, l'information des utilisateurs de cartes reste à améliorer :

– plus d'un utilisateur de carte sur deux déclare prêter sa carte à des proches (il s'agit néanmoins le plus souvent du conjoint) ;

– les moyens de sécurisation des paiements en ligne sont encore largement méconnus (68 % des acheteurs en ligne sont incapables d'en citer spontanément même un seul) ;

[20] Le sondage a porté sur les mesures de prudence suivantes : vérifier le montant affiché quand vous tapez votre code ; garder les yeux sur votre carte au moment du paiement chez un commerçant ; conserver vos tickets de paiement et de retrait ; pointer vos relevés de compte ; se renseigner sur les précautions à prendre pour utiliser sa carte en voyage ; sur Internet, ne payer que sur des sites d'entreprises connues et réputées ; sur Internet, installer un antivirus et/ou un firewall sur votre ordinateur. En outre, une question concernait l'attention portée au pointage des relevés de compte.

– les assurances liées à la carte rassurent, mais les porteurs n'en connaissent pas réellement les conditions ni les garanties, et ne savent pas distinguer l'assistance aux personnes de la protection des usages de la carte ;

– instinctivement, la majorité des porteurs ne se considère pas comme responsable financièrement en cas de fraude, mais sans faire de différence particulière entre la contrefaçon et les autres types de fraude ;

– le délai pendant lequel les porteurs pensent pouvoir effectuer une réclamation après la fraude est largement sous-estimé : 68 % l'évaluent à 10 jours ou moins ;

– si plus de 80 % des victimes de vol ou de perte de leur carte ont fait opposition dans la journée, près de 20 % ont attendu au moins un jour et 5 % plus d'une semaine. 3 % déclarent même ne jamais avoir fait opposition.

4 | 4 L'exposition directe ou indirecte à la fraude n'a que peu d'impact sur les comportements

Une forte exposition directe ou indirecte à la fraude

La fraude est un phénomène qui, bien qu'objectivement limité, touche paradoxalement une part significative des porteurs de cartes :

– 8 % des porteurs de carte de paiement déclarent avoir été victimes d'une fraude sur leur carte ;

– 18 % des porteurs ont par ailleurs été exposés à la fraude de manière indirecte, c'est-à-dire qu'ils connaissent parmi leurs proches une victime de fraude sans pour autant l'avoir vécue eux-mêmes.

Au total, un porteur sur quatre a finalement été exposé directement ou indirectement à la fraude. D'après les témoignages des porteurs concernés, la fraude aurait fait suite au vol ou à la perte de la carte dans 21 % des cas et les paiements sur Internet représenteraient 20 % des origines de fraude. Les retraits et paiements en France, qui constituent la majorité des transactions, ne seraient à l'origine que d'une fraude sur quatre.

Le profil des victimes de fraudes correspond à celui des utilisateurs les plus intensifs : il s'agit plus souvent des hommes, des catégories socioprofessionnelles supérieures, ainsi que des personnes ayant un intérêt pour les nouvelles technologies.

Mais l'exposition à la fraude n'a qu'un impact limité sur les comportements et la perception de la sécurité des cartes

L'impact de l'exposition à la fraude est réel pour les personnes qui ont été elles-mêmes victimes de fraude, mais il reste limité. Ainsi, parmi les victimes de fraude, seules 37 % déclarent avoir diminué leur utilisation de la carte, au profit du chèque (22 % des victimes de fraude) ou des espèces (12 %), 63 % n'ayant pas modifié leur comportement.

L'utilisation des cartes est également perçue comme un peu plus risquée par le porteur lorsqu'il a lui-même été victime d'une fraude (27 % des victimes considèrent que l'utilisation de la carte est risquée contre 19 % dans l'ensemble). En revanche, l'exposition indirecte à la fraude semble n'avoir qu'un effet marginal sur la perception de la sécurité des cartes.

Encadré 13 – Types d'attitudes en matière de sécurité des cartes

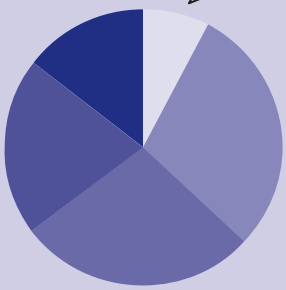
L'enquête réalisée permet d'identifier cinq types de comportements et d'attitude dans la population des utilisateurs de carte :

Les inquiets (15 %)

Angoissés vis-à-vis des cartes, dont ils jugent l'utilisation très risquée, ils ne paient que rarement par ce moyen.

Les confiants (8 %)

Estimant l'utilisation des cartes très sûre, ils utilisent très fréquemment leur carte, dans toutes les situations, sans se poser de question vis-à-vis du risque.



Les prudents (21 %)

Estimant que le contexte n'est pas totalement sûr, ils perçoivent un risque lorsqu'ils utilisent leur carte et prennent beaucoup de précautions.

Les vigilants (28 %)

Ils jugent l'utilisation des cartes assez sûre et, conscients des risques inhérents à la carte, ils l'utilisent sans crainte, tout en restant vigilants.

Les résignés (28 % des porteurs)

S'ils estiment que l'utilisation des cartes est assez sûre, ils ont tout de même le sentiment de prendre un risque à chaque utilisation de leur carte, sans que cela constitue véritablement un frein majeur à leur utilisation.

4|5 Confrontation des principaux résultats du sondage avec les éléments connus par l'Observatoire

La perception généralement positive des porteurs concernant l'utilisation et la sécurité des cartes de paiement est cohérente avec les chiffres publiés ces dernières années par l'Observatoire. Le taux d'équipement des Français relevé par l'Observatoire est élevé, avec 78,6 millions de cartes de types « interbancaire » et « privatif ». En parallèle, la fraude enregistrée sur les systèmes de carte français s'établit en 2006 à 0,064 % du montant des transactions et la tendance par rapport aux années précédentes était à la baisse.

La différenciation du risque perçu en fonction des situations de paiement correspond globalement à la hiérarchie des taux de fraude mesurés par l'Observatoire :

– la confiance élevée des porteurs dans les paiements en face-à-face (94 % des porteurs les considèrent comme sûrs) correspond à un taux de fraude très faible de 0,024 % du montant des transactions ;

– le niveau de confiance des porteurs dans les retraits d'argent au distributeur est inférieur à celle des paiements en face-à-face (89 % des porteurs les considèrent comme sûrs), alors que le taux de fraude enregistré par l'Observatoire est plus faible (0,019 %). Cette

différence peut toutefois s'expliquer par les précautions dont s'entourent les porteurs pour la détention d'argent liquide ;

– les paiements et les retraits d'argent à l'étranger sont perçus dans l'ensemble comme relativement plus risqués. Cette perception est en ligne avec les données connues de l'Observatoire : en 2006, la fraude sur l'ensemble des paiements réalisés par des cartes françaises à l'étranger s'établissait à 0,421 % (contre 0,035 % pour les cartes françaises en France), tandis que la fraude sur les retraits réalisés par des cartes françaises à l'étranger s'établissait à 0,555 % (contre 0,019 % en France). La perception des porteurs varie toutefois très sensiblement si l'on considère seulement ceux qui voyagent effectivement à l'étranger. En effet, seuls 56 % des porteurs considèrent sûrs les paiements à l'étranger, contre 76 % des personnes se rendant effectivement à l'étranger. Ces proportions sont similaires (63 % contre 82 %) en ce qui concerne les retraits d'argent à l'étranger ;

– les paiements à distance sont ceux qui suscitent le plus de réserves, que ce soit pour les paiements sur Internet (considérés sûrs par seulement 39 % des porteurs) ou pour les paiements par courrier ou par téléphone (32 %). Ceci est à rapprocher des estimations réalisées par l'Observatoire : le taux de fraude sur les paiements nationaux à distance est évalué à 0,199 % (soit huit fois plus que pour les paiements en face-à-face et sur automates). Toutefois, on note que les utilisateurs réguliers du paiement sur Internet expriment un niveau de confiance plus élevé (ils sont 71 % à considérer que les paiements sur Internet sont sûrs), phénomène qui ne s'observe pas pour les paiements par courrier ou par téléphone ;

– enfin, les paiements sur automates sont considérés sûrs par 78 % des porteurs. L'Observatoire ne dispose pas de données lui permettant d'évaluer la fraude spécifique à cette situation de paiement, mais les résultats de l'étude qualitative semblent montrer que la médiatisation d'attaques de certains types d'automates a pu générer un comportement de prudence de la part d'une partie des porteurs.

Dans la durée, la fraude concerne une proportion plus significative des Français que ne le mesure l'Observatoire

Il ressort du sondage que 8 % des porteurs déclarent avoir été, au moins une fois dans leur vie, directement victimes d'une fraude, et 18 % supplémentaires indiquent connaître parmi leurs proches au moins une victime de fraude. Seule l'exposition directe à la fraude aurait pourtant un impact sur la perception des porteurs : 27 % des porteurs exposés directement à la fraude considèrent que le paiement par carte est risqué, contre respectivement 18 et 19 % pour les porteurs non-exposés ou exposés indirectement.

Néanmoins, la perception négative résultant d'une exposition directe à la fraude semble persister pendant plusieurs années : le taux apparemment élevé des porteurs concernés par la fraude s'explique par l'accumulation des cas sur plusieurs années, voire plusieurs dizaines d'années.

En croisant les informations sur les comportements, les perceptions et l'exposition à la fraude, l'institut CSA a pu identifier deux groupes de porteurs très significativement différents. Le premier (environ 15 % de la population) rassemble des personnes qualifiées par CSA d'« inquiètes », c'est-à-dire qui jugent que l'utilisation des cartes est très risquée et ne paient en conséquence que rarement par carte. Le deuxième (environ 8 % de la population) rassemble des personnes qualifiées de « confiantes », c'est-à-dire qui estiment l'utilisation des cartes très sûre, les utilisent très fréquemment, dans toutes les situations, sans se poser de question vis-à-vis du risque.

Sur ce point, l'Observatoire ne dispose pas de données lui permettant d'évaluer le nombre de porteurs concernés chaque année par la fraude. Il publie néanmoins le nombre de transactions frauduleuses enregistrées dans les systèmes français, qui peut permettre d'évaluer une borne supérieure du nombre de porteurs concernés. En 2006, 1,7 million de cas de fraude impliquant un porteur français ont été enregistrés : la fraude concerne donc au maximum 2,2 % des cartes en circulation.

Les mesures de prudence recommandées sont connues et appliquées, mais n'ont pas réussi à éliminer tous les comportements à risque

Les mesures de prudence recommandées aux porteurs en situation de paiement par carte ont largement été diffusées auprès du public depuis de nombreuses années, en particulier par les émetteurs et associations de consommateurs membres de l'Observatoire. De ce fait, l'Observatoire n'a pas jusqu'ici communiqué sur l'ensemble de ces mesures. Seules certaines solutions de sécurisation ont fait l'objet d'études ou de recommandations (notamment pour les paiements à distance) dans les précédents rapports.

Les résultats de la présente étude indiquent que l'implication des porteurs dans la sécurité de leurs cartes est élevée : près des trois quarts (72 %) des porteurs estiment avoir un rôle personnel à jouer pour éviter les fraudes. Ils confirment également que les mesures de prudence sont bien comprises et appliquées par la grande majorité des porteurs.

Une proportion faible mais significative des porteurs (5 %) affirme toutefois ne prendre aucune de ces mesures de prudence, tandis qu'une partie d'entre eux considère que ces mesures ne permettent pas d'améliorer la sécurité du paiement par carte.

De plus, la connaissance de ces mesures de prudence n'élimine pas tous les comportements à risque. Malgré les recommandations de la plupart des émetteurs, 53 % des porteurs déclarent ainsi prêter leur carte, principalement à leur conjoint ou à leurs enfants. Suite à la perte ou au vol de la carte, la plupart des porteurs annoncent faire opposition dans la journée (82 %) mais une minorité de porteurs n'a fait opposition que plusieurs jours après la dépossession de la carte.

Concernant spécifiquement le paiement par Internet, les porteurs considèrent comme efficace (à 58 %) l'obligation de fournir le code de sécurisation des paiements à distance (le cryptogramme visuel). Néanmoins, on peut noter la faible notoriété des autres solutions de sécurisation des paiements sur Internet (près de 70 % des acheteurs en ligne n'ont pu en citer aucune), malgré le risque plus élevé perçu par les porteurs.

Les conditions d'utilisation des cartes de paiement sont encore insuffisamment connues

L'Observatoire avait communiqué dans son rapport 2003 sur le cadre juridique applicable en France aux cartes de paiement, en particulier sur deux dispositions protectrices du porteur : la limitation de la responsabilité à un plafond de 150 € avant mise en opposition de la carte (art. L. 132-3 du Code monétaire et financier), et l'absence de responsabilité en cas de paiement « frauduleux, à distance, sans utilisation physique de la carte » (art. L. 132-4).

Les porteurs ne semblent toutefois pas avoir largement connaissance de ces dispositions. Ils considèrent largement (à 70 %) ne pas être financièrement responsables de la fraude quelle que soit son origine (carte perdue ou volée, ou carte altérée ou contrefaite). Le délai légal de

contestation est également largement sous-estimé, probablement parce qu'il est confondu avec un délai d'opposition.

En outre, l'étude qualitative, confirmée par l'enquête quantitative, a montré que la majorité des porteurs ne connaît généralement pas précisément le contenu et les garanties des assurances associées à la plupart des cartes, en particulier celles de type « interbancaire ».

Conseils de prudence à l'usage des porteurs

Pour les différentes raisons évoquées précédemment, l'Observatoire a élaboré une série de conseils de prudence destinés aux porteurs. Ces conseils ont été rédigés en collaboration avec les représentants des consommateurs, des commerçants et des émetteurs, et ont vocation à être réutilisés par ceux-ci, chacun dans son contexte, auprès de leurs publics**.**

La liste qui suit est volontairement rédigée de façon simple et se limite aux principales mesures de précaution. L'Observatoire mettra cette liste de conseils à disposition sur son site Internet et appelle les médias et les pouvoirs publics à relayer largement ces recommandations.

Encadré 14 – Conseils de prudence à l'usage des porteurs

Votre comportement concourt directement à la sécurité de l'utilisation de votre carte. Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

Soyez responsables

– Votre carte est strictement personnelle : ne la prêtez à personne, même pas à vos proches.
– Vérifiez régulièrement qu'elle est en votre possession.
– Si votre carte comporte un code confidentiel, gardez-le secret. Ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter et surtout ne le rangez jamais avec votre carte.
– Lorsque vous composez votre code confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal de votre autre main.
– Vérifiez régulièrement et attentivement vos relevés de compte.

Soyez attentifs

Lors des paiements chez un commerçant :

– Vérifiez l'utilisation qui est faite de votre carte par le commerçant. Ne la quittez pas des yeux.
– Pensez à vérifier le montant affiché par le terminal avant de valider la transaction.

Lors des retraits sur les distributeurs de billets :

– Vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.
– Suivez exclusivement les consignes indiquées à l'écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.
– Mettez immédiatement en opposition votre carte si elle a été avalée par l'automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l'agence.

Lors des paiements sur Internet :

– Protégez votre numéro de carte : ne le stockez pas sur votre ordinateur, ne l'envoyez pas par simple courriel et vérifiez la sécurisation du site du commerçant (cadenas en bas de la fenêtre, adresse commençant par « https », etc.).
– Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les conditions générales de vente.
– Protégez votre ordinateur, en l'équipant d'un antivirus et d'un pare-feu.

Lors de vos déplacements à l'étranger :

– Renseignez-vous sur les précautions à prendre et contactez l'établissement émetteur de votre carte avant votre départ, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.
– Pensez à vous munir des numéros internationaux de mise en opposition de votre carte.

Sachez réagir

Vous avez perdu ou on vous a volé votre carte :

– Faites immédiatement opposition en appelant le numéro que vous a communiqué l'établissement émetteur de la carte. Pensez à le faire pour toutes vos cartes perdues ou volées.
– En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

Votre banque peut vous imposer de faire opposition dans un délai maximum, celui-ci ne pouvant être inférieur à deux jours francs. Si vous faites opposition dans ce délai, vous ne supporterez les débits frauduleux effectués jusqu'à cette date avec votre carte que dans la limite de 150 €. Si en revanche vous dépassez ce délai, vous supporterez l'intégralité des débits frauduleux précédant la mise en opposition. A partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

Vous constatez des anomalies sur votre relevé de compte, alors que votre carte est toujours en votre possession :

Sauf si vous avez commis l'imprudence de communiquer à un proche le numéro et/ou le code confidentiel de votre carte et que celui-ci en a fait usage sans vous prévenir, il faut déposer une réclamation écrite, dès que possible et dans un délai fixé par la loi, de 70 jours à compter de la date de l'opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir dépasser 120 jours. Votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être remboursées sans frais dans le délai maximum d'un mois à compter de la réception de la réclamation.

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, 5e 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 cartes 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 cartes de paiement ;

– il assure une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. 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.

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. Il 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.

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
Directeur adjoint 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 ou son représentant :
  Emmanuel SARTORIUS
  Alain ROCCA
- Le directeur général du Trésor et de la politique économique ou son représentant :
  Maya ATIG
  Audrey SUDARA-BOYER

Sur proposition du ministre chargé de la consommation :

- Le directeur de la direction générale de la concurrence, de la consommation et de la répression des fraudes ou son représentant :
  Virginie BEAUMENIER
  Jean-Pierre GERSKOUREZ

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Pauline FLAUSS
  Vincent MONTRIEUX

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 (Groupe Carte Bleue)

Alain GOLDBERG
Directeur risques et conformité (Natexis 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 de l'Association FO Consommateurs (AFOC)

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

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

Frédérique PFRUNDER
Chargée de mission auprès de la 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)

Marc LOLIVIER
Délégué général de la Fédération des entreprises de vente à distance (FEVAD)

Jean-Marc MOSCONI
Délégué général (MERCATEL)

Philippe SOLIGNAC
Vice-président (Chambre de commerce et d'industrie de Paris)

Guillaume VANOVERSCHELDE
Directeur administratif et financier (DECATHLON)

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL
Executive Vice-President (Gemalto)

Jacques STERN
Directeur du département informatique de l'École normale supérieure (ENS)

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

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, par l'intermédiaire de BMS (Billettique Monétique Services) ;

Les données collectées concernent également six accepteurs de cartes de paiement, à savoir Carrefour, Decathlon, le groupe Casino, France Loisirs, Monoprix et la SNCF. Pour la première fois en 2006, l'Observatoire a également reçu des statistiques recueillies par la FEVAD auprès d'un échantillon représentatif de ses membres.

En raison de changement du périmètre et de certains modes de calculs, toutes les données fournies ici ne sont pas comparables avec les données publiées précédemment par l'Observatoire. Il convient de se reporter à la partie 2 du présent rapport pour une analyse et une mise en perspective des données.

Total des cartes en circulation en 2006 : 78,6 millions

- dont 53,6 millions de cartes de type « interbancaire » (« CB » et Moneo) ;
- et 25 millions de cartes de type « privatif ».

Cartes mises en opposition en 2006 : environ 400 000

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.

Les transactions transfrontalières représentent une très faible part des transactions. En 2006, seules 3,3 % des transactions émises par des porteurs français l'ont été depuis l'étranger (2,5 % en 2005).

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	5 172,59	226,63	101,13	8,09	131,75	12,24
Paiements à distance hors Internet	nd	9,98	5,38	0,79	5,38	1,30
Paiements à distance sur Internet	84,89	6,31	34,62	2,23	7,17	0,72
Retraits	1 295,90	88,35	33,97	4,03	27,85	4,72
Total	**6 553,38**	**331,27**	**175,11**	**15,14**	**172,15**	**18,97**
Cartes de type « privatif »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (en Md€)**	**Volume (millions)**	**Valeur (en Md€)**
Paiement de proximité et sur automate	196,65	22,95	7,77	1,64	15,12	3,36
Paiements à distance hors Internet	0,95	0,23	0,22	0,05	0,54	0,20
Paiements à distance sur Internet	0,67	0,14	0,14	0,03	0,26	0,05
Retraits	11,32	1,03	nd	nd	nd	nd
Total	**209,58**	**24,34**	**8,12**	**1,72**	**15,91**	**3,61**
Total général	**6 762,97**	**355,61**	**183,23**	**16,86**	**188,06**	**22,58**

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 carte 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	**843,9**	**51 923,7**	**184,2**	**26 825,5**	**376,4**	**57 685,1**[1]
Cartes perdues ou volées	522,5	34 448,9	111,4	9 295,6	167,4	11 830,0
Cartes non parvenues	13,4	614,8	3,3	535,6	4,9	479,1
Cartes altérées ou contrefaites	308,0	16 860,1	62,1	15 182,1	96,9	23 249,9
Numéro de carte usurpé	0,0	0,0	4,1	733,4	10,4	801,1
Autres	0,0	0,0	3,2	1 081,7	96,8	21 325,0
Paiements à distance hors Internet	**213,0**	**19 475,7**	**25,4**	**4 567,0**	**nd**	**nd**
Cartes perdues ou volées	0,0	0,0	8,5	1 566,5	nd	nd
Cartes non parvenues	0,0	0,0	0,1	16,2	nd	nd
Cartes altérées ou contrefaites	0,0	0,0	6,0	1 296,8	nd	nd
Numéro de carte usurpé	213,0	19 475,7	1,0	82,8	nd	nd
Autres	0,0	0,0	9,9	1 604,7	nd	nd
Paiements à distance sur Internet	**96,6**	**13 214,0**	**168,4**	**2 051,7**	**nd**	**nd**
Cartes perdues ou volées	0,0	0,0	48,4	5 862,2	nd	nd
Cartes non parvenues	0,0	0,0	0,2	23,2	nd	nd
Cartes altérées ou contrefaites	0,0	0,0	40,9	5 131,2	nd	nd
Numéro de carte usurpé	96,6	13 214,0	2,2	252,2	nd	nd
Autres	0,0	0,0	76,7	8 782,9	nd	nd
Retraits	**72,8**	**15 862,0**	**115,9**	**22 388,3**	**21,1**	**5 047,1**
Cartes perdues ou volées	70,8	15 530,4	16,8	2 927,9	3,4	773,4
Cartes non parvenues	0,5	93,8	0,1	19,7	0,1	19,1
Cartes altérées ou contrefaites	1,5	237,8	98,4	19 298,3	16,5	4 049,6
Numéro de carte usurpé	0,0	0,0	0,6	131,0	0,1	23,1
Autres	0,0	0,0	0,1	11,4	1,0	181,9
Total	**1 226,3**	**100 475,4**	**493,9**	**73 835,5**	**397,5**	**62 732,2**

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	**15,89**	**7 142,51**	**4,38**	**1 248,25**	**2,67**	**1 654,69**
Cartes perdues ou volées	7,31	1 574,74	0,74	246,64	0,92	574,99
Cartes non parvenues	3,47	820,75	0,44	167,81	0,03	4,41
Cartes altérées ou contrefaites	0,66	278,11	2,90	777,35	1,57	911,85
Numéro de carte usurpé	0,38	364,26	0,05	19,33	0,08	48,98
Autres	4,07	4 104,65	0,24	37,12	0,07	114,46
Paiements à distance hors Internet	**0,71**	**306,59**	**3,09**	**1 126,43**	**2,56**	**1 718,84**
Cartes perdues ou volées	0,10	17,77	0,08	22,39	0,13	36,64
Cartes non parvenues	0,07	4,50	0,06	31,22	0,01	4,41
Cartes altérées ou contrefaites	0,07	7,36	0,22	68,06	0,41	192,10
Numéro de carte usurpé	0,38	255,92	2,66	983,72	1,93	1 389,45
Autres	0,08	21,04	0,07	21,03	0,08	96,24
Paiements à distance sur Internet	**0,28**	**205,70**	**0,95**	**219,23**	**1,24**	**441,20**
Cartes perdues ou volées	0,05	56,97	0,01	2,13	0,03	4,53
Cartes non parvenues	0,00	0,00	0,01	0,55	0,01	0,50
Cartes altérées ou contrefaites	0,00	0,00	0,02	3,55	0,08	26,30
Numéro de carte usurpé	0,21	142,73	0,90	211,76	1,11	407,96
Autres	0,02	6,00	0,01	1,24	0,02	1,90
Retraits	**4,45**	**1 492,39**	**0,00**	**0,00**	**0,00**	**0,00**
Cartes perdues ou volées	3,61	863,70	0,00	0,00	0,00	0,00
Cartes non parvenues	0,42	244,33	0,00	0,00	0,00	0,00
Cartes altérées ou contrefaites	0,00	0,00	0,00	0,00	0,00	0,00
Numéro de carte usurpé	0,00	0,00	0,00	0,00	0,00	0,00
Autres	0,42	384,36	0,00	0,00	0,00	0,00
Total	**21,33**	**9 147,18**	**8,42**	**2 593,91**	**6,47**	**3 814,73**

Source : Observatoire de la sécurité des cartes de paiement

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 2 juillet 2007
Dépôt légal 3ème trimestre 2007
ISSN 1767-6665