FRAUDES À LA CARTE BANCAIRE
Sensibliser les commerçants

Myles Simpson

Responsable sécurité et fraude Europe du Sud

MasterCard Europe

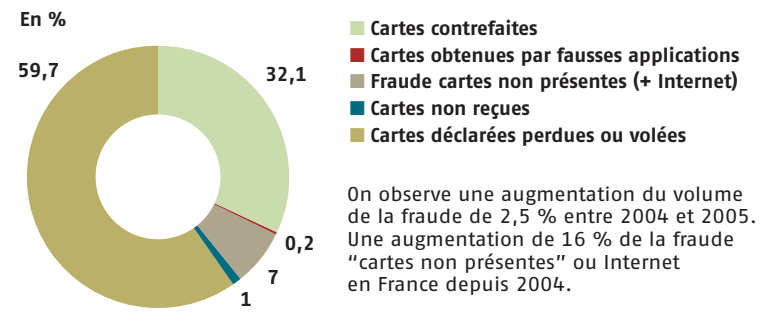
L'industrie des paiements a édicté des directives en matière de sécurité sur les transactions dans les points de vente. Celles-ci restent mal connues des commerçants. Il y a urgence à mieux les diffuser.

Communément, il est admis que les problèmes de vol dans les magasins de détail concernent essentiellement le vol dans la caisse ou dans les stocks. Pour s'en protéger, les commerçants ont mis en place des systèmes de sécurité, investi dans des polices d'assurance et appliqué une politique d'embauche susceptible de réduire ce risque. Mais, aujourd'hui, un nouveau type de délit prend de l'ampleur : le vol des informations personnelles des clients, plus spécifiquement les informations de leurs cartes bancaires utilisées lors des transactions dans le point de vente.

Les commerces collectent et stockent des données concernant leurs clients et ces informations sont d'une grande valeur pour l'activité commerciale. Elles leur permettent de s'adresser plus efficacement aux clients, d'adapter les prix et de gérer le stock. Mais, lorsque le traitement de l'information n'est pas sécurisé, il peut donner lieu à des utilisations frauduleuses. De nos jours, les criminels n'attaquent plus les caisses et les coffres-forts. Ils préfèrent exploiter les vulnérabilités des systèmes informatiques des commerces, afin de voler les fichiers, voire piller les disques durs contenant les informations liées aux transactions des clients.

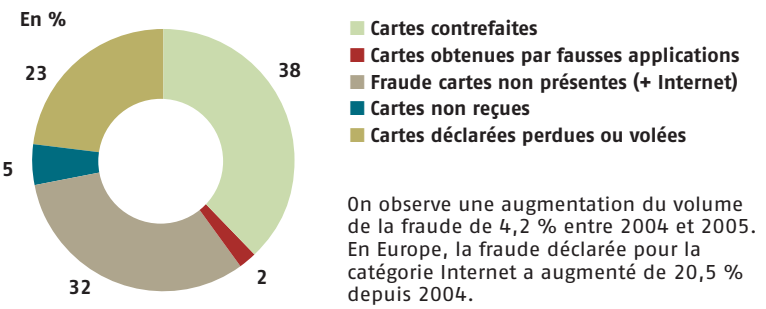
FRAUDE DÉCLARÉE PAR LES BANQUES EN 2005

Sur les cartes MasterCard émises en France



On observe une augmentation du volume de la fraude de 2,5 % entre 2004 et 2005. Une augmentation de 16 % de la fraude "cartes non présentes" ou Internet en France depuis 2004.

Sur les cartes MasterCard émises en Europe



On observe une augmentation du volume de la fraude de 4,2 % entre 2004 et 2005. En Europe, la fraude déclarée pour la catégorie Internet a augmenté de 20,5 % depuis 2004.

Source : MasterCard.

COÛTS SUPPLÉMENTAIRES ET PRÉJUDICE D'IMAGE

Ces actions de pillage informatique, mettant en cause la sécurité des données, font régulièrement les gros titres des journaux. Empê-

« Les spécifications en matière de sécurité ne sont pas toujours partagées avec les prestataires technologiques des commerces qui ont parfois accès à des données clients importantes. »

cher le vol des informations des cartes bancaires représente un défi pour les commerçants, les institutions financières et les consommateurs. Ces derniers courent le risque de se faire voler l'information de leur carte de crédit et de voir leur compte bancaire débité pour des transactions qu'ils n'ont pas réalisées. Les banques, quant à elles, sont exposées à des coûts supplémentaires pour faire face à ces fraudes et les commerçants, enfin, doivent faire face à de sérieux préjudices d'image.

Pourtant, nombre de commerçants ne prennent pas conscience de la vulnérabilité de leurs systèmes informatiques avant d'être effectivement confrontés à une brèche de celui-ci. Tous les acteurs de la chaîne transactionnelle doivent prendre des mesures proactives, afin de protéger les données clients, avant tout dommage : les banques acquéreuses et les commerçants.

DES SPÉCIFICATIONS INSUFFISAMMENT RELAYÉES

Une brèche est souvent le résultat d'un manque d'information sur l'importance de la sécurisation du traitement des données et sur les méthodes disponibles pour leur protection. Les spécifications de l'industrie des paiements en matière de sécurité n'ont probablement pas été suffisamment relayées auprès des commerçants, rendant ainsi aléatoire la diffusion des bonnes pratiques en termes de sécurisation des données.

De plus, ces spécifications ne sont pas toujours partagées avec les prestataires technologiques des commerces. Les entreprises fournissant aux commerçants les infrastructures informatiques pour le traitement des transactions ont parfois accès à des données clients importantes, dont la sécurité risque dès lors d'être compromise. Ces prestataires doivent également prendre des mesures appropriées pour sécuriser les informations des cartes de paiement auxquelles ils ont accès.

Cependant, de nombreux efforts sont actuellement entrepris pour changer cette situation. Les réseaux internationaux de cartes bancaires fournissent généralement des supports d'information et des ressources, afin d'aider les banques et les commerçants dans cette tâche.

UNE MEILLEURE COMMUNICATION

L'industrie des paiements dans son ensemble s'attache à mieux communiquer auprès des commerçants et de tous les acteurs concernés, afin de les sensibiliser à la protection des données des cartes bancaires et d'éviter les brèches des systèmes de traitement des données. Les commerçants sont, dès lors, en mesure de communiquer les directives ayant trait à la sécurité des données au sein de leur organisation, de poser les bonnes questions à leurs fournisseurs informatiques et de mettre en place des procédures susceptibles de réduire le risque de brèche.

L'application des directives de l'industrie des paiements, la compréhension des nécessaires procédures de sécurité et le partage des meilleures pratiques pour la protection des données transactionnelles réduisent considérablement les risques de vulnérabilité des commerçants. Les données de l'industrie indiquent que près de 90 % des fraudes intervenant sur des comptes bancaires pourraient être évitées, si les commerçants suivaient à la lettre les directives imposées par l'industrie des paiements par cartes (*encadré 1*).

C'est en travaillant ensemble que les acteurs de la chaîne des paiements pourront avoir un impact positif sur la protection des données des paiements par carte bancaire. ■

SÉCURITÉ DES TRANSACTIONS

Des règles de sécurité simples

Quelques règles de sécurité simples que les commerçants devraient suivre lors de l'évaluation de leurs systèmes internes de traitement des transactions :

1. Installer un *firewall* pour la protection des données ;
2. Changer les mots de passe mis en place par défaut par les prestataires informatiques ;
3. Protéger les données stockées des détenteurs de carte ;
4. Ne jamais mémoriser la piste magnétique ou le code CVC2 (code 2 de vérification du détenteur de carte) d'une carte ;
5. Crypter les données du détenteur de carte lors de transferts de données sur les réseaux informatiques ;
6. Utiliser des logiciels antivirus ;
7. Développer et utiliser des systèmes et des applications sécurisées ;
8. Assigner un nom d'utilisateur unique et un mot de passe à chaque personne ayant accès au système informatique ;
9. Limiter l'accès physique et virtuel aux données aux personnes habilitées ;
10. Tester et contrôler régulièrement l'efficacité des dispositifs de sécurité ;
11. Surveiller tous les accès aux ressources du réseau et aux données des détenteurs de carte ;
12. Mettre en place une politique stricte de sécurisation de l'information.

Pour plus d'information sur les règles concernant la protection des données chez MasterCard, nous vous invitons à visiter le site www.mastercardmerchant.com.