2008 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 2008
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Madame le Ministre de l'Économie, de l'industrie 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

PROPOS INTRODUCTIF DU PRÉSIDENT

Alors que s'achève le deuxième mandat des membres de l'Observatoire de la sécurité des cartes de paiement, je voudrais souligner combien les enjeux auxquels sont confrontés les professionnels et les utilisateurs des cartes de paiement en termes de sécurité sont au cœur des travaux conduits par notre instance.

La dimension européenne est ainsi devenue très présente dans nos réflexions, du fait des évolutions liées au projet d'Espace unique de paiement en euros (*Single Euro Payments Area* - SEPA) et de la création d'un cadre juridique harmonisé par la directive sur les services de paiement. L'Observatoire a depuis plusieurs années souligné les enjeux liés à l'harmonisation européenne des moyens de paiement et émis des recommandations visant à promouvoir un haut niveau de sécurité des paiements par carte en Europe, jouant bien souvent un rôle précurseur par rapport aux réflexions menées au niveau européen. Cette année, le rapport insiste sur l'importance de la mise en œuvre de procédures harmonisées de certification de la sécurité de cartes en Europe.

L'une des missions essentielles de l'Observatoire est de mesurer la fraude et ses évolutions. Les chiffres publiés chaque année ont été régulièrement enrichis. Ils constituent des données de référence utiles pour l'ensemble des acteurs, car ils permettent de mieux comprendre l'évolution des comportements frauduleux et d'adapter en conséquence les mesures de prudence et de sécurité.

Les statistiques pour 2008 indiquent une montée de la fraude, plus importante que l'augmentation générale du montant des transactions de paiement et de retrait par carte. Cette hausse apparaît principalement en vente à distance, pour les paiements nationaux, mais aussi, et de façon prononcée cette année, pour les transactions effectuées à l'étranger avec des cartes françaises. Les règles de répartition de la fraude permettent toutefois de ne pas faire subir de préjudice aux consommateurs, ceux-ci étant protégés par la loi. L'Observatoire s'est montré attentif à cette évolution de la fraude et a souhaité étudier les conditions de sécurité pour le paiement par carte à distance. Il a considéré qu'il était nécessaire de favoriser un niveau d'authentification renforcé du porteur, chaque fois que cela est possible, afin d'amener la sécurité des paiements à distance à un niveau équivalent à celui des paiements de proximité.

Dans son rapport, l'Observatoire rend également compte de ses analyses sur un certain nombre de thèmes particulièrement d'actualité pour les professionnels et les utilisateurs des cartes de paiement : l'émergence des dispositifs d'« émission immédiate » de cartes de paiement sur le lieu de vente, le développement du « co-marquage » de cartes et la sécurisation des automates de paiement connectés sur des réseaux ouverts.

La richesse de ces travaux constitue une source importante d'informations et de recommandations. Celles-ci contribueront comme chaque année, à n'en pas douter, à guider les efforts de chacun pour garantir la sécurité des paiements par carte.

Christian NOYER

AVANT-PROPOS

L'Observatoire de la sécurité des cartes de paiement a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne[1]. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des systèmes de paiement par carte[2].

Conformément à l'alinéa 6 de l'article L. 141-4 du Code monétaire et financier, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'économie et des finances et transmis au Parlement. Il comprend une étude sur les mesures de sécurité appliquées aux dispositifs d'émission immédiate de cartes de paiement en agence ou en magasin (1ère partie), puis une présentation des statistiques de fraude pour 2008 (2ème partie) et une synthèse des travaux conduits en matière de veille technologique (3ème partie). Enfin, le rapport comprend une étude portant sur la certification de la sécurité des cartes et des terminaux (4ème partie).

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

2 Pour ses travaux, l'Observatoire distingue les systèmes de paiement par carte de type « interbancaire » et ceux de type « privatif ». Les premiers correspondent à ceux dans lesquels il existe un nombre élevé d'établissements de crédit émetteurs et acquéreurs. Les seconds correspondent à ceux dans lesquels il existe un nombre réduit d'établissements de crédit émetteurs et acquéreurs.

1 | MESURES DE SÉCURITÉ APPLIQUÉES AUX DISPOSITIFS D'ÉMISSION IMMÉDIATE DE CARTES DE PAIEMENT EN AGENCE OU EN MAGASIN (« INSTANT ISSUING »)

Dans le cadre de sa mission de suivi des politiques de sécurité mises en œuvre par les émetteurs et les accepteurs, l'Observatoire a décidé de compléter son étude de 2006 relative à la protection des données de carte dans la filière de personnalisation par une étude de la sécurité des dispositifs d'« émission immédiate » de cartes de paiement en agence ou en magasin.

Les opérations de personnalisation, qui consistent à enregistrer sur les cartes vierges les informations permettant leur utilisation par les porteurs, sont le plus souvent effectuées dans des ateliers de personnalisation, qui traitent des volumes industriels de données et de supports cartes, et dont l'étude menée en 2006 avait montré qu'ils mettaient en œuvre des mesures de sécurité permettant d'assurer la protection physique et logique de ces éléments sensibles. Toutefois, afin de répondre avec une plus grande réactivité aux besoins des clients, certains émetteurs mettent en place des pratiques dites d'« émission immédiate » (ou *instant issuing*), consistant à personnaliser les cartes au moment de leur mise à disposition des porteurs. Le fait de nouer la relation contractuelle avec le client directement sur le lieu de vente peut en effet permettre à ce dernier de bénéficier immédiatement d'une offre promotionnelle ou d'un crédit pour réaliser un achat.

Le recours à ce type de solution est largement répandu depuis plusieurs années en France chez les émetteurs de cartes de type « privatif », pour lesquels cela peut représenter une part importante des nouvelles émissions de carte. Elle se développe désormais chez les émetteurs de cartes de type « interbancaire » de réseaux internationaux (MasterCard, Visa). Le Groupement des Cartes Bancaires « CB » travaille également à l'élaboration de règles spécifiques pour mettre en œuvre des dispositifs d'émission immédiate de manière sécurisée, afin de répondre à la demande de certains de ses membres. Le développement du co-marquage[3] peut en outre amener à ce que les opérations de personnalisation soient réalisées, non plus dans les locaux de l'émetteur, mais dans ceux du partenaire commercial.

L'Observatoire a donc souhaité étudier si le niveau de sécurité des solutions d'émission immédiate était équivalent à celui de la personnalisation réalisée en atelier. Pour ce faire, il a recueilli les informations utiles sur la base d'un questionnaire adressé aux représentants des établissements émetteurs[4], des fabricants et personnalisateurs[5] de cartes ainsi que des prestataires techniques[6] impliqués dans la chaîne de personnalisation.

---

3 Pratique consistant à apposer aux côtés de la marque de l'établissement émetteur de la carte celle d'un ou plusieurs partenaires commerciaux

4 Banque Accord, BNP Paribas Personal Finance (ex-Cetelem), Cofinoga-Laser, Finaref, Groupement des Cartes Bancaires « CB », S2P

5 Association des Fabricants et Personnalisateurs de Cartes (AFPC), Giesecke & Devrient

6 ATOS, Monext

L'étude porte sur les risques liés aux activités d'émission immédiate, ainsi que sur les mesures de sécurité mises en œuvre pour se prémunir contre ces risques, à chaque étape de la réalisation de ces activités.

1 | 1 Description de l'émission immédiate

Les opérations d'émission immédiate

Le processus d'émission immédiate de cartes de paiement se compose généralement des étapes suivantes :

- **le recueil des données du client** : le client qui souhaite souscrire à une offre de carte de paiement, en agence bancaire ou auprès d'une enseigne commerciale partenaire de l'émetteur, communique les informations personnelles nécessaires à l'émission de cette carte ;
- **la préparation des données de la carte** : après validation de la demande, les données propres à la carte (numéro de la carte, cryptogramme visuel, clés cryptographiques, code confidentiel) sont générées à partir des informations du porteur, puis transmises au serveur d'émission immédiate, qui prépare les données figurant sur la piste et/ou la puce ;
- **la personnalisation de la carte et sa mise à disposition du client** : les données préparées sont envoyées vers un équipement de personnalisation, situé dans l'agence ou le magasin. Une fois personnalisée, la carte est activée par l'émetteur et remise directement au porteur, qui peut ainsi l'utiliser immédiatement.

Ces étapes se concrétisent par un certain nombre de tâches et d'échanges d'informations, entre différents environnements : l'espace d'accueil de la clientèle, situé en agence ou en magasin, le système de gestion de cartes de l'émetteur, ainsi qu'un serveur d'émission immédiate, pouvant être hébergé chez l'émetteur ou chez un prestataire technique. Ces tâches sont effectuées sur plusieurs types de matériels mis en réseau : PC, serveurs, équipements de personnalisation (voir Encadré 1).

Les données traitées et produites dans le processus d'émission immédiate

Les données recueillies et traitées dans le cadre de l'espace d'accueil de la clientèle comportent les éléments d'identification du porteur (nom, prénom, adresse), voire le code PIN qu'il a pu être autorisé à choisir lui-même, ainsi que des informations relatives à la carte à fabriquer (type de carte, type de visuel associé le cas échéant) et à ses modalités d'usage (retrait et/ou paiement, autorisation systématique, plafonds d'usage, etc.)

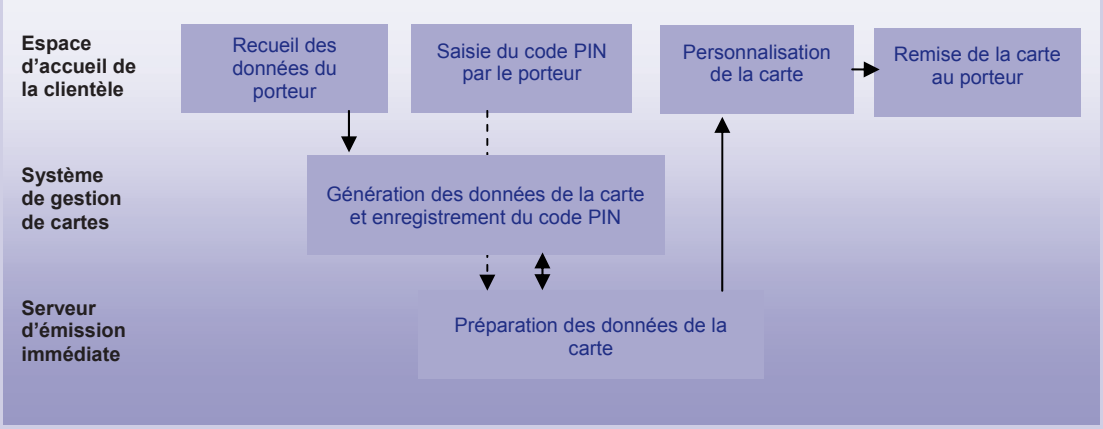
Le système d'information de l'émetteur génère un numéro de carte et une date de validité qu'il envoie au système de gestion de cartes de l'émetteur.

Sur la base de ces informations, le système de gestion de cartes de l'émetteur et le serveur d'émission immédiate traitent et génèrent un ensemble de données supplémentaires, comprenant :

- des données sensibles (données d'encodage de la piste magnétique et/ou préparation des données EMV et des clés et cryptogrammes associés) : ces données, nécessaires à tout processus de personnalisation de carte, sont générées à partir des clés de l'émetteur dans des enceintes cryptographiques ;

– des données de gestion administrative et de contrôle des équipements et des opérations (gestion des autorisations et des accès aux systèmes, commandes envoyées vers l'équipement de personnalisation en agence, éléments de traçabilité, etc.).

Encadré 1 – Actions mises en œuvre dans le cadre de l'émission immédiate



Une émission immédiate de carte se déroule généralement de la façon suivante :

– Le client se présente dans un espace d'accueil de la clientèle, situé en agence bancaire ou auprès d'une enseigne commerciale partenaire de l'émetteur, où un conseiller procède avec lui à l'ouverture d'un dossier de demande de carte de paiement, celle-ci pouvant par exemple être liée à un crédit. Pour ce faire, le conseiller saisit les informations personnelles du porteur.

– Ces données sont transmises au système d'information de l'émetteur pour validation de la demande et attribution d'un numéro de carte.

– Dès lors que la demande est validée, le conseiller initie l'émission immédiate de la carte au moyen d'une application reliée à un serveur d'émission immédiate dédié, situé chez l'émetteur ou son prestataire technique.

– Les données du porteur recueillies en agence ou en magasin sont envoyées au système de gestion de cartes de l'émetteur.

– Le cas échéant, le code confidentiel (PIN) peut être demandé au client, qui le choisit et le saisit alors en agence ou en magasin.

– Le système de gestion de cartes génère des données propres à la carte et les transmet au serveur d'émission immédiate, qui prépare les données de personnalisation de la carte.

– Le serveur d'émission immédiate envoie les données préparées (piste et/ou puce) vers un équipement de personnalisation situé en agence ou en magasin qui est doté de cartes vierges.

– La carte est personnalisée avec les données du client. Elle est ensuite activée auprès de l'émetteur et remise directement au porteur, en agence ou en magasin. Le porteur peut ainsi l'utiliser immédiatement, alors que lorsque la personnalisation est centralisée, il doit attendre que la carte lui soit acheminée.

1|2 La sécurité des dispositifs d'émission immédiate

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

Des solutions de sécurité assurant un degré de protection des données équivalent à celui atteint dans la filière de personnalisation en atelier doivent donc être déployées par les émetteurs et leurs prestataires techniques.

Cependant, en raison de la nature même de l'émission immédiate, dans laquelle une partie des opérations sensibles s'effectue dans un environnement ouvert à la clientèle et donc plus difficile à sécuriser et à contrôler qu'au sein d'un atelier de personnalisation, les spécialistes interrogés considèrent que des mesures de protection spécifiques doivent être mises en place, afin notamment de se prémunir contre les risques de compromission :

– sur l'espace d'accueil de la clientèle : vol et/ou détournement de données traitées par l'équipement de personnalisation et par les applications utilisées, vol de cartes ou de consommables intervenant dans le processus de personnalisation ;
– sur les canaux de communication reliant le point de vente au serveur d'émission immédiate de l'émetteur ou de son prestataire technique : interception des données sur les réseaux, indisponibilité des équipements et systèmes ;
– lors du transport et de l'utilisation des cartes (vierges ou rejetées), ainsi que des consommables (neufs ou usagés).

Les domaines suivants font ainsi l'objet de mesures de sécurité particulières.

L'espace d'accueil de la clientèle

Un ensemble de dispositions de sécurité est généralement mis en œuvre au niveau de l'espace d'accueil de la clientèle, afin de se prémunir notamment contre les cas de compromission visant les équipements de personnalisation. Des mesures de protection physique, telles que des contrôles d'accès aux locaux, une surveillance permanente et généralisée de ceux-ci (vidéosurveillance, dispositifs d'alarme, gardiennage) sont ainsi communément déployées autour de ces équipements. Par ailleurs, ces derniers sont dans certains cas eux-mêmes protégés par des dispositifs spécifiques (scellement, mise sous clé). Les opérations de maintenance sur ces équipements font aussi l'objet de procédures visant à s'assurer qu'aucun élément sensible n'est détourné à cette occasion (exemple du vol de cartes vierges ou rejetées, de consommables du type ruban d'embossage ou d'impression des cryptogrammes visuels).

Afin de protéger l'accès aux applications de validation de demande de carte et de demande de fabrication de carte en émission immédiate, des mécanismes d'authentification sont le plus souvent mis en place afin de se prémunir contre l'usurpation d'identité d'un conseiller. L'attribution de droits restreints sur ces applications permet également d'empêcher un certain nombre d'actes frauduleux, tels que par exemple la production de fausses cartes non reliées à un dossier client, ou encore de doublons, c'est-à-dire de cartes pointant sur un même dossier. Le risque d'interception des données du client, notamment de son code confidentiel lorsque celui-ci est saisi sur le point de vente, peut faire aussi l'objet de mesures spécifiques, telles que l'utilisation de terminaux sécurisés reliés au poste du conseiller. Enfin, des dispositifs

redondants des serveurs applicatifs sont généralement déployés, afin de pallier d'éventuelles indisponibilités des applications.

Ces mesures de sécurité physique et logique sur les sites où sont réalisées les opérations d'émission immédiate peuvent par ailleurs faire l'objet de clauses d'audit dans les contrats liant les émetteurs et leurs partenaires commerciaux.

Les canaux de communication

Afin de se prémunir contre les interceptions de données sur les réseaux reliant les espaces d'accueil de la clientèle aux serveurs des émetteurs ou de leurs prestataires techniques, des liens sécurisés du type réseaux privés virtuels (VPN - *Virtual Private Network*)[7] ou des solutions de chiffrement applicatives reposant sur le protocole de sécurisation SSLv3 (*Secure Socket Layer* version 3)[8] sont habituellement déployés. Pour les données les plus sensibles (PIN), un chiffrement de bout en bout est généralement assuré. Enfin, des solutions de filtrage sont habituellement mises en œuvre pour protéger l'accès aux serveurs d'application mis en réseau, ce qui permet ainsi d'empêcher des tentatives de prise de contrôle des équipements à distance.

Les cartes et les consommables

De même que sur l'espace d'accueil de la clientèle, les cartes et les consommables font l'objet de dispositions et procédures particulières visant à en empêcher le vol ou le détournement lors de leur transport vers et depuis l'espace d'accueil de la clientèle, en utilisant par exemple des transporteurs spécialisés (convoyeurs de fonds) ou des mécanismes d'envoi sécurisé.

De plus, des mesures de protection physique sont le plus souvent utilisées pour protéger les lots de cartes vierges ou rejetées, telles que des coffres ou des enceintes sécurisées directement installées dans les équipements de personnalisation sur le point de vente. Il en est de même pour les consommables (rubans d'embossage ou d'impression des cryptogrammes visuels) utilisés dans ces équipements.

Enfin, les cartes rejetées et les consommables usagés sont détruits de manière sûre, en suivant par exemple une procédure impliquant seulement du personnel autorisé.

On notera que des éléments de traçabilité (automatisés sur les systèmes d'information et équipements impliqués, ou intégrés aux procédures opérationnelles) garantissent un contrôle de bout en bout de l'ensemble de ces opérations sensibles.

L'environnement de l'émetteur

L'ensemble des mesures de sécurité physique et logique mises en œuvre au niveau de l'espace d'accueil de la clientèle, des canaux de communication et des cartes et consommables fait l'objet de recommandations que les réseaux internationaux (Visa, MasterCard) appliquent aux émetteurs et à leurs prestataires techniques. Le Groupement des Cartes Bancaires « CB » travaille également à l'élaboration d'exigences de sécurité dans le domaine de l'émission immédiate.

---

7 L'utilisation de VPN consiste à créer un réseau cloisonné par un processus logique, en utilisant une technique de « tunnel ».

8 Le protocole SSLv3 permet une sécurisation au niveau applicatif.

Les préconisations de ces réseaux en termes de sécurité et d'organisation sont en grande partie inspirées de ce qui existe pour la personnalisation en atelier (protection des données sensibles, traçabilité, etc.) et sont adaptées à l'émission immédiate (équipements de personnalisation distants à sécuriser, contrôle des accès sur ces équipements, protection des réseaux de communication, etc.). Ces recommandations et exigences sont naturellement amenées à évoluer en fonction des pratiques et des besoins identifiés sur le marché.

1|3 Conclusion

Les opérations de personnalisation, qui présentent un haut niveau de sensibilité, sont par nature plus difficiles à sécuriser lorsqu'elles sont réalisées auprès d'un grand nombre de points de vente (agences ou magasins), accessibles à un large public, que lorsqu'elles sont effectuées dans des ateliers de personnalisation, qui traitent des volumes industriels et disposent d'importants moyens de sécurité.

Selon les informations recueillies par l'Observatoire auprès des représentants des établissements émetteurs, des fabricants et personnalisateurs de cartes et des prestataires techniques, les mesures de sécurité physique et logique mises en œuvre lors des différentes phases d'émission immédiate permettent de couvrir de manière satisfaisante les risques liés à ces activités. Ces mesures seront encore amenées à évoluer à mesure du développement de ce type de personnalisation pour les cartes de type « interbancaire », afin de prendre en compte le contexte particulier de la protection des données sensibles de la puce.

Selon les spécialistes interrogés, aucun cas de compromission n'a été relevé à ce jour concernant les dispositifs d'émission immédiate déployés. L'Observatoire invite toutefois les différents acteurs concernés à demeurer très attentifs à la sécurité de ces dispositifs et à ajuster en permanence le niveau de sécurité mis en œuvre en fonction de l'évolution des risques constatée.

2 | STATISTIQUES DE FRAUDE POUR 2008

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 et reprises en annexe D du présent rapport. Une synthèse des statistiques pour 2008 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou retrait) et l'origine de la fraude (carte perdue ou volée, carte non parvenue, carte altérée ou contrefaite, numéro de carte usurpé). En complément, une série d'indicateurs détaillés est présentée dans l'annexe C de ce rapport.

Encadré 2 – Statistiques de fraude : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire recueille les données de l'ensemble des émetteurs de cartes, de type « interbancaire » ou « privatif ». Il complète ces données par des statistiques établies par la Fédération du e-commerce et de la vente à distance (Fevad), qui consulte un échantillon de 33 entreprises représentant 38 % du chiffre d'affaires de la vente à distance aux particuliers.

Les statistiques calculées par l'Observatoire portent ainsi sur :

– 412,9 milliards d'euros de transactions réalisées en France et à l'étranger à l'aide de 58,2 millions de cartes de type « interbancaire » émises en France (dont 1,3 million de porte-monnaie électroniques) ;

– 26,8 milliards d'euros de transactions réalisées (principalement en France) avec 27,2 millions de cartes de type « privatif » émises en France ;

– 24,4 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.

Les données recueillies proviennent :

– de dix émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;

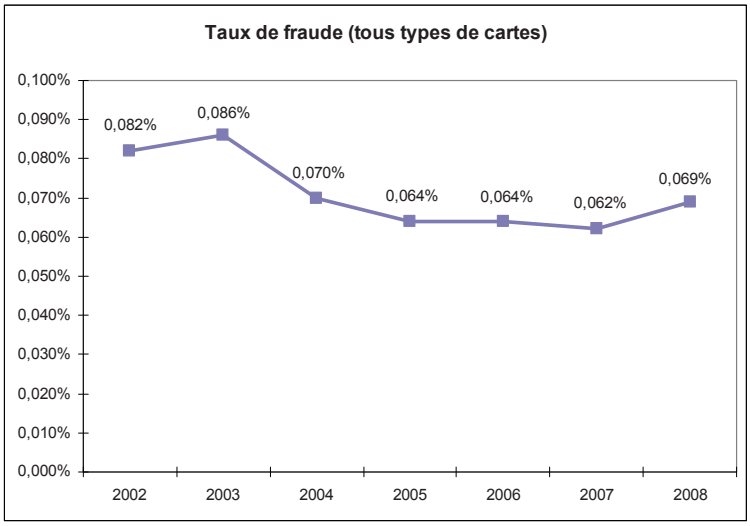
– des 146 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et du Groupement Carte Bleue pour les données internationales ;

– des émetteurs du porte-monnaie électronique Moneo.

2|1 Vue d'ensemble

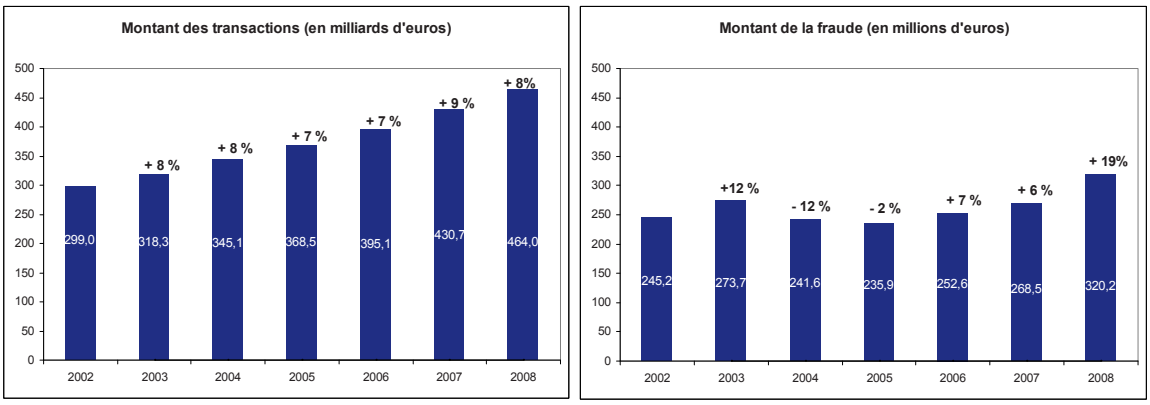
Le taux de fraude sur les paiements et les retraits par carte enregistré en 2008 dans les systèmes français est de 0,069 %. Il est en augmentation comparé à celui des années précédentes (0,062 % en 2007 et 0,064 % en 2005 et 2006 - voir Tableau 1). En effet, la progression des montants de fraude (320,2 millions d'euros en 2008 contre 268,5 millions d'euros en 2007, soit une hausse de 19,3 %) est plus importante que la croissance du montant

des transactions (464,0 milliards d'euros en 2008 contre 430,7 milliards d'euros en 2007, soit une hausse de 7,7 % – voir Tableau 2). Le montant moyen d'une transaction frauduleuse est stable, à 131 euros contre 130 euros en 2007.



Source : Observatoire de la sécurité des cartes de paiement

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



Source : Observatoire de la sécurité des cartes de paiement

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

On observe une augmentation du taux de la fraude émetteur – c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France. Il s'établit en 2008 à 0,057 %, pour un montant de fraude de 249,2 millions d'euros (contre 0,049 % et 199,8 millions d'euros en 2007).

Le taux de la fraude acquéreur – c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France quelle que soit l'origine géographique de la carte – est en légère diminution. Il s'établit en 2008 à 0,045 %, pour un montant de fraude de 201,9 millions d'euros (contre 0,044 % en 2007, pour un montant de fraude de 183,2 millions d'euros).

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

2|2 Répartition de la fraude par type de carte

	Taux de fraude (Montant de la fraude en millions d'euros)				
	2004	**2005**	**2006**	**2007**	**2008**
Cartes de type « interbancaire »	0,069 % (224,1)	0,064 % (218,8)	0,065 % (237,0)	**0,063 %** (253,6)	**0,070 %** (304,3)
Cartes de type « privatif »	0,082 % (17,5)	0,067 % (17,1)	0,052 % (15,6)	**0,052 %** (15,0)	**0,054 %** (16,0)
Total	0,070 % (241,6)	0,064 % (235,9)	0,064 % (252,6)	**0,062 %** (268,5)	**0,069 %** (320,2)

Source : Observatoire de la sécurité des cartes de paiement

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

Pour les cartes de type « interbancaire », le taux de fraude est en hausse en 2008, et s'établit à 0,070 %, pour un montant de fraude de 304,3 millions d'euros (contre 0,063 % en 2007, pour un montant de fraude de 253,6 millions d'euros). Pour ce type de carte, les taux de fraude émetteur et acquéreur sont respectivement de 0,057 % et de 0,046 % (contre 0,049 % et 0,044 % en 2007). La valeur moyenne d'une transaction frauduleuse est de 127 euros, contre 125 euros en 2007.

Pour les cartes de type « privatif », le taux de fraude n'augmente que légèrement, à 0,054 %, pour un montant de fraude de 16,0 millions d'euros (contre 0,052 % et 15,0 millions d'euros en 2007). Pour ce type de cartes, les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,046 % et à 0,042 % (contre 0,044 % et 0,046 % en 2007). La valeur moyenne d'une transaction frauduleuse s'élève à 357 euros en 2008, contre 432 euros en 2007.

2|3 Répartition de la fraude par zone géographique

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

	2004	2005	2006	2007	2008
Transactions nationales	**0,033 % (103,9)**	**0,029 % (97,8)**	**0,031 % (109,6)**	**0,029 % (114,5)**	**0,031 % (130,9)**
Transactions internationales	**0,417 % (137,7)**	**0,408 % (138,1)**	**0,362 % (143,0)**	**0,368 % (154,0)**	**0,427 % (189,4)**
Dont émetteur français et acquéreur étranger	0,463 % (55,2)	0,458 % (64,1)	0,453 % (76,4)	0,476 % (85,3)	0,594 % (118,3)
Dont émetteur étranger et acquéreur français	0,391 % (82,5)	0,373 % (74,1)	0,295 % (66,5)	0,288 % (68,7)	0,291 % (71,0)
Total	**0,070 % (241,6)**	**0,064 % (235,9)**	**0,064 % (252,6)**	**0,062 % (268,5)**	**0,069 % (320,2)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 4 – **Répartition de la fraude par zone géographique**

La répartition de la fraude par zone géographique demeure marquée par un déséquilibre entre les transactions nationales et internationales : 59 % de la fraude portent sur les transactions internationales, alors que ce type de transaction compte à peine pour 10 % de la valeur des transactions par carte enregistrées dans les systèmes français.

Dans un contexte de croissance soutenue du montant des transactions nationales (+ 7,9 %), le taux de fraude de celles-ci est en légère hausse, mais demeure à un niveau très faible, à 0,031 % en 2008, contre 0,029 % en 2007.

La fraude sur les transactions internationales augmente pour sa part en 2008, à la fois en taux et en montant. Le taux de fraude liée aux transactions effectuées à l'étranger avec des cartes émises en France augmente nettement et s'établit à 0,594 %, pour un montant de fraude de 118,3 millions d'euros (contre 0,476 % en 2007, pour un montant de fraude de 85,3 millions d'euros). Le taux de fraude liée aux transactions effectuées en France avec des cartes émises à l'étranger est en légère hausse et s'établit à 0,291 %, pour un montant de fraude de 71,0 millions d'euros (contre 0,288 % en 2007, pour un montant de fraude de 68,7 millions d'euros).

Encadré 3 – Répartition du préjudice de la fraude

L'Observatoire a pu, en 2008 comme en 2007, estimer, pour l'ensemble des systèmes de type « privatif » et de type « interbancaire », des indicateurs de la répartition du préjudice de la fraude entre le porteur, le commerçant et leurs banques. Il est important de noter que ces indicateurs ne valent que pour le préjudice lui-même, et non pour les coûts totaux de traitement ou d'assurance engendrés par la fraude. Ces indicateurs donnent une tendance mais restent théoriques et ne peuvent refléter que la répartition directe de la fraude supportée par les acteurs. Par construction en effet, ils se réfèrent aux dispositions légales et réglementaires encadrant l'opposition par le porteur en cas de perte ou de vol, ainsi que la contestation par celui-ci en cas d'utilisation frauduleuse de sa carte. De plus, ils ne peuvent tenir compte totalement des pratiques commerciales des émetteurs ou des acquéreurs.

Tous systèmes confondus, la répartition du préjudice pour les transactions nationales en 2008 est la suivante : 2,6 % sont supportés par les porteurs, 43,9 % sont supportés par les établissements émetteurs et acquéreurs et 53,5 % sont supportés par les commerçants, principalement en vente à distance. La part supportée par les commerçants, qui était de 46 % en 2007, augmente de façon significative du fait de la croissance de la fraude sur les paiements à distance, qui est très majoritairement supportée par les commerçants.

De plus, sur les 320,2 millions d'euros de fraude enregistrés par les systèmes français en 2008, on peut estimer qu'environ 96,0 millions d'euros (soit 30 %) seraient supportés par les systèmes étrangers. Ceci découle de l'application des règles internationales de partage de responsabilité dans le cadre de la mise en œuvre du standard EMV et du dispositif d'authentification pour les paiements à distance « 3D-Secure ».

2|4 Répartition de la fraude par type de transaction

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

Transactions nationales

	Taux de fraude (Montant de la fraude en millions d'euros)				
Transactions nationales	**2004**	**2005**	**2006**	**2007**	**2008**
Paiements	**0,036 % (81,2)**	**0,033 % (82,8)**	**0,035 % (92,3)**	**0,032 % (95,6)**	**0,036 % (111,7)**
- dont paiements de proximité et sur automate	0,029 % (63,5)	0,025 % (59,2)	0,024 % (59,1)	0,017 % (45,4)	0,015 % (44,5)
- dont paiements à distance	0,177 % (17,7)	0,196 % (23,6)	0,199 % (33,2)	0,236 % (50,1)	0,252 % (67,2)
- dont par courrier / téléphone	nd	nd	0,194 % (19,8)	0,201 % (23,8)	0,280 % (28,5)
- dont sur Internet	nd	nd	0,208 % (13,4)	0,281 % (26,4)	0,235 % (38,8)
Retraits	**0,027 % (22,7)**	**0,017 % (15,0)**	**0,019 % (17,4)**	**0,020 % (19,0)**	**0,018 % (19,1)**
Total	**0,033 % (103,9)**	**0,029 % (97,8)**	**0,031 % (109,6)**	**0,029 % (114,5)**	**0,031 % (130,9)**

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 5 – **Répartition de la fraude nationale par type de transaction**

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

– le taux de fraude sur les paiements de proximité et sur automate continue de diminuer et s'établit à 0,015 %, pour un montant de fraude de 44,5 millions d'euros (contre 0,017 % en 2007 et 45,4 millions d'euros). Ceci témoigne du renforcement des mécanismes cryptographiques opéré depuis plusieurs années. Les paiements de proximité et sur automate comptent pour 69 % des transactions nationales, et pour 34 % du montant de la fraude.

– le taux de fraude sur les paiements à distance est en hausse en 2008 et s'établit à 0,252 % pour un montant de fraude de 67,2 millions d'euros (contre 0,236 % en 2007, pour un montant de fraude de 50,1 millions d'euros). Les paiements à distance, qui représentent 6 % de la valeur des transactions nationales, comptent ainsi désormais pour 51 % du montant de la fraude. Cette hausse de la fraude est à relativiser compte tenu de la croissance très dynamique du volume et de la valeur des paiements à distance (+ 25,6 % entre 2007 et 2008).

  L'observation comparée des évolutions pour les paiements par courrier / téléphone et sur Internet montre une inversion de tendance entre ces deux canaux. La fraude augmente plus fortement pour les paiements sur Internet que pour ceux effectués par courrier ou téléphone (+ 47,0 % contre + 19,7 %), mais le taux de fraude enregistré pour les transactions par courrier / téléphone devient supérieur compte tenu de la nette baisse du montant de ces transactions (- 14,0 %). La croissance du montant des paiements sur Internet étant supérieure à celle de la fraude, le taux de fraude des transactions sur Internet diminue à 0,235 % (contre 0,281 % en 2007).

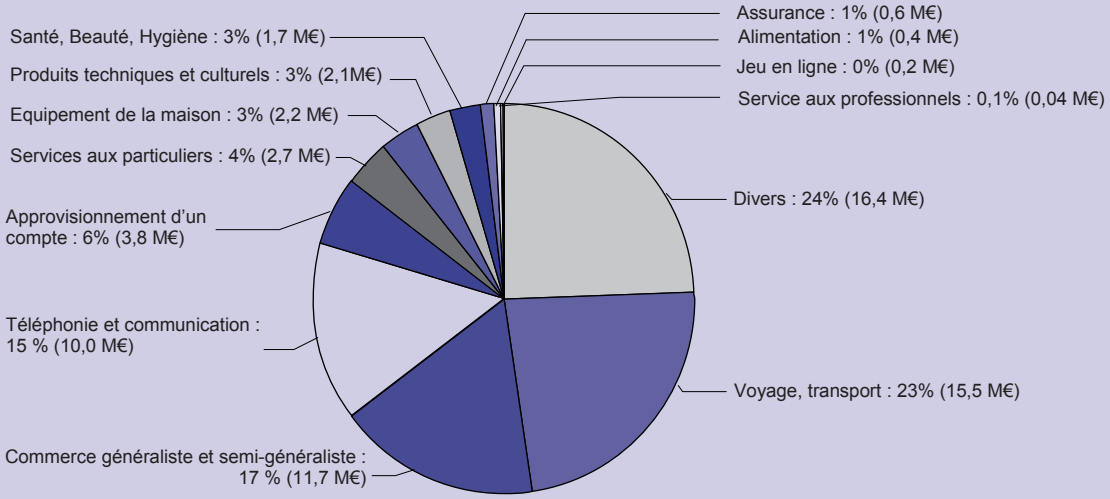
  Les analyses statistiques menées par la Fédération du e-commerce et de la vente à distance (Fevad) confirment sur ce point les données collectées par le Groupement des Cartes Bancaires « CB ».

  L'Observatoire est attentif à l'évolution de la fraude sur les paiements à distance. Une étude des solutions de sécurité mises en œuvre figure au chapitre 3 du présent rapport.

– le taux de fraude sur les retraits diminue à seulement 0,018 %, pour un montant de fraude de 19,1 millions d'euros (contre 0,020 % en 2007, pour un montant de fraude de 19,0 millions d'euros). Les retraits représentent 25 % des transactions nationales et comptent pour 15 % du montant de la fraude.

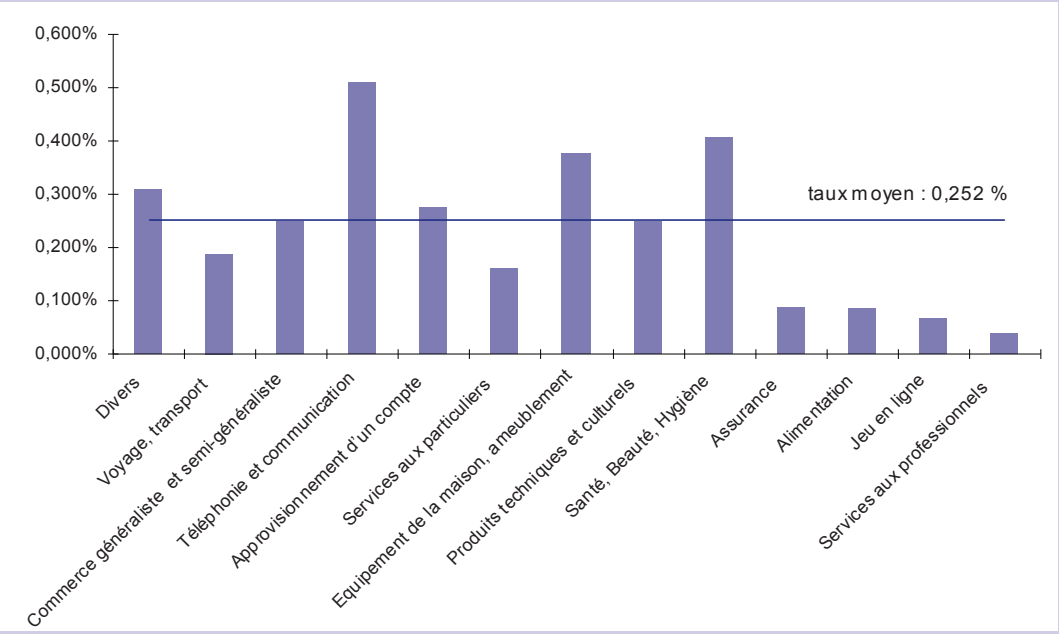
Encadré 4 – Fraude nationale en vente à distance selon le secteur d'activité

Pour la première fois cette année, l'Observatoire a collecté des données permettant de fournir des indications sur la segmentation de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions nationales.



Ventilation de la fraude sur les paiements à distance par secteur d'activité pour les transactions nationales (montant de la fraude en millions d'euros)

Les secteurs Voyage / transport, Commerce généraliste et semi-généraliste et Téléphonie / communication représentent 55 % de la fraude, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Santé / beauté / hygiène, Equipement de la maison / ameublement) (cf. histogramme ci-après). Néanmoins, l'Observatoire remarque qu'au sein d'un même secteur, le taux de fraude varie sensiblement d'un commerçant à l'autre selon les mesures de sécurité déployées.



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

Source : Observatoire de la sécurité des cartes de paiement

Transactions internationales

	Taux de fraude (Montant de la fraude en millions d'euros)		
Émetteur français – Acquéreur étranger	**2006**	**2007**	**2008**
Paiements	**0,421 % (54,0)**	**0,483 % (65,2)**	**0,655 % (99,3)**
- dont paiements de proximité et sur automate	0,288 % (28,1)	0,299 % (30,0)	0,286 % (32,0)
- dont paiements à distance	0,840 % (26,0)	1,024 % (35,1)	1,698 % (67,2)
- dont par courrier / téléphone	0,684 % (5,7)	0,790 % (7,6)	1,284 % (11,2)
- dont sur Internet	0,898 % (20,3)	1,117 % (27,4)	1,815 % (56,0)
Retraits	**0,555 % (22,4)**	**0,455 % (20,0)**	**0,399 % (19,1)**
Total	**0,453 % (76,4)**	**0,476 % (85,3)**	**0,594 % (118,3)**
Émetteur étranger – Acquéreur français	**2006**	**2007**	**2008**
Paiements	**0,344 % (61,5)**	**0,334 % (62,8)**	**0,339 % (65,4)**
Retraits	**0,107 % (5,0)**	**0,117 % (5,9)**	**0,110 % (5,6)**
Total	**0,295 % (66,5)**	**0,288 % (68,7)**	**0,291 % (71,0)**

Source : Observatoire de la sécurité des cartes de paiement

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

En ce qui concerne les transactions internationales, l'Observatoire ne dispose d'une décomposition fine de la fraude par type de transaction que pour les seules transactions réalisées par des cartes françaises à l'étranger. La principale observation relative à ces transactions réside dans l'augmentation très nette de la fraude pour les paiements à distance (+ 91,5 %, soit un montant de fraude de 67,2 millions d'euros). Le taux de fraude pour ces paiements atteint le niveau de 1,698 %, ce qui est le taux le plus élevé jamais relevé par l'Observatoire. Cette évolution significative renforce l'importance de la mise en œuvre de mesures de sécurité permettant de s'assurer que c'est bien le porteur légitime de la carte qui est à l'origine du paiement.

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 ;

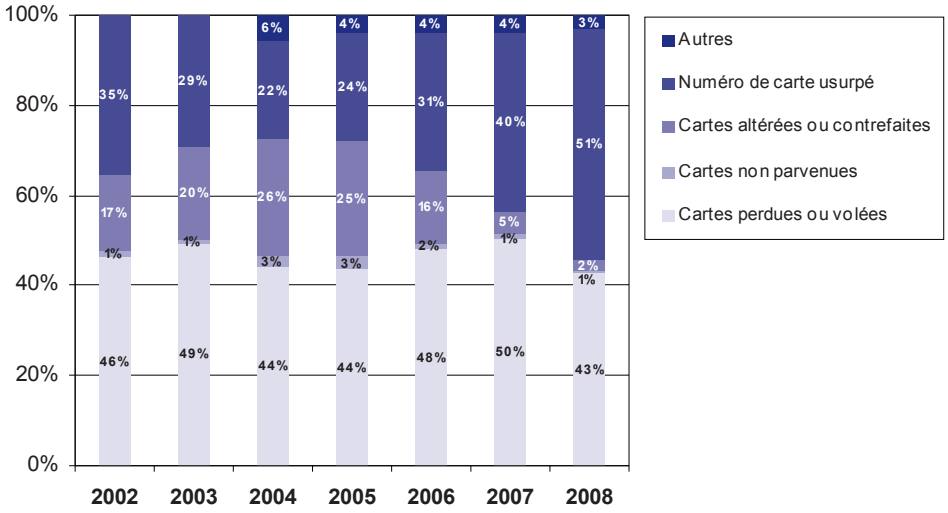
– carte non parvenue : la carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;

– 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 dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements).



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 7 – **Répartition de la fraude selon son origine (transactions nationales, en valeur)**

En augmentation depuis 2005, l'origine de fraude la plus importante (51,3 %, contre près de 40 % en 2007) est désormais celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance. La fraude liée aux pertes et vols de cartes représente encore 42,6 % des paiements nationaux frauduleux. La contrefaçon de cartes n'est plus à l'origine que de 2,4 % des paiements nationaux frauduleux (contre 5 % en 2007 et 16 % en 2006). Enfin, on observe une stabilité de la rubrique « autres », qui est généralement utilisée par les systèmes de carte de type « privatif » pour indiquer les fraudes par ouverture frauduleuse d'un compte ou d'un dossier de crédit (fausse identité) et qui est très significative pour ce type de carte (près de 50 %).

2008	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	55,8	42,6 %	53,4	43,4 %	2,4	30,1 %
Carte non parvenue	0,9	0,7 %	0,3	0,3 %	0,6	6,9 %
Carte altérée ou contrefaite	3,1	2,4 %	2,6	2,1 %	0,5	6,5 %
Numéro usurpé	67,2	51,3 %	66,6	54,2 %	0,6	7,9 %
Autres	3,9	2,9 %	-	-	3,9	48,6 %
Total	**130,9**	**100 %**	**122,9**	**100 %**	**7,9**	**100 %**

Source : Observatoire de la sécurité des cartes de paiement

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

Encadré 5 – Indicateurs des services de police et de gendarmerie

Pour l'année 2008, les services de police et de gendarmerie enregistrent une légère baisse des cas recensés en matière de fraude relative aux cartes de paiement. 54 058 faits de falsification et usage de cartes de paiement ont été constatés, et 3 719 individus ont été mis en cause, motivant 1 430 mesures de garde en vue.

Les attaques de distributeurs automatiques de billets (DAB) augmentent avec 427 piratages de DAB en 2008 (contre 391 en 2007, 515 en 2006, 200 en 2005, et 80 en 2004). A celles-ci s'ajoutent 3 attaques de distributeurs automatiques de carburant (DAC) (contre 36 en 2007) et 17 attaques de terminaux de paiement.

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

– l'interpellation d'une équipe de neuf personnes spécialisée dans la captation de données de carte, la contrefaçon et l'utilisation de cartes en France et dans plusieurs pays européens. Le préjudice est estimé à plus de 500 000 euros ;

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

Les autorités françaises ont continué en 2008 à coopérer étroitement avec leurs homologues européens, notamment des pays de l'Est. Cette démarche a conduit à des actions concrètes qui ont permis le démantèlement d'ateliers clandestins en France mais aussi en Roumanie. Cela s'avère nécessaire pour lutter efficacement contre la fraude devant l'essor des groupes organisés et de la criminalité transfrontalière.

3 | VEILLE TECHNOLOGIQUE

3|1 Solutions de sécurité pour le paiement à distance

La vente à distance, entendue au sens large, c'est-à-dire par Internet, courrier ou téléphone (*Mail Order / Telephone Order* – MO/TO), a connu ces dernières années en France une forte croissance, tirée notamment par la progression du commerce par Internet (ou commerce électronique). En effet, les ventes en ligne ont progressé en montant de 25 % en 2008 selon la Fédération du e-commerce et de la vente à distance (Fevad). Dans le même temps, la carte de paiement est devenue le moyen de paiement majoritairement utilisé pour régler les achats en vente à distance, avec 85 % des paiements en 2008[9].

Compte tenu de la spécificité des mesures de sécurité mises en œuvre dans le cadre des paiements à distance par rapport aux paiements de proximité, ainsi que de la différence des taux de fraude relevés dans les statistiques de l'Observatoire sur ces deux situations de paiement, l'Observatoire a souhaité examiner les solutions de sécurité mises en œuvre dans le cadre du paiement à distance, initié par Internet, par courrier ou par téléphone.

Les caractéristiques sécuritaires du paiement à distance

Les transactions de paiement par carte à distance présentent, au niveau des contrôles effectués, des caractéristiques très différentes de celles du paiement de proximité.

En effet, la grande majorité des paiements à distance actuels se basent exclusivement sur la fourniture d'un ensemble de données statiques et donc rejouables : le numéro de la carte (PAN – *Primary Account Number*), sa date de validité, le cryptogramme visuel CVx2 (« Card Verification Value 2 » pour Visa, « Card Verification Code 2 » pour Mastercard) ; l'opération de paiement n'est, en règle générale, pas associée à une authentification du porteur.

Ces données peuvent donc avoir été interceptées par un tiers ou être détournées par un employé indélicat d'un intervenant de la chaîne de paiement. D'autre part, le porteur peut contester avoir autorisé les paiements.

De plus, l'opération de paiement à distance ne fait généralement pas l'objet d'une authentification certaine et d'un recueil de la preuve du consentement donné par le porteur. Le marchand peut donc facturer plus que le montant convenu, et le porteur peut contester avoir donné son accord pour le montant débité.

Toutefois, les commerçants et prestataires de service sont en mesure de s'assurer que la carte n'a pas été signalée comme perdue ou volée et que le plafond de paiement n'est pas dépassé.

Une fois reçu l'ordre de paiement, que ce soit par Internet, courrier ou téléphone ou, le commerçant enregistre généralement les données de carte dans son système d'information.

9 Source : Fevad

Pour se prémunir contre les risques de vol de ces fichiers cartes, tels que ceux intervenus ces dernières années, principalement aux Etats-Unis, ces fichiers doivent faire l'objet de protections adaptées.

Il résulte des limites des contrôles effectués pour les paiements par carte à distance que le taux de fraude dans ces paiements est nettement supérieur à celui sur les paiements de proximité et sur automate : en 2008, ce taux s'établit à 0,252 % contre 0,015 % pour les paiements de proximité et sur automate. Associé à la progression des paiements à distance, cela entraîne une augmentation importante du montant de la fraude sur les paiements à distance, qui s'élève en 2008 à 67,2 millions d'euros, contre 50,1 millions d'euros en 2007. Ainsi, les paiements à distance, qui représentent 6 % de la valeur des transactions nationales, comptent désormais pour 51 % du montant de la fraude.

Les solutions de sécurité

Détection des transactions suspectes et assurance

Pour lutter contre la fraude, les commerçants et les banques ont de plus en plus recours à des systèmes permettant de détecter les transactions suspectes et d'effectuer des vérifications supplémentaires ou de refuser certaines transactions. Ces systèmes, déclarés à la CNIL, se fondent sur une analyse du comportement du client, du lieu d'origine de la commande et une comparaison de ses achats auprès de plusieurs commerçants pour déterminer la probabilité qu'une transaction soit frauduleuse. Ils ont pu être adaptés pour prendre en compte l'utilisation de numéros de cartes dynamiques.

Ces systèmes peuvent être complétés par des solutions d'assurance ou de garantie. Le porteur est quant à lui protégé par la loi en cas d'utilisation frauduleuse de son numéro de carte. Il peut également souscrire à des assurances le protégeant contre les défauts éventuels de livraison.

Protection contre le vol de données de carte statiques

Tant que le paiement à distance continuera d'être possible au moyen des données statiques mentionnées ci-dessus, il sera nécessaire d'assurer la confidentialité de ces données. Ces données peuvent être capturées et détournées à plusieurs endroits : lors de leur transmission ou pendant leur stockage dans des bases de données ou, pour les transactions sur Internet, sur les postes informatiques des porteurs.

La capture de données de carte lors de leur transmission est réalisable quel que soit le mode de communication utilisé, Internet, courrier ou téléphone, mais elle est essentiellement problématique sur Internet, où une capture automatisée et donc aisée d'un nombre important de données serait possible. C'est pourquoi ces informations sont toujours transmises au moyen d'un protocole sécurisé comme HTTPS. Ce protocole est adopté depuis de nombreuses années par l'ensemble des commerçants en ligne et remplit correctement son rôle. Sa seule faiblesse est que sa sécurité dépend de la bonne authentification du site marchand par le client, laquelle peut être mise à mal par diverses tromperies comme le phishing. Une éducation des internautes et un travail sur l'ergonomie permettent une meilleure reconnaissance des sites légitimes et des sites frauduleux. Un exemple de solution est le certificat « Extended Validation Certificate », qui est délivré au site après des contrôles renforcés et indique à l'internaute qu'il se trouve sur un site ayant subi ces vérifications supplémentaires par le biais d'indicateurs visuels (tels que la barre d'adresse en vert).

Le risque de capture de données de carte dans les bases de données des commerçants ou des intermédiaires financiers nécessite un contrôle strict de la sécurité de ces bases. C'est pourquoi un programme comme PCI DSS (*Payment Card Industry - Data Security Standard*) a été adopté par tous les réseaux internationaux de carte pour établir des règles de protection des données liées aux cartes, à leur utilisation et à leur stockage. Il s'applique directement au commerçant ou à l'hébergeur de son système de paiement. Il définit des exigences en matière de sécurité que commerçants et/ou prestataires doivent respecter. L'application du programme est auditée à la demande des réseaux internationaux. En France, ce programme devrait être adapté aux spécificités d'utilisation de la carte à puce.

La capture de données de carte sur les ordinateurs des porteurs se produit de plus en plus couramment, du fait de la contamination croissante des postes par des logiciels espions. Face à cela, des actions sont entreprises pour sensibiliser les porteurs aux bonnes pratiques en matière de sécurité informatique et pour leur fournir des systèmes sûrs.

Utilisation de données de carte dynamiques

Plutôt que de devoir protéger les données de carte contre le vol à cause de leur caractère réutilisable, une autre solution consiste à remplacer ces données statiques par des données dynamiques, à usage unique. Ces numéros sont utilisables aussi bien par Internet que par téléphone ou par courrier.

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

Authentification et consentement du porteur

Pour prévenir directement l'utilisation frauduleuse de données de carte, il est possible de mettre en place des mesures d'authentification du porteur et de validation de son consentement à chaque ordre de paiement.

Dispositifs d'authentification du porteur

Pour les systèmes de paiement par carte de type « interbancaire », le consentement et l'authentification sont assurés en paiement de proximité par la présentation du montant facturé sur écran au porteur, suivie de la saisie par ce dernier de son code PIN, conformément au standard EMV[10]. Cette solution, qui nécessite le recours à un terminal de paiement, n'est pas adaptée au paiement à distance, tant lorsqu'il s'agit de paiements effectués sur des sites marchands français avec des cartes nationales ou étrangères, que lorsqu'il s'agit de paiements avec des cartes françaises sur des sites étrangers.

Aujourd'hui, on constate que la solution d'authentification la plus répandue en vente à distance, par Internet et en MO/TO, est le recours à une information statique (mot de passe, information personnelle comme la date de naissance), solution qui présente l'avantage d'un déploiement simple et peu coûteux et d'une utilisation aisée.

[10] Le contrôle du code confidentiel n'est toutefois pas possible lors des paiements réalisés chez les commerçants français pour les cartes de type « interbancaire » d'origine étrangère qui fonctionnent en mode piste.

Cependant, avec le recours à une authentification du porteur par donnée statique, les paiements par carte à distance restent exposés aux mêmes attaques que précédemment, à savoir par exemple sur Internet la récupération des mots de passe par phishing, logiciels espions, etc. Pour répondre à cette menace, plusieurs solutions techniques sont envisageables et sont proposées ponctuellement par les banques à une partie de leur clientèle, parmi lesquelles :

– l'utilisation de codes à usage unique délivrés au moyen d'une carte papier. Cette solution présente le risque de vol ou de copie de la carte papier, risque qui peut être limité lorsque cette carte permet de composer le code à usage unique à partir de différentes combinaisons connues seulement du porteur ;

– l'utilisation de codes à usage unique générés par un serveur de la banque émettrice et adressés au porteur par téléphone (SMS ou serveur vocal vers poste fixe). Cette solution présente l'avantage d'être multi-canal, puisque le code est envoyé par un autre canal de communication que celui utilisé pour la commande.

– l'utilisation de codes à usage unique délivrés au moyen d'un dispositif matériel. Un exemple de solution de ce type, dédié aux cartes de type « interbancaire », est CAP (*Chip Authentication Protocol*) / DPA (*Dynamic Passcode Authentication*), qui permet la génération d'un code à usage unique par la carte de paiement insérée dans un petit lecteur autonome sur lequel le porteur tape son code PIN. Cette solution présente de plus l'avantage de pouvoir générer des codes liés aux caractéristiques de la transaction à valider, empêchant la manipulation de ces caractéristiques et les contestations ultérieures.

Des travaux sont en cours pour permettre d'utiliser ce type de solutions non seulement par Internet comme c'est possible aujourd'hui, mais aussi en commande par téléphone ou courrier postal.

Architectures de mise en œuvre de l'authentification

Si l'utilisation de dispositifs activés au choix du porteur permet de protéger celui-ci contre l'utilisation illicite de sa carte et d'offrir une garantie supplémentaire aux commerçants pour les achats ainsi protégés, une généralisation du recours à l'authentification des porteurs sur la base de normes d'interopérabilité, contribuerait à améliorer la lutte contre la fraude.

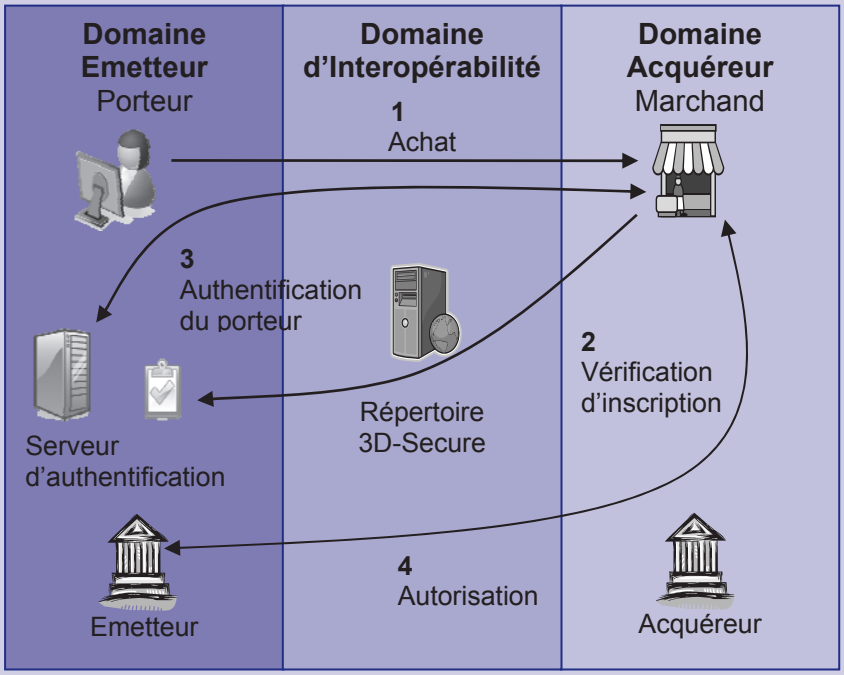
Pour le domaine Internet, les systèmes de paiement par carte de type « interbancaire » ont mis en place une architecture commune, permettant aux commerçants de demander l'authentification des porteurs et aux banques d'acheminer les informations relatives à l'authentification de leurs clients. Un exemple de solution de ce type est « 3D-Secure »[11] qui, à partir de la demande effectuée par le serveur du commerçant, permet de remonter à la banque du porteur, de l'authentifier, de recueillir son accord sur les conditions de réalisation de la transaction (montant, etc.) et d'établir des preuves ou certificats justifiant la transaction effectuée par le client. La méthode d'authentification est à choisir par la banque et peut être commune avec la méthode d'authentification pour la banque en ligne.

Compte tenu du caractère international du réseau Internet, le succès de « 3D-Secure » dépendra de la généralisation de son adoption par les différents systèmes de paiement par carte. En France, « 3D-Secure » est progressivement déployé par les banques acquéreurs membres du Groupement des Cartes Bancaires « CB » auprès de leurs commerçants. Les

[11] « 3D-Secure » est un protocole commun de communication entre le marchand, la banque acquéreur et la banque émettrice. Développé par Visa pour améliorer la sécurité des paiements en ligne, il est offert sous le nom commercial « Verified by Visa ». Des services basés sur ce protocole sont offerts par MasterCard sous le nom « MasterCard SecureCode » et par JCB International sous le nom « J/Secure ».

banques émettrices de ce groupement ont également mis en place des mécanismes d'authentification de leurs porteurs. Depuis le 1er octobre 2008, un transfert de responsabilité est entré en vigueur entre banques du système « CB », qui fait que lorsqu'un commerçant subit un paiement frauduleux alors que la transaction de paiement a été traitée selon le protocole « 3D-Secure » auprès de l'émetteur, c'est ce dernier qui supporte désormais la responsabilité, et non plus l'acquéreur et *in fine* le commerçant.

Encadré 6 – Principe de fonctionnement de 3D-Secure



Conclusion

La fraude sur les paiements à distance est non seulement nettement supérieure à celle sur les paiements de proximité et sur automate, mais elle est également en hausse. C'est pourquoi l'Observatoire a souhaité approfondir l'étude de la sécurité des paiements à distance, dans le prolongement des travaux menés en 2007.

En effet, la spécificité des paiements à distance ne permet pas de leur appliquer directement les solutions de sécurité utilisées pour protéger les paiements de proximité, mais des solutions adaptées au paiement à distance, au moins sur Internet, sont aujourd'hui disponibles et sont employées : numéro de carte dynamique, authentification du porteur par mot de passe, etc.

Cependant, les solutions actuelles ne couvrent pas tous les risques auxquels sont exposés aujourd'hui les paiements à distance, notamment la capture des données de la carte et des données d'authentification statiques. En conséquence, l'Observatoire recommande de renforcer les méthodes de sécurisation, afin d'amener la sécurité des paiements à distance à un niveau équivalent à celui des paiements de proximité et sur automate.

Pour cela, en complément de l'authentification par le porteur du site marchand, l'Observatoire invite à privilégier des méthodes de paiement en vente à distance permettant une authentification du porteur. Il recommande de généraliser progressivement l'authentification du porteur pour tout acte de paiement et de renforcer les méthodes d'authentification utilisées, afin de permettre au commerçant d'être assuré de l'authenticité de la carte et du porteur, ainsi que du consentement de celui-ci. Pour aider à se prémunir contre les risques identifiés, le recours à une authentification non rejouable du porteur est fortement recommandé, chaque fois que cela est possible et pertinent. Diverses solutions techniques sont déjà disponibles : code à usage unique généré par une calculette ou envoyé par SMS, lecteur autonome de carte EMV, etc., dont le choix revient aux systèmes de paiement par carte et à leurs émetteurs. Pour faciliter leur usage, il est important que ces solutions bénéficient d'un coût de déploiement maîtrisé et d'une ergonomie adaptée, et que leur diffusion s'accompagne d'une information et d'une éducation du porteur.

La mise en place de tels systèmes concerne toutes les parties, aussi l'Observatoire incite-t-il l'ensemble des acteurs à s'y impliquer.

3|2 Impacts du co-marquage sur la sécurité des cartes de paiement

Le « co-marquage » des cartes de paiement est une pratique consistant à apposer aux côtés de la marque de l'établissement émetteur de la carte celle d'un ou plusieurs partenaires commerciaux. Le co-marquage doit être distingué du « co-badgeage », qui consiste pour un émetteur à nouer une alliance avec différents réseaux de carte et à faire figurer leurs logotypes sur sa carte (Carte Bancaire, Visa, MasterCard, Moneo, etc.).

Le co-marquage est une pratique ancienne, très développée dans certains pays anglo-saxons où elle a permis le développement de nombreuses offres de cartes dites « affinitaires » en ce qu'elles permettent de toucher une clientèle de porteurs ayant un lien privilégié avec le ou les partenaires commerciaux associés à l'émetteur (réseaux de restaurants, d'hôtels ou de pétroliers par exemple). Déjà existant en France pour les cartes de type « privatif », le co-marquage était resté jusqu'à un passé récent relativement limité car il n'était pas permis au sein du système « CB ». Les établissements membres de « CB » avaient en effet souhaité jusque là attacher un caractère neutre et universel à la carte « CB » et conserver un lien fort entre la carte et sa banque émettrice. Cette interdiction a été levée le 1er octobre 2007, pour aligner les pratiques françaises avec celles des pays voisins dans le cadre de l'ouverture du marché européen des moyens de paiement (*Single Euro Payments Area* – SEPA).

Depuis cette date, les initiatives de nouvelles cartes co-marquées se sont développées, et comprennent désormais une cinquantaine de nouvelles offres de cartes. Celles-ci sont de types variés : cartes de débit auxquelles est ajouté un programme affinitaire, cartes de débit associées à une ligne de crédit à la consommation ou cartes prépayées rechargeables.

Cette évolution nouvelle a pu faire naître des interrogations, notamment de la part des représentants des consommateurs, d'une part sur la confusion possible pour les porteurs entre les fonctions de paiement par débit ou par crédit, mais ceci ne relève pas du champ de compétence de l'Observatoire, et d'autre part sur le maintien par l'établissement émetteur de la maîtrise de la sécurité de ses cartes co-marquées. L'Observatoire a donc souhaité examiner si les nouveautés introduites étaient susceptibles d'avoir un impact en termes de sécurité et si les conditions sécuritaires associées à ces nouvelles offres de cartes de paiement étaient satisfaisantes.

Modifications possibles en termes de sécurité

Le co-marquage est susceptible de modifier les pratiques au cours des différentes étapes du cycle de vie des cartes de paiement. En effet, si le co-marquage implique avant tout une modification du visuel de la carte et des offres affinitaires, le partenaire peut également jouer un rôle actif lors de la souscription de l'offre de carte ou lors de son émission. De plus, le fonctionnement des offres affinitaires implique un partage des données personnelles des clients entre l'émetteur et ses partenaires, et peut se traduire par l'ajout d'applications non bancaires dans la carte.

Souscription

La souscription de la carte par le porteur comprend la fourniture par celui-ci d'un ensemble de données personnelles et bancaires, la vérification de ses pièces justificatives et la signature d'un contrat. Dans le cas des cartes co-marquées, la souscription peut se faire soit auprès de l'émetteur de la carte, soit auprès du partenaire commercial.

Dans le premier cas, les procédures sont identiques à celles d'une souscription de carte non co-marquée. Cependant, les informations personnelles des porteurs et leurs données bancaires peuvent faire l'objet d'un partage entre l'émetteur et les partenaires impliqués, créant potentiellement chez les partenaires des bases de données sensibles qui devraient alors bénéficier d'une protection appropriée.

Une souscription auprès de l'enseigne partenaire implique le transfert à celle-ci du recueil des données personnelles du client. Il importe en conséquence que ces données soient protégées de la même manière que lorsqu'elles sont recueillies dans le domaine bancaire, afin de garantir leur confidentialité, notamment lors de leur conservation ou de leur transmission à l'émetteur ou son prestataire technique. Lorsque l'enseigne partenaire se voit confier tout ou partie de la vérification des données personnelles du client, ces opérations requièrent le même niveau de diligence que celui existant dans l'environnement bancaire afin, notamment, de s'assurer de la véracité des informations collectées.

Emission

Pour la plupart des cartes co-marquées émises aujourd'hui en France, la fabrication et la personnalisation des cartes sont effectuées par l'émetteur ou par son prestataire technique sous sa responsabilité. C'est l'émetteur ou son prestataire agissant pour son compte qui adresse ensuite les cartes directement aux porteurs. Ces opérations de production sont sensibles en termes de sécurité, notamment en raison de l'importance de la protection des données personnelles et des données bancaires lors de la phase de personnalisation. La protection de la carte et des données de sécurité comme le code confidentiel est également particulièrement importante lors de la délivrance de la carte au porteur. L'intervention du partenaire commercial dans la phase d'émission de la carte peut influer sur le déroulement de ces opérations mais, au plan de la sécurité, il est important que les cartes co-marquées, comme toutes les cartes de paiement, suivent un processus d'émission présentant des mesures qui, au final, garantissent le même niveau de sécurité que dans le cas de l'émission de cartes bancaires non co-marquées.

Dans le domaine des cartes de type « privatif », qui sont actuellement en France des cartes à piste, certaines cartes co-marquées sont émises directement sur des lieux de vente (*instant issuing*). Cette pratique est également appelée à se développer dans le cas des cartes de type « interbancaire ». Afin de prévenir tout risque d'obtention illégitime de cartes par des fraudeurs,

des contrôles appropriés sont requis pour encadrer cette opération (voir chapitre 1 du présent rapport).

Utilisation

Le co-marquage permet un usage plus varié des cartes de paiement. Il implique en outre une modification de leur visuel, compte tenu de l'apposition des éléments commerciaux du partenaire de l'émetteur (marque, logotype, éléments de communication). A l'avenir, ce changement de visuel pourrait s'accompagner d'un changement de forme pour le support carte (carte découpée, carte miniaturisée…). Ces évolutions, en donnant à la carte une apparence originale voire ludique, sont susceptibles de modifier la perception du porteur quant à la nature bancaire de son instrument de paiement. Un effort de communication et de sensibilisation est donc nécessaire pour s'assurer que les porteurs sont bien informés qu'ils doivent prendre avec les cartes co-marquées les mêmes précautions qu'avec toute carte de paiement.

D'autre part, ces cartes peuvent aussi être amenées à contenir des applications affinitaires aux côtés des applications bancaires. Il est important que ces applications affinitaires ne compromettent pas la sécurité des applications bancaires et des données associées, ce qui implique de s'assurer qu'elles respectent la politique de sécurité de la carte (par exemple le cloisonnement entre applications).

Mesures sécuritaires

Protection des données bancaires

Il est important que les données de carte (PAN, date d'expiration, CVx2) fassent l'objet, lors de leur stockage et de leur transmission, d'une protection adéquate par l'émetteur et ses partenaires. Les émetteurs de cartes co-marquées doivent donc s'assurer que leurs partenaires se conforment aux exigences de sécurité applicables en la matière.

Un exemple d'exigences communes de protection des fichiers de données de carte est le programme PCI DSS (*Payment Card Industry - Data Security Standard*). Il est désormais adopté en France, avec des adaptations tenant compte du fonctionnement des cartes de type « interbancaire » avec une puce et un contrôle de code confidentiel plutôt qu'en mode piste. Ainsi, les émetteurs français de cartes de type « interbancaire » ou « privatif », leurs prestataires techniques et leurs partenaires commerciaux mettent en œuvre ces exigences de sécurité, y compris pour les cartes co-marquées.

Une bonne pratique mise en œuvre par les émetteurs consiste également à éviter l'emploi de données personnelles en dehors de l'environnement informatique de production, par exemple par leur transformation en données anonymes dans les jeux de test.

Sécurité de l'opération d'émission

Actuellement en France, l'émission des cartes co-marquées reste principalement sous le contrôle des émetteurs. Ceux-ci sont donc en mesure d'assurer cette opération sensible selon les mêmes normes sécuritaires que pour les cartes non co-marquées.

Longtemps limitée au renouvellement de cartes à piste perdues ou endommagées, sans modification du code PIN, l'émission immédiate sur le lieu de vente est sur le point d'être étendue à l'émission initiale de la carte, y compris lorsque celle-ci est à puce. Cette opération

est plus risquée et nécessite d'être correctement encadrée, notamment pour s'assurer de la sécurité de la gestion des stocks de cartes et des données sensibles utilisées pour la personnalisation des cartes (cf. voir chapitre 1).

Sécurité de la carte

Afin de se prémunir contre tout risque d'atteinte à l'image de sérieux des cartes co-marquées et de matérialiser leur statut de carte de paiement, les émetteurs de cartes co-marquées appliquent obligatoirement leur logo au recto ou au verso de celles-ci, et demandent à leurs partenaires commerciaux de communiquer clairement sur le caractère de carte de paiement de leurs cartes. De plus, l'émetteur de la carte conserve la propriété et l'entière responsabilité de celle-ci ; il est donc important qu'il reste l'interlocuteur du porteur, qui est ainsi assuré que sa carte bénéficiera du même niveau de protection qu'une carte de paiement non co-marquée.

Pour garantir la sécurité des cartes multifonctions, il est nécessaire d'assurer le cloisonnement des différentes applications. Cela passe par la sélection de cartes prévues à cet effet. Le Groupement des Cartes Bancaires « CB » édite un catalogue de cartes agréées, fournissant un niveau de sécurité adapté à ce type d'usage.

Conclusion

Le co-marquage des cartes de paiement consiste à apposer, aux côtés de la marque de l'établissement émetteur de la carte, celle d'un ou plusieurs partenaires commerciaux. Il s'agit d'une pratique déjà répandue dans de nombreux pays, mais qui n'était pratiquée jusqu'à il y a peu en France que par les systèmes de carte de type « privatif ». Depuis le 1er octobre 2007, le Groupement des Cartes Bancaires « CB » a autorisé cette pratique pour les cartes « CB », suivant en cela les préconisations encadrant la mise en place de l'Espace unique de paiement en euros (*Single Euro Payments Area* – SEPA).

De nombreuses initiatives de cartes co-marquées ont ainsi vu le jour en France, suscitant parfois des inquiétudes de la part des consommateurs sur le maintien par l'établissement émetteur de la maîtrise de ses cartes co-marquées. L'Observatoire a en conséquence examiné si cette nouvelle pratique pouvait avoir un impact en termes de sécurité et si les conditions de sécurité dans lesquelles ces nouvelles cartes étaient utilisées étaient satisfaisantes.

Le co-marquage d'une carte de paiement peut amener le partenaire commercial de l'établissement émetteur soit à réaliser tout ou partie des opérations de souscription et d'émission de la carte, soit à partager avec l'établissement émetteur les informations personnelles et les données bancaires du client.

L'Observatoire constate que les projets développés à ce jour en France mettent en œuvre des mesures de sécurité répondant aux risques pouvant en résulter. Pour toute nouvelle carte, il recommande aux établissements émetteurs de veiller à l'application complète des mesures de sécurité existant aujourd'hui dans l'environnement des cartes de paiement pour le recueil, le stockage et la gestion des données sensibles.

Une évolution peut également consister à faire coexister sur la carte différentes applications, par exemple l'application de fidélité du partenaire commercial aux côtés de l'application bancaire de paiement. Il importe en conséquence d'assurer qu'une parfaite maîtrise de la sécurité des données sensibles soit maintenue et, en cas de coexistence de plusieurs applications sur la même carte, de vérifier qu'aucune d'entre elles ne remette en cause la sécurité de l'application de paiement. L'Observatoire recommande, en cas de coexistence

d'applications, que les émetteurs choisissent des cartes répondant à un niveau éprouvé et reconnu de protection de l'application de paiement.

3 | 3 Sécurité des réseaux d'automates de paiement

Les automates de paiement sont des dispositifs d'acceptation permettant au porteur de carte d'effectuer un paiement seul, sans l'intervention d'aucune autre personne physique. La mise en œuvre de ces machines par les accepteurs implique le déploiement d'une infrastructure de réseaux, dont le but est de relier plusieurs automates entre eux en utilisant des équipements permettant de concentrer les flux de transactions effectuées sur ces automates pour les envoyer vers le serveur de la banque acquéreur. Or la nature des réseaux mis en œuvre évolue du fait de l'utilisation des nouvelles techniques de communication (IP[12], Wifi[13], GPRS[14]…). De plus, alors que les standards et les réseaux utilisés par le passé étaient détenus et maîtrisés par l'opérateur de télécommunication historique, se généralise à présent l'usage de réseaux dits « ouverts », qui ne sont pas dédiés au paiement et dont la maîtrise de la sécurité est plus complexe car ils impliquent un plus grand nombre d'acteurs.

Dans le prolongement des études menées en 2006 sur l'utilisation de réseaux ouverts dans l'environnement des cartes de paiement[15], d'une part, et sur la sécurité des automates[16], d'autre part, l'Observatoire a donc souhaité examiner les enjeux, pour la sécurité des réseaux d'automates de paiement, de l'évolution des types de réseaux utilisés.

Caractéristiques des réseaux d'automates de paiement

On dénombre environ 60 000 automates de paiement en France en 2008, installés par les commerçants pour répondre à des besoins de distribution automatique ciblés, pour des produits ou services tels que carburant, titres de transport, péages, parkings, DVD, boissons, vélos en libre service, etc. Ces automates acceptent généralement à la fois les cartes de type « interbancaire » et certaines cartes de type « privatif ». Certains automates acceptent également les porte-monnaie électroniques.

Les automates de paiement s'inscrivent dans des infrastructures de réseaux, qui font intervenir différents types d'équipements, de protocoles de communication et d'acteurs, selon l'architecture générale décrite dans le schéma ci-après.

12 *Internet Protocol*, protocole de communication standard sur lequel est basé Internet.

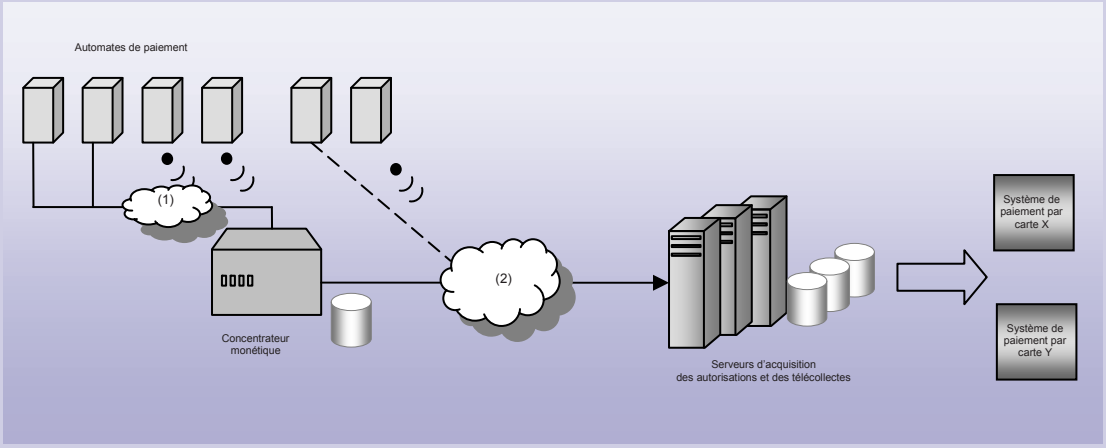
13 Le Wifi est une technique de réseau informatique sans fil, utilisée comme moyen d'accès à haut débit à Internet.

14 Le GPRS (*General Packet Radio Service*) est un protocole de communication orienté données pour la téléphonie mobile, fonctionnant sur les réseaux GSM et permettant un débit de données plus élevé.

15 Cf. Rapport annuel 2006 de l'Observatoire, pp. 25 à 30

16 Cf. Rapport annuel 2006 de l'Observatoire, pp. 30 à 38

Encadré 7 – Architecture type de réseaux d'automates



Les automates de paiement installés chez le commerçant (par exemple distributeurs automatiques de carburant dans une station-service) sont généralement reliés à un équipement informatique fédérateur, le concentrateur monétique, qui reçoit les données correspondant aux transactions de paiement réalisées sur ces automates et effectue la liaison avec le(s) serveur(s) acquéreur(s). Ce dernier transmet ensuite les demandes d'autorisation et les télécollectes au(x) système(s) de paiement par carte concerné(s).

On peut toutefois observer des variantes dans la mise en œuvre de ces architectures de réseaux. L'automate peut par exemple se connecter à un point d'accès local ou à un prestataire distant qui assure le relais des données vers les serveurs d'acquisition.

Le périmètre de la présente étude se concentre sur les réseaux reliant les automates aux concentrateurs (représentés en (1) sur le schéma) et les concentrateurs aux serveurs acquéreurs (représentés en (2) sur le schéma). Est aussi traité le cas où les automates accèdent sans concentrateur aux serveurs acquéreurs (représenté en pointillé sur le schéma). Les réseaux reliant les serveurs d'acquisition aux systèmes de paiement par carte ne sont pas traités dans cette étude.

Les réseaux d'automates de paiement mettent en jeu différents équipements permettant d'une part de traiter et d'autre part d'échanger les données de transactions de paiement par carte entre différentes catégories d'acteurs :

– le commerçant accepteur ;

– la banque acquéreur ;

– le ou les prestataires techniques et prestataires de service, qui prennent en charge tout ou partie de la gestion des équipements et des réseaux de communication.

Les équipements utilisés pour les traitements des données sont principalement des serveurs informatiques, le plus souvent dotés d'un système d'exploitation dit « embarqué », c'est-à-dire soit dérivé d'une version standard, comme Microsoft Windows ou Linux, et spécialement adapté aux fonctions mises en œuvre par ce matériel, soit développé spécifiquement pour cet appareil (systèmes propriétaires).

Différentes techniques de communication peuvent être utilisées pour transmettre les données de paiement, reposant sur des équipements physiques et des protocoles de communication distincts. On distingue ainsi généralement deux principaux types de techniques permettant d'interconnecter les équipements entre eux : avec fil (câbles, fibres optiques) ou sans fil (radiocommunications telles que Wifi ou GPRS). Par ailleurs, le protocole de communication X25, jusqu'alors largement utilisé dans les réseaux filaires, laisse

progressivement la place au protocole de communication IP sur lequel est basé Internet et que l'on retrouve également sur les réseaux sans fil.

Chez l'accepteur, la liaison entre l'automate et le concentrateur monétique s'effectue ainsi de plus en plus fréquemment avec des techniques sans fil (telles que Wifi ou GPRS), qui offrent un certain nombre de facilités pour le raccordement des matériels d'acceptation, en termes de souplesse d'installation et de couverture de service.

La liaison entre le concentrateur et l'acquéreur repose généralement sur une liaison IP, avec des équipements qui sont souvent filaires. Dans le cas où l'automate du commerçant accepteur est directement relié au système acquéreur, la liaison est, là encore, le plus souvent IP et peut être soit filaire soit sans fil.

Impacts en termes de sécurité de l'utilisation de réseaux ouverts

Protéger le réseau par lequel sont transmises les informations de gestion de l'automate suppose en premier lieu de protéger l'automate lui-même, afin d'éviter qu'une installation de matériel ou de logiciel à des fins frauduleuses ne puisse permettre de prendre le contrôle du réseau de communication auquel l'automate est relié. Il est également nécessaire de prendre des mesures pour assurer la protection du réseau proprement dit, en particulier lorsqu'il s'agit d'un réseau ouvert.

Protection des équipements

Protection physique

L'intégrité des automates fait l'objet d'une attention particulière. Des mesures sont prises pour assurer la protection physique de ces équipements lors des interventions ou des opérations de maintenance, effectuées par le personnel du commerçant et le personnel de maintenance. Ces derniers sont également invités à faire preuve de vigilance vis-à-vis de toute modification extérieure de ces équipements. En outre, l'ouverture des automates entraîne généralement une désactivation des fonctions de paiement, qui ne peuvent être réactivées qu'après intervention d'un opérateur habilité.

Protection des systèmes d'exploitation

La sécurité des systèmes d'exploitation embarqués est un élément essentiel pour la protection des réseaux d'automates eux-mêmes. Ces systèmes, qui comportent un ensemble de fonctionnalités et une configuration par défaut, peuvent en effet être la cible de fraudeurs cherchant à exploiter leurs vulnérabilités pour accéder à un des équipements, et ainsi prendre le contrôle du réseau d'automates. L'utilisation des nouvelles techniques de communication et de systèmes d'exploitation basés sur ceux du grand public est de nature à faciliter ce type d'attaque logique.

C'est pourquoi il est nécessaire de mettre en œuvre des mesures de sécurité pour se prémunir contre ce risque. L'une des solutions consiste à durcir la sécurité des systèmes d'exploitation, afin d'optimiser la sécurité des équipements composant le réseau d'automates compte tenu de l'utilisation qui en est faite. Il s'agit de supprimer ou de désactiver les composants logiciels et les fonctionnalités inutilisés, qui pourraient faciliter le travail d'un attaquant ou présenter des failles de sécurité, et de mettre en place des restrictions d'accès à certaines données. La configuration par défaut doit en outre être adaptée pour n'autoriser que les communications nécessaires, et

ne pas permettre à l'équipement d'être interconnecté à Internet sans contrôle. De telles mesures ont déjà été préconisées en 2003 et mises à jour en 2008 par le Groupement des Cartes Bancaires « CB » pour les distributeurs automatiques de billets. Il serait ainsi utile de les étendre à l'ensemble des automates connectés sur des réseaux ouverts.

Des mises à jour régulières du système d'exploitation sont également de nature à renforcer le niveau de sécurité des équipements. Par exemple, pour une meilleure réactivité face aux nouveaux scénarios de fraude, la mise en œuvre des correctifs de sécurité devrait pouvoir s'effectuer à distance et de manière sécurisée, c'est-à-dire par la signature des éléments transmis et sa vérification sur l'équipement destinataire avant l'opération de mise à jour.

Protection des réseaux ouverts

Impact de l'utilisation de réseaux ouverts

L'évolution de la nature des réseaux utilisés dans le cadre de la mise en réseau d'automates fait intervenir un plus grand nombre d'acteurs, ce qui pose la question de la propriété et de la maîtrise des techniques utilisées.

Jusqu'à la dérégulation des télécommunications, les réseaux étaient la propriété d'un seul opérateur et n'étaient accessibles qu'à son personnel. Le contrôle de ces réseaux et de leurs équipements par l'opérateur assurait une certaine sécurité.

Depuis, la dérégulation et le développement d'Internet ont favorisé l'apparition de multiples opérateurs et fournisseurs de services exploitant des réseaux largement interconnectés et mutualisés. Le contrôle de la confidentialité et de l'intégrité des données qui sont échangées sur ces réseaux dits « ouverts » devient plus difficile. La connaissance des protocoles de communication s'est également largement répandue. De plus, l'utilisation croissante des techniques sans fil rend les réseaux plus facilement accessibles. Or ces réseaux ne comportent pas nativement de dispositif de sécurisation de bout en bout. La maîtrise de la sécurité des données échangées devient ainsi plus difficile à assurer.

Le passage des réseaux dédiés dits « propriétaires » aux réseaux ouverts afin de relier les automates aux concentrateurs s'effectue au rythme du renouvellement des automates, dont la durée de vie peut atteindre dix ans. Coexistent ainsi aujourd'hui des réseaux dédiés et des réseaux ouverts. Les réseaux reliant les équipements fédérateurs aux serveurs d'acquisition commencent également à utiliser le protocole de communication IP.

Compte tenu de la sensibilité des données de paiement transmises, qui comprennent notamment le numéro de la carte (PAN), la date de fin de validité, le nom du porteur et les données de la piste magnétique (si elles sont lues) ou les certificats de transaction (dans le cas d'EMV), des mesures de sécurité doivent être mises en œuvre par les différents acteurs concernés pour en garantir la confidentialité et l'intégrité. Ces mesures doivent viser à se prémunir contre le risque d'écoute et de vol des données. Il s'agit d'une part d'éviter qu'un fraudeur puisse réutiliser ces données pour effectuer des paiements à distance ou des transactions de proximité dans les pays fonctionnant en mode « piste » et, d'autre part, d'empêcher l'intrusion d'un fraudeur qui chercherait à réaliser de fausses transactions ou à attaquer le système.

Mesures de sécurité

Les prestataires offrant des services de communication proposent généralement des mécanismes de sécurité adaptés aux protocoles de communication utilisés et à la nature des données échangées. Ces mécanismes peuvent être complétés par des exigences des banques acquéreurs ou des systèmes de paiement par carte, qui s'appliquent également aux commerçants et à leurs prestataires.

Mesures mises en œuvre au niveau du commerçant

Afin de sécuriser la liaison IP entre les automates et le concentrateur monétique du commerçant, les prestataires proposent deux types de mesures : les réseaux privés virtuels (ou VPN - *Virtual Private Network*) ou un protocole de sécurisation SSLv3 ou équivalent (*Secure Socket Layer* version 3). L'utilisation de VPN consiste à créer un réseau cloisonné par un processus logique. Les données à transmettre sont ainsi encapsulées et sécurisées par des algorithmes cryptographiques, ce qui garantit leur confidentialité et leur intégrité, tandis que les équipements établissant le VPN sont également authentifiés. Le protocole SSLv3 permet, lui, une sécurisation au niveau applicatif. Il fonctionne en mode client-serveur et assure l'authentification du serveur (i.e. le concentrateur dans le cas présent), l'intégrité des données, leur confidentialité (par l'utilisation d'une session chiffrée), ainsi que, de manière optionnelle, l'authentification du client (i.e. l'automate).

Des mesures complémentaires peuvent également être mises en œuvre pour se prémunir contre les risques liés à l'usage de techniques sans fil. Dans le cas de l'utilisation de la technique Wifi notamment, des mesures d'authentification et de chiffrement sont généralement mises en œuvre entre l'automate et la borne sans fil avec laquelle il communique, qui reposent sur l'utilisation de certificats. Le recours à l'authentification est également possible en cas d'utilisation de la technique GPRS. Le Groupement des Cartes Bancaires « CB » recommande ainsi le chiffrement pour les automates communiquant en mode GPRS.

Mesures mises en œuvre par le prestataire en charge du réseau de communication

La sécurisation de la liaison IP entre le concentrateur et le serveur acquéreur repose également sur l'utilisation de VPN ou du protocole SSLv3.

Mesures mises en œuvre par les banques acquéreurs

En dépit des mesures de sécurité décrites ci-dessus, la banque acquéreur ne dispose pas d'une maîtrise complète de la sécurité des données échangées sur les réseaux de communication, compte tenu de la multiplicité des acteurs impliqués et du fait que les réseaux sont la propriété des prestataires offrant ces services. C'est pourquoi les banques acquéreurs appliquent un certain nombre de prescriptions en matière d'authentification et de chiffrement des transactions, pour en assurer la protection de bout en bout. Elles demandent également aux commerçants et à leurs prestataires de mettre en œuvre ces mesures de sécurité pour ce qui concerne la liaison entre les automates et le concentrateur.

Ainsi, le standard international PCI DSS (*Payment Card Industry – Data Security Standard*), établi par PCI Security Standard Council, exige le chiffrement des données de paiement par carte transmis sur les réseaux ouverts, afin d'en assurer la protection.

Même lorsque les données transitent par un VPN, le Groupement des Cartes Bancaires « CB » impose donc le chiffrement de bout en bout[17] des données de transactions, pour garantir leur confidentialité.

De plus, le Groupement des Cartes Bancaires « CB » exige l'utilisation d'un protocole de sécurisation SSLv3 ou équivalent. Dans ce cadre, l'authentification du serveur d'acquisition (ou du concentrateur) est obligatoire. Elle repose sur l'utilisation d'un certificat. En complément, la mise en œuvre d'une authentification du concentrateur (ou de l'automate) est également recommandée, mais non obligatoire. En effet, dans le cas de réseaux d'automates de paiement, c'est le concentrateur qui appelle le serveur d'acquisition (et l'automate qui appelle le concentrateur) pour transmettre les données de transaction, mais le concentrateur n'est jamais appelé par le serveur d'acquisition. Pour assurer un bon niveau de sécurité, il est donc nécessaire que le dispositif appelant présente un certificat au dispositif appelé, la réciproque n'étant pas indispensable. On note d'ailleurs que les appareils certifiés à ce jour sont *de facto* tous équipés par les fabricants d'un système d'authentification du concentrateur (ou de l'automate).

S'agissant des systèmes de carte de type « privatif », dans la mesure où ils partagent des équipements avec le système « CB », notamment le matériel d'acceptation des accepteurs, ils bénéficient des mesures de sécurité développées pour répondre aux exigences de « CB ».

Conclusion

Les automates de paiement sont généralement déployés dans des infrastructures de réseaux, qui se caractérisent par une utilisation de plus en plus fréquente de réseaux ouverts et de techniques de communication sans fil (GPRS, Wifi, etc.). Cette évolution de la nature des réseaux utilisés peut introduire de nouveaux risques en termes de sécurité physique et logique des équipements et de confidentialité des données traitées et échangées.

Pour se prémunir contre ces risques, les commerçants, les émetteurs et leurs prestataires mettent en œuvre des mesures de sécurité spécifiques, incluant l'utilisation de réseaux privés virtuels ou de protocoles de sécurisation. Des mécanismes complémentaires de chiffrement des données et d'authentification des équipements sont également employés, en particulier en cas d'utilisation de techniques sans fil.

L'Observatoire recommande à l'ensemble des acteurs concernés de généraliser l'utilisation de telles mesures de protection des données, qui sont indispensables pour assurer la sécurité des automates de paiement s'inscrivant dans des réseaux ouverts et pourraient également être mis en œuvre pour renforcer le niveau de sécurité en cas d'utilisation de réseaux propriétaires.

L'Observatoire préconise en outre que l'ensemble des systèmes de paiement par carte mette en œuvre des exigences permettant d'assurer un niveau de sécurité des réseaux d'automates équivalent à celui préconisé aujourd'hui par le Groupement des Cartes Bancaires « CB » pour la mise en réseau de DAB. En particulier, il est recommandé que des certificats soient utilisés à la fois sur les automates et sur les concentrateurs, afin de permettre une authentification mutuelle de ces appareils.

En complément, l'Observatoire invite les fabricants de matériels et les prestataires à durcir les systèmes d'exploitation embarqués sur les automates et les concentrateurs monétiques, afin d'accroître leur niveau de sécurité et en particulier d'empêcher des connexions non autorisées

[17] De bout en bout s'entend ici de l'automate au serveur d'acquisition.

vers ces appareils. Il est également souhaitable que ces systèmes puissent être régulièrement mis à jour, à distance et de façon sécurisée.

Enfin, l'Observatoire considère que les fonctions de paiement des automates, ainsi que leur environnement matériel, logiciel et réseau, devraient faire l'objet d'une procédure d'agrément par le système de paiement par carte. Une telle procédure devrait s'appuyer sur une évaluation sécuritaire et contribuerait à garantir un niveau de sécurité élevé et homogène des réseaux d'automates.

3|4 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 cinq ans de façon à mesurer l'avancement de la migration EMV, l'Observatoire a de nouveau recueilli auprès du Groupement des Cartes Bancaires « CB » et de l'EPC des statistiques relatives à cette migration en France et en Europe. Ces chiffres montrent que la migration est en cours partout en Europe, avec une progression correcte dans la plupart des pays, globalement en ligne avec l'engagement des banques européennes au sein de l'EPC d'avoir achevé cette migration fin décembre 2010. L'Observatoire s'inquiète cependant des disparités persistantes dans la progression de la migration, qui sont susceptibles de laisser perdurer une fraude transfrontalière européenne significative.

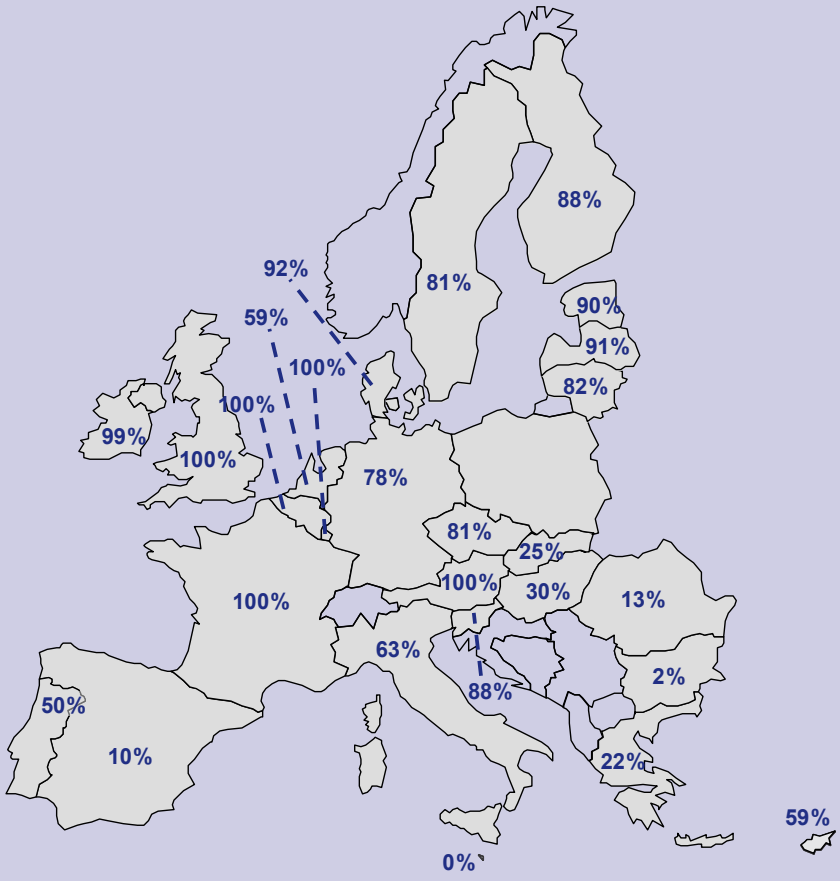
État de la migration en France

En France, la migration au standard EMV est quasiment terminée. Fin mars 2009, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes « CB », 99,5 % des terminaux et automates, et 100 % des distributeurs automatiques de billets étaient conformes aux spécifications EMV. Le 0,5 % restant de terminaux et automates, peu utilisés, seront migrés lors de leur remplacement normal.

État de la migration en Europe

Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2009, 67,5 % des cartes interbancaires circulant au sein des 27 États membres de l'Union européenne sont maintenant conformes à la spécification EMV (+ 6 points par rapport à mars 2008). Pays par pays, la situation reste contrastée (voir Encadré 8). Alors que la mise en conformité aux règles d'interopérabilité de SEPA a commencé depuis début 2008, la migration EMV de plusieurs pays soit est à peine débutée (Bulgarie), soit reste peu avancée (Espagne, Grèce, Roumanie).

Encadré 8 – Déploiement des cartes EMV en Europe



Source : European Payments Council – mars 2009

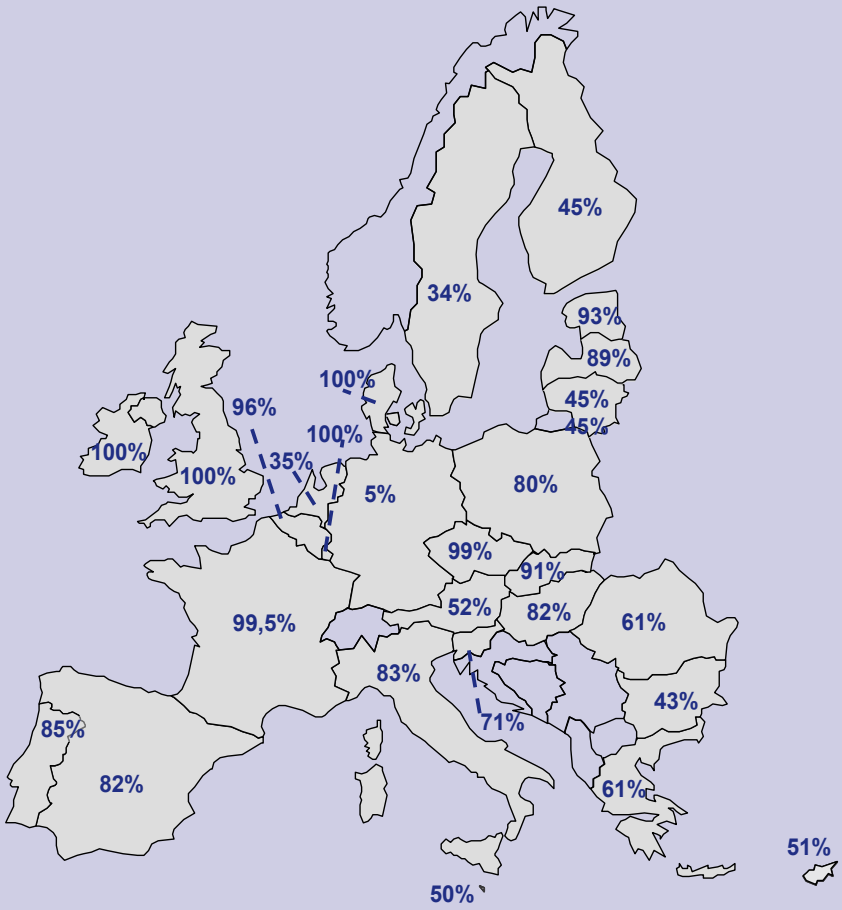
Par rapport à l'an dernier, on constate une progression générale de la migration des cartes au standard EMV. Toutefois, plusieurs pays débutent à peine leur migration, comme la Bulgarie et Malte, ou sont peu avancés, comme l'Espagne, la Grèce et la Roumanie.

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

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

Concernant l'acquisition, la migration vers EMV progresse sensiblement : à fin mars 2009, 75,9 % des terminaux de paiement (voir Encadré 9) et 92,0 % des distributeurs automatiques de billets (voir Encadré 10) sont conformes à EMV (soit une progression de + 9 points pour chacun de ces indicateurs par rapport à mars 2008). La situation reste très contrastée pays par pays, tant en taux d'équipement qu'en progression d'une année sur l'autre.

Encadré 9 – Déploiement des terminaux et automates EMV en Europe



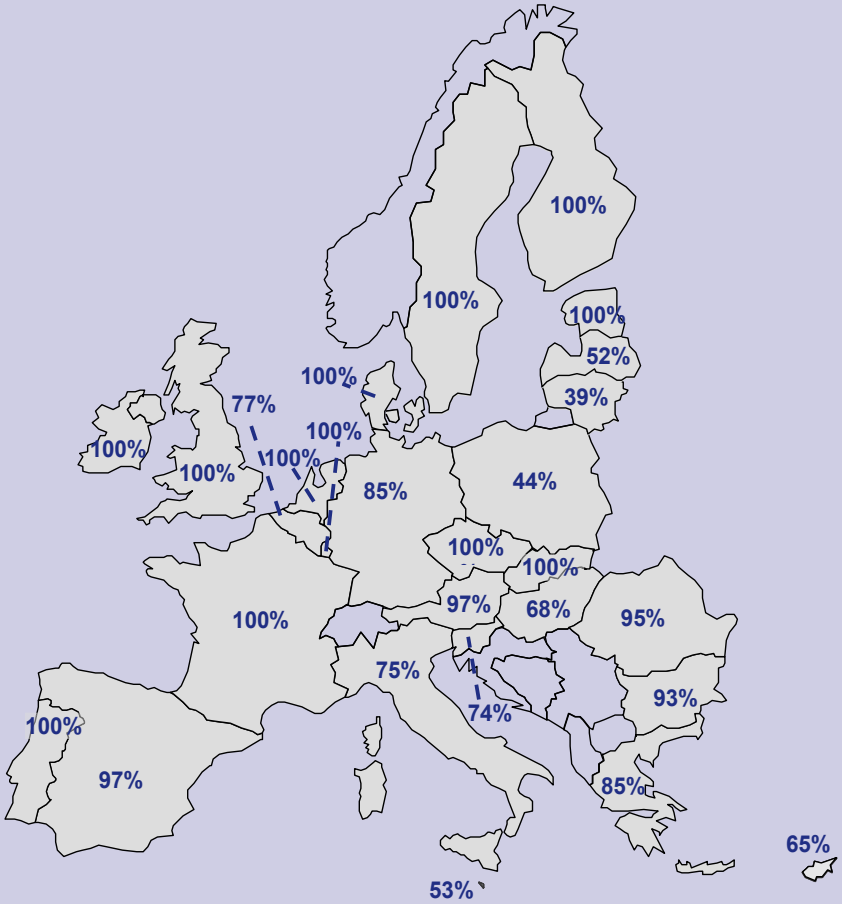
Source : European Payments Council – mars 2009

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

La situation évolue toujours très peu en Allemagne par rapport à mars 2008, ce pays restant à un faible niveau d'équipement. La migration a en revanche progressé en Suède, aux Pays-Bas et au Danemark, ce dernier pays ayant achevé sa migration.

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 10 – Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2009

La progression de la migration des distributeurs de billets est plus homogène dans les différents pays européens et les taux de migration sont globalement plus élevés que pour les cartes et les terminaux. Il subsiste toutefois quelques disparités. Les pays en cours de migration de leur parc de distributeurs automatiques de billets au standard EMV ont probablement choisi de migrer en priorité les automates utilisés par les touristes et les visiteurs étrangers. L'Allemagne et l'Italie restent en deçà des niveaux de déploiement des autres grands pays mais leur niveau d'équipement s'est amélioré depuis mars 2008.

4 | LA CERTIFICATION DE LA SÉCURITÉ DES CARTES ET DES TERMINAUX

Depuis plusieurs années, l'Observatoire s'est montré attentif aux enjeux liés à la sécurité des cartes et des terminaux de paiement dans le cadre de la constitution d'un espace européen des paiements.

Dès 2005, il avait expliqué l'importance des procédures d'évaluation et de certification de la sécurité des cartes et des terminaux et recommandé que des accords puissent être mis en œuvre au niveau européen pour que ces procédures soient harmonisées, afin d'assurer un niveau élevé et homogène de sécurité des paiements par carte en Europe.

Compte tenu de l'importance de ce sujet, l'Observatoire a souhaité rendre compte des propositions exprimées à ce jour dans ce domaine par les différents acteurs concernés : banques, systèmes de paiement par carte, industriels, organismes de certification, autorités européennes et banques centrales.

4 | 1 Etat des lieux de la certification de la sécurité des cartes et des terminaux en Europe : des pratiques hétérogènes

On peut observer que l'ensemble des systèmes de paiement par carte opérant en Europe met en œuvre des procédures consistant à vérifier le niveau de sécurité des cartes et des terminaux utilisés. Ces procédures varient cependant assez fortement d'un système à l'autre de sorte qu'il n'est pas possible à l'heure actuelle de considérer que les cartes et les terminaux sont d'un niveau de sécurité équivalent.

Le processus de certification

Le processus de certification des cartes de paiement et des terminaux d'acceptation comprend généralement les quatre étapes suivantes (voir Encadré 11) :

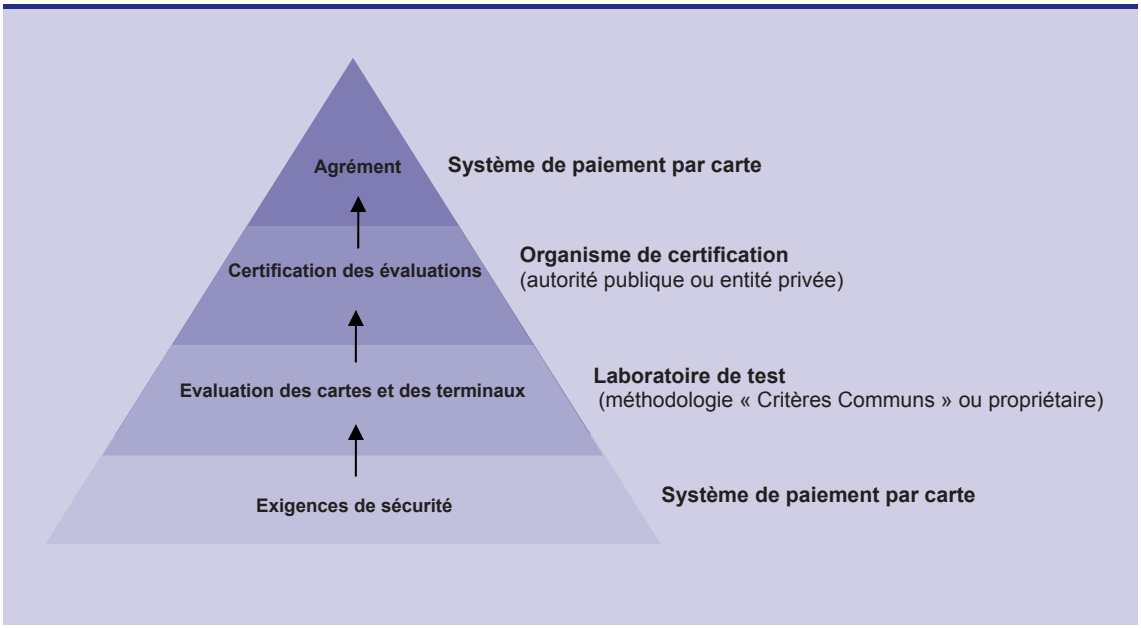
– la définition par le système de paiement par carte des exigences de sécurité applicables aux cartes et aux terminaux, que les industriels doivent respecter ;

– les évaluations sécuritaires, qui sont réalisées par des laboratoires spécialisés, selon différentes méthodologies. Les industriels doivent y soumettre leurs produits pour vérifier qu'ils respectent bien les exigences de sécurité prévues ;

– la certification des évaluations, qui peut être conduite par différents types d'acteurs et permet d'attester la qualité des évaluations sécuritaires effectuées. Les industriels obtiennent ainsi de ces organismes de certification un certificat prouvant que leur produit est conforme aux exigences de sécurité fixées par le système de paiement par carte ;

– l'agrément délivré par le système de paiement par carte, sur la base du certificat présenté par le fabricant de carte ou de terminal.

Encadré 11 – Schéma type du processus de certification



Des pratiques hétérogènes selon les systèmes de paiement par carte

En France, le système de paiement par carte « CB » s'appuie sur des procédures de certification dont la qualité est élevée[18]. Pour les cartes, la conduite des évaluations répond à la norme internationale des « Critères Communs » (voir Encadré 12) et le processus de certification entre dans le cadre d'un « Schéma national », placé sous l'autorité de la Direction centrale de la sécurité des systèmes d'information (DCSSI), service du Premier ministre.

Les informations recueillies au niveau européen montrent que les pratiques en matière de certification divergent selon les pays et les systèmes de paiement par carte, du fait de l'utilisation de différentes méthodologies d'évaluation et du recours à différents types d'organismes de certification.

Concernant les méthodologies d'évaluation utilisées :

– la plupart des systèmes de paiement par carte fondent leurs évaluations sur des méthodologies de type propriétaire, qui ont le plus souvent été développées par les réseaux internationaux (telles que MasterCard CAST pour les cartes et PCI PED pour les terminaux) ;

– dans quelques cas toutefois (comme en France pour les cartes et au Royaume Uni pour les terminaux), la méthodologie d'évaluation mise en œuvre repose sur des standards internationaux, non propriétaires (cf. norme ISO dite des « Critères Communs »).

[18] Cf. Rapport annuel 2005 de l'Observatoire, p. 44

Encadré 12 – Les Critères Communs

La norme internationale dite des « Critères Communs d'évaluation de la sécurité des technologies de l'information » (ISO/IEC 15408) permet de s'assurer que les processus de spécification des exigences de sécurité, de développement du produit et d'évaluation de la sécurité ont été conduits de la façon la plus rigoureuse possible.

Contrairement à d'autres standards de sécurité informatique, les Critères Communs ne définissent pas un ensemble de règles auxquelles les produits informatiques doivent se conformer. Il s'agit plutôt d'un cadre qui permet aux utilisateurs de formuler des exigences en matière de sécurité et aux fournisseurs d'affirmer que leurs produits sont conformes à ces exigences.

A cet effet, la méthodologie des Critères Communs repose sur trois concepts principaux :

– le profil de protection (*Protection Profile* – PP), qui est un document exprimant les exigences en matière de sécurité d'une communauté d'utilisateurs ;
– la cible de sécurité (*Security Target* – ST), qui est un document (généralement rédigé par le fournisseur du produit) décrivant les capacités du produit en termes de sécurité et listant les éventuels profils de protection que le produit prétend respecter ;
– le niveau d'assurance (*Evaluation Assurance Level* – EAL), qui regroupe l'ensemble des mesures prises pour se conformer aux exigences de sécurité, ainsi que l'évaluation des vulnérabilités dont le niveau de résistance aux attaques. Les niveaux d'assurance vont du niveau EAL-1 (le moins exigeant) au niveau EAL-7 (le plus exigeant). Ces niveaux d'assurance comportent des exigences dans différents domaines : gestion de configuration (ACM), livraison et exploitation (ADO), développement (ADV), guides (AGD), support au cycle de vie (ALC), tests (ATE) et évaluation des vulnérabilités (AVA). Le niveau de résistance aux attaques, qui va de « élémentaire » à « élevé », est mentionné dans le certificat.

S'agissant des organisations retenues pour la certification :

– environ la moitié des pays européens disposent d'un cadre de certification au niveau national. Celui-ci est le plus souvent placé sous l'autorité d'une entité privée (association bancaire par exemple). Dans les pays où il existe une autorité publique, celle-ci peut être impliquée dans la certification des cartes ou des terminaux mais, contrairement à la situation française, les systèmes de paiement par carte ne s'appuient pas nécessairement sur les certificats délivrés par ces autorités pour accorder leur agrément ;
– lorsqu'il n'existe pas de tel cadre de certification au niveau national, la certification s'effectue sous le contrôle d'organismes privés internationaux (comme Visa, MasterCard, PCI SCC, EMVCo) pour les systèmes de carte internationaux actifs dans le pays, ainsi que le cas échéant pour les cartes du système national co-badgé.

Ainsi, les systèmes de paiement par carte actifs en Europe ne disposent pas à l'heure actuelle de règles communes concernant le niveau de sécurité des cartes et des terminaux, ni d'approche harmonisée pour la certification des évaluations sécuritaires. Cette situation oblige les fabricants de cartes et de terminaux à soumettre leurs produits à différents processus de certification, ce qui est source de coûts et de délais et n'est donc pas optimal dans la perspective de la construction d'un marché intégré des paiements de détail.

La diversité des pratiques actuelles soulève également un enjeu important sur le plan de la sécurité, dans la mesure où elle ne permet pas de garantir un niveau de sécurité élevé et homogène pour les cartes et les terminaux utilisés en Europe. Or un système de paiement par carte A qui accepte les cartes d'un système de paiement par carte B d'un niveau de sécurité inférieur peut être exposé à un risque de fraude plus important. Il existe en outre un risque potentiel d'alignement de la sécurité par le bas, compte tenu du renforcement de la concurrence sur le marché européen des paiements par carte qui peut amener à la recherche de coûts plus faibles au détriment de la sécurité.

4 | 2 Importance de la mise en œuvre d'un cadre européen de certification harmonisé

Le besoin d'harmonisation des procédures de certification

Compte tenu des enjeux liés à l'évolution du contexte européen, l'Observatoire avait d'ores et déjà souligné dans son rapport annuel 2005 la nécessité d'uniformiser les procédures d'évaluation et de certification existantes. Pour cela, il avait identifié plusieurs voies de progrès possibles, afin de favoriser l'émergence de critères d'équivalence et la reconnaissance mutuelle des certificats.

Les banques centrales de l'Eurosystème ont également exprimé, dans le *6e Rapport d'étape sur SEPA*, publié le 24 novembre 2008, la nécessité d'une telle harmonisation et elles ont défini un certain nombre de conditions nécessaires à l'instauration d'un tel cadre harmonisé :

– en premier lieu, il s'agit de définir un niveau de sécurité physique des cartes et des terminaux qui soit approprié et homogène, à respecter par l'ensemble des cartes et des terminaux SEPA ;

– il convient en deuxième lieu de garantir que les méthodologies d'évaluation et de certification appliquées par les laboratoires de test et les organismes de certification soient équivalentes en termes de niveau de qualité ;

– si plusieurs méthodologies d'évaluation et de certification ou si plusieurs organismes de certification continuent à co-exister, comme cela est vraisemblable, il est nécessaire en troisième lieu de définir un mécanisme de gouvernance européenne, capable d'assurer la reconnaissance mutuelle des certifications sécuritaires. Ce mécanisme de gouvernance doit présenter les garanties nécessaires en termes de légitimité et de neutralité pour permettre d'établir la confiance des utilisateurs dans ce dispositif. Un tel cadre harmonisé contribuerait en outre à simplifier le processus d'évaluation et de certification pour les fabricants de cartes et de terminaux, en leur permettant d'obtenir de l'une des autorités de certification des certificats valables dans l'ensemble de l'espace SEPA (concept du *one-stop shopping*).

Les progrès réalisés par les acteurs du marché

Les acteurs du marché ont progressé dans le sens souhaité par l'Observatoire, et conformément aux orientations du *6e Rapport d'étape sur SEPA* de l'Eurosystème, même si les travaux doivent encore se poursuivre pour atteindre les objectifs fixés. Le bilan est aujourd'hui le suivant.

La définition des exigences de sécurité applicables aux cartes et aux terminaux semble avancer de manière satisfaisante. En effet, concernant la sécurité des composants de la carte, l'EPC a défini comme exigence le niveau « EAL4+ » de la norme « Critères Communs » avec une résistance élevée aux attaques, qui est celui actuellement requis en France pour les cartes à puce de type « interbancaire ». Concernant les terminaux, l'EPC a défini des exigences de sécurité qui comprennent, d'une part, les spécifications PCI PED pour le clavier et le lecteur de piste, et, d'autre part, des exigences complémentaires pour d'autres composants du terminal. Ces exigences de sécurité ont dorénavant vocation à servir de socle commun pour l'ensemble des systèmes de paiement par carte conformes aux règles SEPA.

Le choix d'une méthodologie d'évaluation n'est pour l'instant pas fixé. Les industriels appellent de leurs vœux le choix d'une méthodologie commune d'évaluation, mais la situation varie selon qu'il s'agisse des cartes ou des terminaux, dans la mesure où le périmètre et la nature des équipements à certifier diffèrent. L'approche « Critères Communs » constitue pour les fabricants de cartes la méthodologie de référence depuis des années. En revanche, la majorité des fabricants de terminaux semble favorable à l'approche PCI. Toutefois, des travaux engagés en commun par des systèmes de paiement par carte, des organismes de certification et des laboratoires de test visent à créer un cadre d'évaluation des terminaux selon la méthodologie des « Critères Communs »[19].

Concernant les différents cadres de certification utilisés en Europe, on ne constate pas véritablement d'évolution qui permettrait une convergence entre les organisations nationales et internationales. Si les fabricants de terminaux ne semblent pas marquer de préférence pour l'un ou l'autre modèle et sont surtout sensibles aux questions de coûts et de délais de mise sur le marché, les fabricants de cartes se montrent davantage habitués à des cadres de certification indépendants des systèmes de paiement par carte. Le choix de la méthodologie des « Critères Communs », s'il se généralisait, impliquerait toutefois une préférence naturelle pour un cadre de certification indépendant, comme c'est le cas en France aujourd'hui avec une autorité de certification placée sous l'égide des pouvoirs publics.

Enfin, l'instauration d'un mécanisme de gouvernance européenne, visant à assurer l'équivalence des certificats délivrés par les organismes de certification et leur reconnaissance mutuelle par les systèmes de paiement par carte au sein de l'espace SEPA, constitue le chantier le plus difficile. Les industriels y sont naturellement favorables, puisque cela leur permettrait de réduire leurs coûts et les délais de mise sur le marché. L'Eurosystème, tout comme la Commission européenne, ont marqué leur souhait de voir un tel mécanisme se mettre en œuvre. Il existe des initiatives qui sont encore à l'étude pour jeter les bases d'un organisme qui serait chargé de définir des critères d'éligibilité pour les laboratoires de test et les organismes de certification, sur la base d'exigences de sécurité communes et de méthodologies communes. L'enjeu pour un tel organisme sera toutefois de bénéficier de la légitimité et de la neutralité nécessaires pour imposer des règles d'équivalence à des acteurs de marché, qui sont par définition en position de concurrence.

Les banques centrales de l'Eurosystème suivent avec beaucoup d'intérêt les progrès réalisés par les acteurs du marché et ont pris l'initiative d'organiser des rencontres avec les différentes parties prenantes pour permettre un échange de vues sur les travaux en cours et favoriser l'émergence de positions communes. La Commission européenne vient pour sa part de lancer une consultation sur le sujet.

Conclusion

La construction de l'espace unique de paiement en euros représente un enjeu fort en termes de sécurité, dans la mesure où l'interopérabilité entre les différents systèmes de carte en Europe implique la définition de standards communs, dans un contexte de concurrence renforcé. Pour maintenir le haut niveau de sécurité atteint aujourd'hui en France et éviter un alignement par le bas, il est essentiel que les exigences de sécurité définies au niveau européen soient d'un niveau élevé et homogène.

[19] Travaux conduits par le « JTEMS » - *Joint Interpretation Library Terminal Evaluation Methodology Subgroup*, qui réunit des systèmes de paiement par carte (membres du groupe de travail CAS : Visa, MasterCard, Cartes Bancaires), des associations bancaires (APACS, ZKA), des autorités publiques (DCSSI et ses homologues anglais, allemand, hollandais) ainsi que des laboratoires de test accrédités « Critères Communs » et des experts de ce domaine.

Afin d'assurer la confiance des acteurs concernés dans le fait que les exigences sécuritaires prévues sont bien respectées, des dispositifs d'évaluation sécuritaire des cartes et des terminaux et de certification des résultats de ces évaluations sont mis en œuvre. Or les pratiques des différents pays européens et systèmes de paiement par carte en la matière obéissent aujourd'hui à des méthodologies et des règles d'organisation qui ne sont pas homogènes. Dans le cadre de SEPA, il est donc nécessaire d'harmoniser les procédures d'évaluation et de certification et de poser des critères d'équivalence pouvant servir de base à une reconnaissance mutuelle des certificats.

L'Observatoire salue les progrès réalisés par les acteurs du marché concernant la définition des exigences de sécurité applicables aux cartes et aux terminaux. Il constate également le maintien à ce stade des cadres de certification existants, ce qui renforce le besoin de disposer d'un mécanisme de gouvernance européenne en matière d'évaluation et de certification. Il soutient les travaux engagés à cette fin et invite à leur poursuite. En particulier, il souligne l'importance de mettre en place un mécanisme de gouvernance européenne approprié, pour parvenir à la définition de critères d'équivalence des certificats délivrés par les organismes de certification et à leur reconnaissance mutuelle par les systèmes de paiement par carte, et assurer ainsi la confiance des différents acteurs dans les paiements par carte effectués au sein de l'espace SEPA. L'Observatoire appelle de ses vœux une implication des autorités européennes et nationales pour définir rapidement un mécanisme de régulation européen qui pourrait être assuré par une autorité publique, et qui permette de maintenir la confiance du public en accompagnant les innovations technologiques.

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, modifié par le décret n° 2009-654 du 9 juin 2009, 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 les institutions assimilées et dont les fonctions sont le retrait ou le transfert de fonds. Elles ne couvrent pas les cartes monoprestataires bénéficiant d'une dérogation au monopole bancaire par l'article L. 511-7 I. 5 du Code monétaire et financier. Ces cartes, parfois appelées « cartes purement privatives », sont émises par un seul établissement et acceptées en paiement par lui-même ou par un nombre limité d'accepteurs ayant noué avec lui des liens de solidarité financière et commerciale.

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

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

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

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

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

– les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai (supérieur à 40 jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;

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

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

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

Attributions

Conformément à l'article L. 141-4 du Code monétaire et financier et au décret du 2 mai 2002 modifié par le décret n° 2009-654 du 9 juin 2009 précités, les attributions de l'Observatoire de la sécurité des cartes de paiement sont de trois ordres :

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

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

– il assure une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. A cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des cartes de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

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

Composition

Le décret du 2 mai 2002 précité modifié par le décret n° 2009-654 du 9 juin 2009 a déterminé la composition de l'Observatoire. Conformément à ce texte, l'Observatoire comprend :

– un député et un sénateur ;

– huit représentants des administrations :

– le gouverneur de la Banque de France ou son représentant ;

– le secrétaire général de la Commission bancaire ou son représentant ;

– dix représentants des émetteurs de cartes de paiement, notamment de cartes bancaires, de cartes privatives et de porte-monnaie électroniques ;

– cinq représentants du collège consommateurs du Conseil National de la Consommation ;

– cinq représentants des commerçants issus notamment du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;

– trois personnalités qualifiées en raison de leurs compétences.

La liste nominative des membres de l'Observatoire figure en annexe B.

Les membres de l'Observatoire autres que ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de la Commission bancaire sont nommés pour trois ans. Leur mandat est renouvelable.

Le président est désigné parmi ces membres par le ministre chargé de l'économie et des finances. Son mandat est de trois ans, renouvelable. Monsieur Christian NOYER, Gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément au décret du 2 mai 2002 modifié par le décret n° 2009-654 du 9 juin 2009, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté en 2003 un règlement intérieur qui précise les conditions de son fonctionnement.

Le secrétariat de l'Observatoire, assuré par la Banque de France, est chargé de l'organisation et du suivi des séances, de la centralisation des informations nécessaires à l'établissement des statistiques de la fraude sur les cartes de paiement, de la collecte et de la mise à disposition des membres des informations nécessaires au suivi des mesures de sécurité adoptées et à la veille technologique en matière de cartes de paiement. Le secrétariat prépare également le rapport annuel de l'Observatoire, remis au début de chaque année au ministre chargé de l'économie et des finances et transmis au Parlement.

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'économie et des finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail chargés, l'un d'harmoniser et d'établir des statistiques en matière de fraude, l'autre d'assurer une veille technologique relative aux cartes de paiement.

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat sont tenus de conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. A cette fin, l'Observatoire a inscrit dans son règlement intérieur l'obligation incombant aux membres de s'engager auprès du président à veiller strictement au caractère confidentiel des documents de travail.

ANNEXE B | LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

La composition de l'Observatoire a été définie par un arrêté du ministre de l'économie, des finances et de l'industrie du 20 avril 2006, complété par un arrêté du 22 juin 2006. Elle a été modifiée en 2007 par deux arrêtés en date du 27 juin et du 25 octobre 2007, ainsi qu'en 2009 par un arrêté en date du 29 juin 2009.

Liste des membres jusqu'au 20 avril 2009

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD
Député

Nicole BRICQ
Sénatrice

Représentant du secrétaire général de la Commission bancaire

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

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

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

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

- Le haut fonctionnaire de défense :
  Emmanuel SARTORIUS
  Claude MAUDELONDE

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

Sur proposition du ministre chargé de la consommation :

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

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Maxence DELORME
  Solène DUBOIS

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 – Mastercard France

Armand de MILLEVILLE
Vice président exécutif – American Express France

Jean-Marie DRAGON
Directeur marketing – Argent au quotidien - La Banque Postale

Bernard DUTREUIL
Directeur – Fédération bancaire française

Alain GOLDBERG
Directeur risques et conformité – Natixis Paiements

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

François LANGLOIS
Directeur des Relations institutionnelles – BNP Paribas Personal Finance

Jean-Christophe LEGALLAND
Groupement Carte Bleue

Cédric SARAZIN
Directeur Business et stratégie – Groupement des Cartes Bancaires

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

Michèle DAUPHIN
Représentante conseillère technique – Familles de France

Valérie GERVAIS
Secrétaire générale – Association FO Consommateurs (AFOC)

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

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

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

Représentants des organisations professionnelles de commerçants

Philippe JOGUET
Chef du service réglementation et développement durable – Fédération des entreprises du commerce et de la distribution (FCD)

Marc LOLIVIER
Délégué général – Fédération du e-commerce et de la vente à distance (Fevad)

Jean-Jacques MELI
Chambre de commerce et d'industrie du Val d'Oise

Jean-Marc MOSCONI
Délégué général – Mercatel

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

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL
Executive Vice-President – Gemalto

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

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

Liste des membres depuis le 29 juin 2009

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD
Député

Nicole BRICQ
Sénatrice

Représentant du secrétaire général de la Commission bancaire

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

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

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

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

- Le haut fonctionnaire de défense :
  Emmanuel SARTORIUS

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

Sur proposition du ministre chargé de la consommation :

- Le directeur de la direction générale de la concurrence, de la consommation et de la répression des fraudes ou son représentant :
  Brigitte HOUPPERT

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

- Le directeur des affaires criminelles et des grâces ou son représentant :
  Maxence DELORME
  Cédric SAUNIER

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

Yves BLAVET
Directeur de la monétique et du commerce électronique – Société Générale

Jean-Marc BORNET
Administrateur – Groupement des Cartes Bancaires

Jean-François DUMAS
Vice président – American Express France

Bernard DUTREUIL
Directeur – Fédération bancaire française

Bernard GOURAUD
Directeur des technologies – Banque Fédérale des Banques Populaires

François LANGLOIS
Directeur des Relations institutionnelles – BNP Paribas Personal Finance

Frédéric MAZURIER
Directeur administratif et financier – Société des Paiements Pass (S2P)

Gérard NEBOUY
Administrateur – Groupement Carte Bleue

Emmanuel PETIT
Président Directeur Général – Mastercard France

Narinda VIGUIER
Directeur – Stratégie et pilotage interbancaire – Crédit Agricole SA

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

Régis CREPY
Confédération nationale – Associations familiales catholiques (CNAFC)

Valérie GERVAIS
Secrétaire générale – Association FO Consommateurs (AFOC)

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

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

Représentants des organisations professionnelles de commerçants

Philippe JOGUET
Chef du service réglementation et développement durable – Fédération des entreprises du commerce et de la distribution (FCD)

Marc LOLIVIER
Délégué général – Fédération du e-commerce et de la vente à distance (Fevad)

Jean-Jacques MELI
Chambre de commerce et d'industrie du Val d'Oise

Jean-Marc MOSCONI
Délégué général – Mercatel

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

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL
Executive Vice-President – Gemalto

David NACCACHE
Professeur – Ecole normale supérieure

Sophie NERBONNE
Directeur adjoint à la direction des affaires juridiques, internationales et de l'expertise – Commission nationale de l'informatique et des libertés (CNIL)

ANNEXE 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 146 membres du Groupement des Cartes Bancaires « CB » par l'intermédiaire de celui-ci, ainsi que de MasterCard et du Groupement Carte Bleue pour les données internationales ;
- dix émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;
- les émetteurs du porte-monnaie électronique Moneo.

L'Observatoire a également reçu des statistiques recueillies par la Fevad auprès d'un échantillon représentatif de ses membres.

Total des cartes en circulation en 2008 : 84,7 millions

- dont 58,2 millions de cartes de type « interbancaire » (« CB » et Moneo) ;
- et 27,2 millions de cartes de type « privatif ».

Cartes mises en opposition en 2008 : environ 530 000

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

Le marché des cartes de paiement en France

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
Cartes de type « interbancaire »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiement de proximité et sur automate	5 770,62	264,43	125,04	9,46	146,05	13,03
Paiements à distance hors Internet	108,88	9,83	6,58	0,87	6,66	1,86
Paiements à distance sur Internet	211,35	16,04	50,59	3,04	13,27	1,59
Retraits	1 478,52	104,44	40,26	4,78	29,66	5,09
Total	**7 569,37**	**394,74**	**222,46**	**18,15**	**195,64**	**21,56**
Cartes de type « privatif »	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**	**Volume (millions)**	**Valeur (Md€)**
Paiement de proximité et sur automate	250,06	23,16	10,70	1,73	16,70	2,72
Paiements à distance hors Internet	4,81	0,36	0,02	0,00	0,03	0,01
Paiements à distance sur Internet	4,03	0,43	0,20	0,05	0,33	0,09
Retraits	11,80	1,04	nd	nd	nd	nd
Total	**270,70**	**24,98**	**10,93**	**1,79**	**17,07**	**2,82**
Total général	**7 840,07**	**419,73**	**233,39**	**19,93**	**212,71**	**24,37**

Source : Observatoire de la sécurité des cartes de paiement

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

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	**569,1**	**38 240,6**	**168,4**	**30 523,7**	**309,9**	**61 687,4**[1]
Cartes perdues ou volées	517,4	35 707,6	78,4	8 931,8	99,8	10 589,1
Cartes non parvenues	5,0	269,0	1,0	176,5	4,7	541,6
Cartes altérées ou contrefaites	46,7	2 264,0	77,6	18 963,1	67,3	24 778,3
Numéro de carte usurpé	0,0	0,0	6,6	1 840,1	77,0	15 209,1
Autres	0,0	0,0	4,8	612,3	61,2	10 569,3
Paiements à distance hors Internet	**395,6**	**28 060,1**	**51,7**	**8 940,3**	**nd**	**nd**
Cartes perdues ou volées	0,0	0,0	16,4	2 867,0	nd	nd
Cartes non parvenues	0,0	0,0	0,1	6,7	nd	nd
Cartes altérées ou contrefaites	0,0	0,0	14,2	2 700,5	nd	nd
Numéro de carte usurpé	395,6	28 060,1	13,8	1 945,2	nd	nd
Autres	0,0	0,0	7,2	1 420,9	nd	nd
Paiements à distance sur Internet	**274,6**	**38 501,2**	**418,5**	**55 543,6**	**nd**	**nd**
Cartes perdues ou volées	0,0	0,0	118,2	15 462,3	nd	nd
Cartes non parvenues	0,0	0,0	0,2	18,6	nd	nd
Cartes altérées ou contrefaites	0,0	0,0	115,7	16 353,0	nd	nd
Numéro de carte usurpé	274,6	38 501,2	140,9	17 432,2	nd	nd
Autres	0,0	0,0	43,6	6 277,5	nd	nd
Retraits	**78,7**	**18 117,2**	**113,9**	**19 075,9**	**18,3**	**5 579,9**
Cartes perdues ou volées	76,1	17 690,1	12,7	1 955,5	3,2	777,8
Cartes non parvenues	0,4	80,2	0,1	27,9	0,1	28,7
Cartes altérées ou contrefaites	2,3	346,8	100,8	17 039,2	14,7	4 691,9
Numéro de carte usurpé	0,0	0,0	0,2	31,3	0,2	49,5
Autres	0,0	0,0	0,1	21,9	0,1	32,1
Total	**1 318,0**	**122 919,1**	**752,5**	**114 083,6**	**328,2**	**67 267,3**

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 « Emetteur 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	**14,54**	**6 244,39**	**7,10**	**1 490,55**	**4,12**	**1 731,08**
Cartes perdues ou volées	6,38	1 427,24	1,34	311,59	0,99	405,56
Cartes non parvenues	1,90	390,81	0,12	57,07	0,13	39,80
Cartes altérées ou contrefaites	1,63	493,41	5,26	1 035,64	2,64	1 111,56
Numéro de carte usurpé	0,41	184,93	0,17	52,08	0,22	131,68
Autres	4,22	3 747,99	0,22	34,18	0,14	42,49
Paiements à distance hors Internet	**1,17**	**423,52**	**6,31**	**2 262,87**	**3,50**	**1 697,78**
Cartes perdues ou volées	0,08	49,35	0,11	20,39	0,12	42,30
Cartes non parvenues	0,03	4,80	0,01	7,40	0,02	2,07
Cartes altérées ou contrefaites	0,17	17,64	0,42	203,07	0,33	216,06
Numéro de carte usurpé	0,75	311,18	5,68	2 009,02	2,99	1 422,22
Autres	0,13	40,54	0,10	22,99	0,04	15,13
Paiements à distance sur Internet	**0,54**	**255,99**	**2,04**	**502,65**	**1,49**	**332,73**
Cartes perdues ou volées	0,11	84,32	0,02	1,67	0,03	6,36
Cartes non parvenues	0,04	23,35	ns	0,97	0,01	0,07
Cartes altérées ou contrefaites	0,02	1,82	0,11	12,11	0,09	18,84
Numéro de carte usurpé	0,32	131,43	1,87	483,99	1,35	306,50
Autres	0,05	15,07	0,03	3,92	0,01	0,97
Retraits	**3,90**	**1 007,57**	**0,02**	**2,09**	**nd**	**Nd**
Cartes perdues ou volées	3,41	826,94	nd	nd	nd	nd
Cartes non parvenues	0,33	131,77	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	0,02	2,09	nd	nd
Numéro de carte usurpé	0,00	1,54	nd	nd	nd	nd
Autres	0,15	47,32	nd	nd	nd	nd
Total	**20,14**	**7 931,47**	**15,47**	**4 258,16**	**9,11**	**3 761,59**

Source : Observatoire de la sécurité des cartes de paiement

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

Définition de la fraude

A des fins de recensement statistique, l'Observatoire estime qu'il convient de considérer comme constitutif de fraude :

Toute utilisation illégitime d'une carte de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation :

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

2. quels que soient :

- les moyens employés pour récupérer, sans motif légitime, les données ou le support de la carte (vol, détournement du support de la carte, des données physiques ou logiques, des données de personnalisation et/ou récupération du code secret, et/ou du cryptogramme, piratage de la piste magnétique et/ou de la puce…) ;
- les modalités d'utilisation de la carte ou des données qui lui sont attachées (paiement ou retrait, en paiement de proximité ou à distance, par utilisation physique de la carte ou du numéro de carte, sur automate…) ;
- la zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :
  - émetteur français et carte utilisée en France,
  - émetteur étranger et carte utilisée en France,
  - émetteur français et carte utilisée à l'étranger ;
- le type de carte de paiement, tel que défini à l'article L. 132-1 du Code monétaire et financier, y compris les porte-monnaie électroniques ;

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

[1] Dans le cas d'Internet, l'accepteur peut être différent du fournisseur de service, ou d'un tiers de confiance (paiements, dons effectués par des internautes en soutien d'un site, d'une idéologie…).

Typologie de la fraude

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

Les origines de fraude :

- *carte perdue ou volée :* le fraudeur utilise une carte de paiement obtenue à l'insu de son titulaire légitime, suite à une perte ou à un vol ;
- *carte non parvenue :* la carte a été interceptée lors de son envoi à son titulaire légitime par l'émetteur. Ce type d'origine se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut moins facilement constater qu'un fraudeur est en possession d'une carte lui appartenant et où il met en jeu des vulnérabilités spécifiques aux procédures d'envoi des cartes ;
- *carte falsifiée ou contrefaite :* une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation. La contrefaçon d'une carte suppose la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou une personne quant à sa qualité substantielle. Pour les paiements effectués sur automate de paiement, une telle carte, fabriquée par le fraudeur, supporte les données nécessaires à tromper le système. En commerce de proximité, une carte contrefaite est une carte fabriquée par un fraudeur, qui présente certaines sécurités (dont l'aspect visuel) d'une carte authentique, supporte les données d'une carte authentique et est destinée à tromper la vigilance d'un accepteur ;
- *numéro de carte usurpé :* le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (voir le paragraphe sur les techniques de fraude ci-dessous) et utilisé en vente à distance ;
- *numéro de carte non affecté :* utilisation d'un PAN[2] cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance ;
- *fractionnement du paiement :* action qui consiste à scinder le paiement en vue de passer en dessous des plafonds fixés par l'émetteur.

Les techniques de fraude :

- *skimming :* technique qui consiste en la copie, dans un commerce de proximité ou dans des distributeurs automatiques, des pistes magnétiques d'une carte de paiement à l'aide d'un lecteur à mémoire appelé « skimmer ». Éventuellement, le code confidentiel est également capturé de visu, à l'aide d'une caméra ou encore par détournement du clavier numérique. Ces données seront inscrites ultérieurement sur les pistes magnétiques d'une carte contrefaite ;
- *ouverture frauduleuse de compte :* ouverture d'un compte de référence en fournissant de fausses données personnelles ;
- *usurpation d'identité :* actes frauduleux liés à un paiement par carte et supposant l'utilisation de l'identité d'une autre personne ;
- *répudiation abusive :* contestation par le porteur, de mauvaise foi, d'un ordre de paiement valide dont il est l'initiateur ;
- *piratage d'automates de paiement ou de retrait :* techniques qui consistent à placer des dispositifs de duplication de cartes sur des automates de paiement ou des distributeurs automatiques de billets ;

2 *Personal Account Number*

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

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

Les types de paiement :

– *paiement de proximité*, réalisé au point de vente ou sur automate ;

– *paiement à distance* réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen ;

– *retrait* (retrait DAB ou autre type de retrait).

La répartition du préjudice entre :

– la banque du commerçant, acquéreur de la transaction ;

– la banque du porteur, émettrice de la carte ;

– le commerçant ;

– le porteur ;

– les éventuelles assurances ;

– et les autres types d'acteurs.

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

– l'émetteur et l'acquéreur sont, tous deux, établis en France. On dira également, dans ce cas, que la transaction est nationale ;

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

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

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 3 juillet 2009
Dépôt légal 3ème trimestre 2009
ISSN 1767-6665