FRAUDE SUR CARTES BANCAIRES*

“La sécurité permet de développer les services”

INTERVIEW

Marc Andries
Chef du Service de la surveillance des moyens de paiement scripturaux
Banque de France

Le taux de fraude des paiements de proximité par carte est très faible en France ; il est plus élevé pour les transactions à distance. La Banque de France a donc recommandé l’utilisation d’un code secret non rejouable, solution qui devrait également servir pour sécuriser les transactions de banque en ligne. Elle explique sa position sur ce dispositif qui va être généralisé à l’ensemble de la clientèle d’ici à juin 2010.

Pouvez-vous dresser un état des lieux de la sécurité des paiements par carte en France ?

Ce qui ressort des statistiques qui sont calculées chaque année par l’Observatoire de la sécurité des cartes de paiement [1], c’est la stabilité du niveau global de la fraude enregistrée dans les systèmes français (c’est-à-dire pour des cartes françaises utilisées en France et à l’étranger et pour des cartes étrangères utilisées en France). Le taux de la fraude s’établit en effet chaque année entre 0,065 et 0,070 %. Rapporté au volume de transactions par carte, c’est un pourcentage faible. En 2008, alors que le montant des transactions effectuées par cartes se montait à 461 milliards d’euros, la fraude représentait 320 millions d’euros (*encadré 1*).

Si l’on analyse plus en détail ces statistiques, on observe néanmoins des évolutions divergentes.

En premier lieu, l’écart s’accroît entre les taux de la fraude domestique (exercée en France avec des cartes françaises) et de la fraude internationale (celle portant sur des cartes françaises utilisées à l’étranger ou sur des cartes étrangères utilisées en France). Le premier est très bas : 0,031 %, ce qui est une bonne mesure du niveau de qualité de la sécurité des cartes françaises, tandis que le second s’élève en 2008 à 0,427 %. L’importance de la fraude internationale s’explique par le fait que certains pays ne sont pas encore passés à la carte à puce ou que parfois les systèmes des banques ne filtrent pas ce genre de transactions.

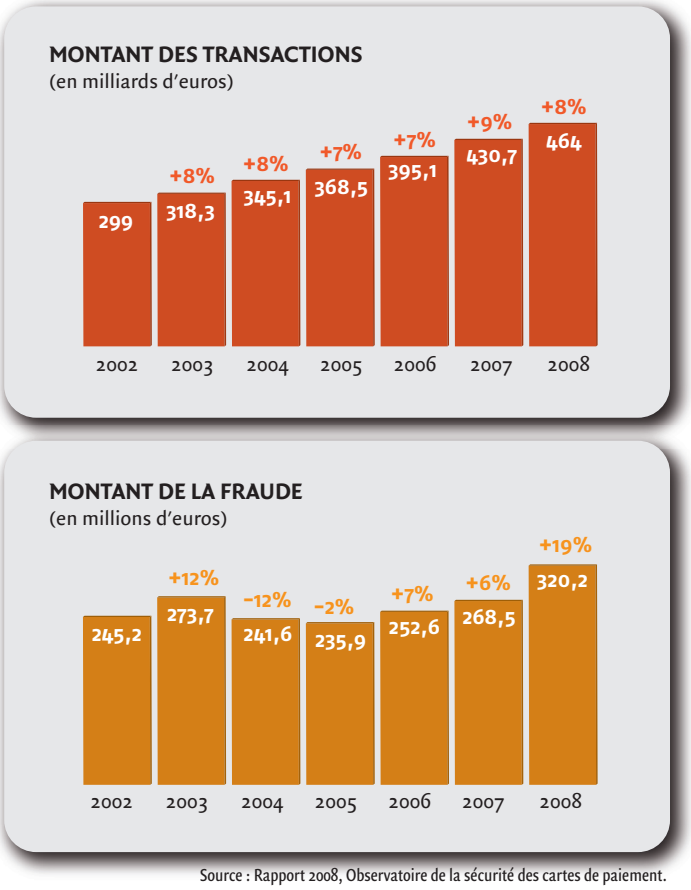
En deuxième lieu, il y a maintenant un écart très net entre la fraude enregistrée sur les paiements de proximité ou sur automates, et celle qui cible le paiement à distance (par Internet, par téléphone ou par courrier). La fraude constatée en France chez les commerçants en

* Voir sur le même sujet le Cahier techno de *Revue Banque* n°718.

[1] Observatoire de la sécurité des cartes de paiement, rapport 2008, *www.observatoire-cartes.fr*

1. ÉVOLUTION DES MONTANTS DE TRANSACTIONS ET DE FRAUDE

Pour des cartes françaises utilisées en France et à l'étranger, et pour des cartes étrangères utilisées en France



Source : Rapport 2008, Observatoire de la sécurité des cartes de paiement.

paiement de proximité et dans les automates diminue jusqu'à un niveau jamais atteint : 44,5 millions d'euros, soit un taux de fraude de 0,015 %. Cette baisse illustre la disparition du phénomène de la "Yescard" [2] suite à la mise en œuvre des mesures de lutte contre la contrefaçon demandées par la Banque de France. Ce renforcement des mesures amène les fraudeurs à se tourner davantage vers les paiements à distance qui sont, pour l'instant, moins sécurisés (*encadré 2*).

■ Qu'en est-il pour les paiements à distance ?

Pour les paiements nationaux par carte effectués à distance, c'est-à-dire par internet, téléphone ou courrier, le taux de fraude est de 0,252 %, correspondant à 67,2 millions d'euros. Ce phénomène est encore plus accru pour les paiements internationaux puisque la fraude sur les paiements à distance enregistrée pour des cartes françaises chez des commerçants étrangers augmente très significativement et atteint un taux de fraude de 1,698 %, équivalent à un montant de fraude de 67,2 millions d'euros. Ces taux sont en augmentation de manière inquiétante.

En juillet 2008, le gouverneur de la Banque de France a donc recommandé aux banques de mettre en place des solutions de sécurité pour les paiements à distance. Il s'agit de solutions d'authentification non rejouable, c'est-à-dire fondées sur l'utilisation de codes à usage unique. Ce type de solution permet de s'assurer que le numéro de la carte n'a pas été usurpé, tout comme le permet la saisie du code confidentiel sur le terminal d'un commerçant ou sur un automate. Pour le paiement à distance, notamment sur Internet, il n'est pas question de saisir son code confidentiel car il serait vraisemblablement vite récupéré par des logiciels espion. C'est pourquoi l'on parle d'authentification non rejouable : le code qui sert au porteur pour s'authentifier n'est valide qu'une seule fois, de sorte que s'il est récupéré par un fraudeur, celui-ci ne pourra pas s'en servir.

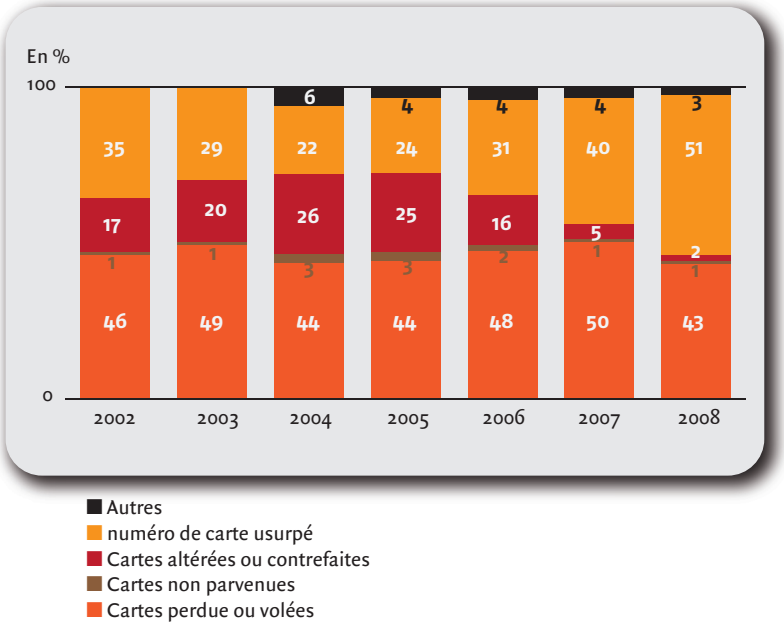
■ Où en sont les banques dans la mise en application des codes à usage unique ?

Les banques avaient jusqu'à juin 2009 pour commencer à déployer ce type de solution auprès de leur clientèle ; elles devront achever ce déploiement pour juin 2010. À cette date, l'ensemble de la clientèle bancaire sera ainsi dotée de solutions d'authentification non rejouable pour pouvoir effectuer des paiements sur Internet sécurisés et aussi s'en servir pour effectuer des opérations sensibles sur la banque en ligne, notamment comme des virements (*encadré 3*). L'idée est d'utiliser les mêmes solutions de sécurisation pour les paiements à distance et la banque en ligne, de façon à simplifier les démarches des utilisateurs.

[2] Une YesCard est une carte à puce, vierge à l'origine, dans laquelle un programme et des données spécifiques sont programmées par un pirate. Elle se comporte comme un émulateur de carte bancaire, elle simule parfaitement son fonctionnement, à la différence près qu'elle accepte n'importe quel code à 4 chiffres (source : wikipédia).

3. RÉPARTITION DE LA FRAUDE SELON SON ORIGINE

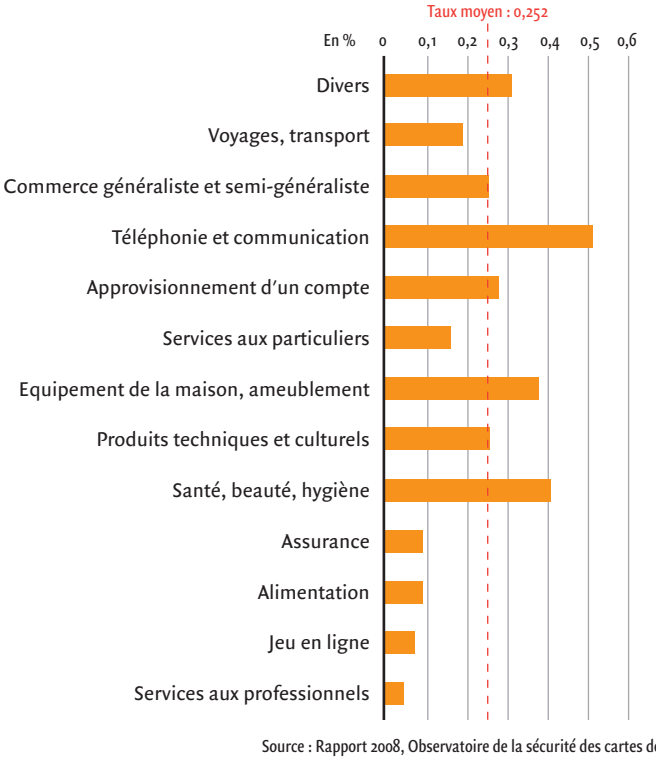
Transactions nationales, en valeur



Source : Rapport 2008, Observatoire de la sécurité des cartes de paiement.

2. TAUX DE FRAUDE SUR LES PAIEMENTS À DISTANCE

Résultats classés par secteur d'activité pour les transactions nationales



Source : Rapport 2008, Observatoire de la sécurité des cartes de paiement.

■ Avez-vous des recommandations sur le choix d'une solution spécifique ?

Sur le plan technique, nous n'attendons pas une solution plutôt qu'une autre. En pratique, les banques travaillent sur deux types de solutions : soit l'envoi d'un code à usage unique sur le téléphone portable par SMS, grâce à un dialogue entre le site marchand et celui de la banque ; soit l'équipement de la clientèle par un boîtier qui génère ce code unique en utilisant la carte bancaire du client. Ces deux solutions répondent aux attentes de la Banque de France.

■ Que pensez-vous des nouvelles formes de paiement comme celles développés sur téléphone mobile ?

La Banque de France veut aider au développement de nouveaux produits et à l'innovation, mais elle est attachée à ce que cela se fasse dans un contexte de sécurité. Il est important de penser la sécurité très en amont, comme cela s'est fait pour les cartes sans contact pour lesquelles la Banque de France a fait part de ses recommandations. De la même façon, nous discutons à l'heure actuelle avec les promoteurs du paiement sans contact par téléphone.
Nous tenons compte des spécificités de chaque type de solution de paiement innovante. Il faut par exemple protéger l'environnement informatique et télécom qui est utilisé pour éviter les usurpations, les intrusions ou les contrefaçons.

■ Les représentants du commerce craignent que trop de sécurité ne freine le commerce à distance dans un contexte qui est déjà à la morosité économique…

Aujourd'hui, la fraude sur les canaux à distance est supportée par les commerçants qui l'intègrent dans leurs coûts et leurs prix. Je pense, et certaines enquêtes tendent à le montrer que les clients sont disposés à utiliser des solutions sécurisées. Beaucoup se posent la question de savoir comment faire des achats sur Internet sans craindre pour leur compte ou leurs données de paiement. Il faut leur apporter une réponse ; le monde du commerce a son rôle à jouer pour habituer sa clientèle à utiliser les solutions de sécurité qui sont fournies par le monde bancaire. La Banque de France veille à ce que les solutions d'authentification non rejouable soient faciles à utiliser par les clients. Elle ne souhaite pas créer de frein pour le développement du commerce électronique. Bien au contraire, il s'agit de permettre qu'il continue à se développer en rendant disponibles des solutions adaptées en termes de sécurité.

> “Il est important, et cela fait partie des recommandations de la Banque de France, que les établissements français se préparent à [la] concurrence [européenne] en allant vers davantage de services.”

■ Quelle est la situation à cet égard dans les autres pays européens ?

Les pays du nord de l'Europe utilisent déjà depuis plusieurs années des solutions d'authentification non rejouable pour la banque en ligne. Cela a permis le développement de nombreux services, comme des souscriptions de produits, jusqu'à un stade beaucoup plus avancé que ce qui est possible en France où le client repasse généralement à un moment ou un autre en agence pour faire les vérifications nécessaires.

Dans le monde du paiement, la directive sur les services de paiement et le Sepa créent les conditions d'un marché européen totalement intégré. Dans deux ou trois ans, il y aura davantage de concurrence entre les acteurs européens, qui pourront prospecter des marchés au-delà de leur territoire national tout en fonctionnant sur les plateformes de leur pays d'origine, car les moyens de paiement auront été standardisés et les règles juridiques harmonisées. Il est important, et cela fait partie des recommandations de la Banque de France, que les établissements français se préparent à cette concurrence en allant vers davantage de services. Nous voyons l'introduction de cette sécurité comme un moyen de développer des services plus nombreux en ligne.

■ Existe-t-il une démarche d'harmonisation de la sécurité en Europe ?

Les régulateurs de plusieurs pays, principalement en Scandinavie, au Bénélux, en Allemagne, en Autriche, au Royaume-Uni et désormais aussi en France, ont demandé au secteur bancaire, quand il ne l'avait pas déjà fait, de mettre en place de telles mesures de sécurité. L'Eurosystème vient également de se prononcer en ce sens. Les mesures demandées par les régulateurs reposent toutes sur l'authentification non rejouable qui paraît la mieux adaptée pour les transactions à distance. En revanche, les régulateurs n'imposent pas telle ou telle solution d'authentification, le choix est laissé entre plusieurs solutions techniques possibles ; l'existence de plusieurs solutions peut compliquer la vie des fraudeurs. Le mouvement est en cours depuis longtemps dans d'autres pays et c'est pourquoi il s'inscrit en France dans un calendrier réaliste de mise en œuvre entre 2009 et 2010. Au-delà de l'Europe, de tels dispositifs sont également demandés par les autorités, comme par exemple aux États-Unis, à Hong Kong ou à Singapour. ■