## Fraude à la carte bancaire

# « Mieux vaut prévenir que guérir »

**JEAN-MICHEL SCHNEIDER**
Directeur commercial ACI Worldwide

L'identification du « point faible », c'est-à-dire les emplacements où se produisent les piratages, est une méthode novatrice pour la prévention des fraudes à la carte bancaire.

La fraude à la carte bancaire, et en particulier le piratage en magasin (*skimming*), est l'un des problèmes auxquels certaines banques européennes doivent encore faire face. Comme l'ont constaté les banques les plus novatrices, l'identification du « point faible » (*point of compromise* ou POC) est d'une grande importance dans la lutte contre les fraudes à la carte bancaire. Il est désormais clair que cette identification doit être utilisée plus largement et se voir attribuer davantage d'importance.

Plus de 4 571 fraudes par *skimming* ont été enregistrées en 2006. Pour les banques d'Europe, elles se sont traduites par une perte dépassant les 305 millions d'euros[1]. Pour contrer cette tendance croissante, l'idéal serait que les banques puissent identifier dans leur clientèle les cartes les plus exposées aux fraudes, et agir avant qu'un problème ne se produise. Ce scénario peut paraître utopique, mais il n'est pas irréalisable. Il existe déjà des solutions qui permettraient aux banques de reprendre le contrôle et de battre les fraudeurs à leur propre jeu.

La détection du POC est la principale méthode utilisable pour la prévention des fraudes à la carte bancaire. Le POC est le lieu où se produit le piratage des informations concernant la carte (numéros et codes), dans le but de soutirer de l'argent au compte. Il fait toujours référence à un terminal : si le piratage s'est produit en plusieurs points chez le même marchand, on parle de plusieurs POC au même emplacement.

### Prévenir plutôt que réagir

L'identification des POC est tellement capitale qu'elle permet aux institutions financières de dégager les tendances et de définir des règles en fonction des emplacements où se produisent les piratages. Cependant, l'intérêt majeur des POC n'apparaît que lorsqu'ils permettent d'identifier les possibilités de fraudes assez tôt pour que la banque puisse prendre des mesures préventives afin de protéger les cartes à risques avant le vol. Dans ce cas, la détection des POC et l'application de contre-mesures peuvent réduire de plus de moitié les pertes par incident, avec un minimum d'efforts.

### Identification des POC

Pour identifier les POC, la banque doit disposer d'un nombre suffisant de cartes qui ont subi des transactions frauduleuses confirmées. Si le nombre de cartes est trop faible, l'identification est moins certaine, mais un POC peut souvent se localiser avec juste deux ou trois cartes. Les cartes piratées apportent des informations très utiles sur l'historique des dépenses, et l'existence d'un point d'achat commun devrait commencer à se dégager. Il faut que ce point précède la première transaction frauduleuse, et que toutes les cartes aient été utilisées au même emplacement, sur le même terminal et dans une même période. Plus les dates d'achat sont éloignées, plus la probabilité est faible qu'il s'agisse du vrai POC.

### Que faire après une identification ?

Lorsque, pour plusieurs cartes, un emplacement commun et une même période ont été identifiés, il faut déterminer quels sont les autres titulaires de cartes soumis

1. European ATM Crime Report 2006, The European ATM Security Team (EAST).

au même risque, en appliquant la « fenêtre de piratage ». Cette fenêtre est la période qui va de la première à la dernière transaction de carte sur le POC considéré. Elle s'allonge si, pour d'autres cartes, de nouvelles transactions frauduleuses apparaissent. À partir de cette fenêtre, il faut interroger la base de données des transactions de la banque, pour connaître les autres cartes qui ont été utilisées sur le même terminal et dans cette même période.

### Bloquer ou ne pas bloquer les cartes à risque ?

Une fois qu'on a obtenu la liste des cartes à risques, il faut décider de l'action à entreprendre. À ce moment, les banques hésitent souvent entre l'impact sur le client et la prévention des fraudes. Il est clair qu'un plus grand nombre d'actions préventives impliquera davantage de clients. Les banques ont cependant plusieurs possibilités, avec des impacts différents. Selon l'emplacement du POC, la banque peut choisir de « bloquer » ou de « surveiller » les cartes à risques ou bien de ne rien faire... Si le POC se trouve dans une chaîne de vente à hauts risques, où les fraudes confirmées sont fréquentes, la banque peut décider que bloquer les cartes et les renouveler limitera l'impact sur le client. Au contraire, si le POC n'entre pas dans une catégorie à hauts risques, ou que le nombre de cartes impliquées est insuffisant pour établir une certitude, la banque peut choisir de simplement surveiller les cartes à risques. Toute nouvelle activité sur ces cartes sera considérée comme suspecte et rapportée à l'équipe anti-fraude.

> *« Pour identifier les POC, la banque doit disposer d'un nombre suffisant de cartes qui ont subi des transactions frauduleuses confirmées. »*

### Utiliser les bons outils

Les méthodes mentionnées plus haut peuvent avoir un impact considérable sur les pertes résultant des fraudes. En revanche, elles peuvent aussi augmenter la charge de travail du personnel. L'identification des POC et l'initiation d'actions sur un grand nombre de cartes peuvent s'avérer difficiles et lourdes si l'on utilise des procédures manuelles. La seule façon d'identifier les POC et de les gérer correctement est de faire appel à un outil de gestion des risques conçu dans ce but. Une autre possibilité est d'utiliser une solide suite de gestion des risques, intégrant la fonction POC en standard. L'interface donne accès aux alertes identifiées et générées automatiquement par le système, dès qu'il détecte un POC probable. Le système affiche le POC et une liste des cartes « à risques », afin que le responsable puisse les analyser. Ensuite, lorsque la décision est prise sur les actions à entreprendre, le système permet d'agir rapidement sur une ou plusieurs cartes. En quelques clics, le responsable peut placer une « surveillance » sur les cartes considérées moins risquées, et « bloquer » les autres. Les cartes à surveiller sont placées automatiquement dans une liste qui peut être consultée lors de l'écriture de règles. Les solutions les plus puissantes peuvent également consulter les fraudes des marchands. Ainsi, les emplacements reconnus pour des actions frauduleuses sont renvoyés dans le système de l'émetteur, pour identifier automatiquement les cartes à risques. Pour combattre les malversations futures, il est essentiel de pouvoir introduire des contre-mesures à partir de données exactes sur les tendances des fraudes.

Les institutions financières rencontrent actuellement plusieurs problèmes. La sécurité est l'un deux, notamment pour les fraudes à la carte bancaire, mais c'est aussi l'un des domaines importants pour la compétitivité à long terme des banques. Elles devront toujours ménager un équilibre entre l'impact sur le client et la prévention de fraudes, mais comme le dit le proverbe, *« mieux vaut prévenir que guérir »*. Pour préserver ou regagner la confiance et la fidélité de leurs clients, les banques d'Europe devront de plus en plus appliquer cet adage dans le cadre de leurs stratégies de sécurité. ■

### Solution proposée par ACI

■ **ACI Proactive Risk Manager** est une solution complète de détection des risques permettant d'évaluer les risques en quasi-temps réel ou temps réel, sur l'ensemble des activités et des comptes clients d'une institution. Dotée d'un éventail de fonctions, allant des règles définies par l'utilisateur à la technologie de réseau neuronale en passant par la gestion automatisée des dossiers, elle offre les moyens de réduire les pertes de manière économique, tout en limitant l'exposition aux risques.