Cartes et guichets automatiques
L'évaluation des risques

GILBERT LOUARD
Responsable marketing secteur banque, NCR

La fraude à la carte bancaire et aux automates est un phénomène mondial. Les risques les plus connus concernent la carte et le code confidentiel, mais d'autres domaines nécessitent une attention continue pour ne pas devenir les points faibles de la chaîne de sécurité.

Au cours de ces récentes années, l'industrie bancaire a fait des efforts considérables pour améliorer la sécurité de l'utilisation des cartes de paiement, et le récent rapport de l'Observatoire de la fraude à la carte de paiement montre que le taux de fraude reste limité. Ceci n'empêche pas de considérer tout incident de compromission comme un échec de la prévention et nous rappelle la nécessité de maintenir l'avance sur les fraudeurs qui agissent comme des gangs internationaux aux moyens financiers conséquents.

Les évolutions autour de la carte, avec l'introduction des spécifications EMV et de la protection du code confidentiel, avec les nouvelles méthodes de gestion des systèmes cryptographiques, ont renforcé la sécurité des éléments personnels de l'utilisateur dans les systèmes de paiement et de retrait. Les fraudeurs se concentrent maintenant vers les points les plus faibles. Ceci est dans la tradition de l'évolution du glaive et du bouclier. Les contre-mesures traditionnelles passives arrivent à la limite de leurs possibilités ; il est désormais nécessaire de prévoir des solutions actives de détection qui permettent d'agir sans délai contre les fraudeurs.

Enjeux

L'augmentation des cas d'usurpation d'identité, avec en corollaire la fraude aux guichets automatiques, constitue sans aucun doute un des plus grands défis du secteur. Au-delà des pertes financières qu'elle provoque, elle est aussi – et surtout – susceptible d'affecter la confiance du client.

Ce délit financier qui ne connaît pas de frontières a ainsi un essor sans équivalent au niveau mondial. Il est le fait de professionnels bénéficiant de vastes ressources financières ainsi que de réseaux bien établis, et liés au crime organisé. Mais qu'est-ce que l'usurpation d'identité ? Il en existe plusieurs définitions, mais la plus simple est de considérer qu'il y a usurpation d'identité lorsqu'un malfaiteur s'approprie des informations personnelles de quelqu'un d'autre et les utilise ensuite pour faire des achats ou capter ses liquidités. Cela se traduit non seulement par d'importantes pertes sèches pour les organismes financiers, mais aussi par une perte de temps pour le consommateur qui devra passer des heures, voire des semaines ou des mois, à prouver qu'il n'est pas à l'origine de ces dettes et de ces achats.

La collaboration des industries EMV

La collaboration sectorielle est la clé du succès pour réduire le risque d'usurpation d'identité. Les pouvoirs publics compétents et le gouvernement, ainsi que des structures privées, luttent non seulement contre la criminalité, mais collaborent également avec les consommateurs et les entreprises afin de mieux comprendre le phénomène et de déployer des contre-mesures collectives.

La France est depuis longtemps partisane de l'utilisation des cartes à puce. Grâce à son introduction dans les années quatre-vingt-dix, elle a connu un recul spectaculaire de la fraude sur son territoire.

Usurpation d'identité et fraude aux GAB

Quel est le lien entre l'usurpation d'identité et le problème croissant de

la fraude aux guichets automatiques ? Il n'existe que peu d'estimations du coût global qu'engendre la criminalité aux guichets automatiques, et rares sont les pays qui publient ce type de données. Toutefois, selon Gartner, ces coûts atteindraient les 2,5 milliards de dollars US par an.

Le guichet automatique est un dispositif subissant à la fois la compromission et la fraude. L'usurpation d'identité et le vol d'informations personnelles peuvent y prendre différentes formes :

- le *« card skimming »*, lorsque le fraudeur installe un dispositif de copie sur le lecteur de carte (ou autour de celui-ci) pour copier les informations de la bande magnétique ;
- le *« card trapping »*, lorsque le malfaiteur pose un « collet marseillais ». Ce dispositif consiste à piéger la carte à l'intérieur du lecteur et à en récupérer le code confidentiel (soit avec l'installation d'une caméra à proximité du clavier, ou par la simple observation lors de la saisie). La carte est ensuite récupérée par le fraudeur et peut être utilisée à un guichet automatique (mais pas uniquement) qui devient ainsi un point de fraude.
- Une carte authentique ou falsifiée peut être utilisée par un malfaiteur pour des retraits d'espèces. Les données copiées sur une carte falsifiée – carte de téléphone ou bancaire –, tout comme le code confidentiel, ont pu être obtenus ailleurs par usurpation d'identité.

En Europe, le Royaume-Uni est un haut lieu de ce type de fraude, et plus spécifiquement du *skimming*. En 2005, le *card skimming* a, pour la première fois, baissé de 34 % pour atteindre le chiffre de 96,8 millions de livres sterling, soit environ 174 millions de dollars US. Par ailleurs, les malfaiteurs professionnels ont été longtemps actifs en Amérique du Sud.

> *« Le guichet automatique est un dispositif subissant à la fois la compromission et la fraude. L'usurpation d'identité et le vol d'informations personnelles peuvent y prendre différentes formes : le « card skimming » ou le « card trapping »*

Quel est dès lors le coût global de la fraude aux guichets automatiques ? Il se détaille en deux parties. D'une part, les pertes sèches et, de l'autre, les coûts liés à la fraude. Ceux-ci incluent les pertes réelles, les frais d'émission d'une nouvelle carte, de changement de code confidentiel, la remise en état du guichet et le manque à gagner encouru tant au niveau des transactions que des frais et des commissions pendant la période d'inactivité de la carte. D'autre part, moins facile à chiffrer mais plus important, l'impact potentiel sur le consommateur.

L'évaluation du risque parle d'elle-même. On sait que les guichets automatiques constituent le véhicule bancaire le plus utilisé au monde, puisque 60 à 80 % des transactions financières traditionnellement effectuées en agence s'y déroulent désormais.

Les mesures antifraudes

Diverses contre-mesures permettant de lutter contre la fraude peuvent actuellement être mises en place pour sécuriser le réseau et protéger l'utilisateur. De multiples technologies et services basés sur une expérience et un savoir-faire touchant aux méthodes criminelles et frauduleuses à travers le monde peuvent être adaptées aux exigences individuelles des exploitants de guichets automatiques.

Voici un bref aperçu de certaines de ces mesures : premièrement, la conformité aux normes. L'intérêt du secteur pour la technologie à puce et l'EMV va certainement mettre à mal la fraude aux cartes bancaires.

Deuxièmement, apparaissent les cartes sans contact à côté des cartes traditionnelles. Rien qu'aux États-Unis, on compte déjà quelque 17 millions de cartes sans contact. À l'instar des cartes conventionnelles, celles-ci bénéficieront à terme de la norme EMV pour assurer une sécurité et une interopérabilité globales.

Ensuite, la technologie sans contact a déjà connu une forte croissance dans la grande distribution et les transports. Conscients que cette évolution constitue un pas important dans la conquête du marché des paiements qui s'effectuent actuellement en espèces, les émetteurs de cartes encouragent les clients à y recourir. Des initiatives intersectorielles vont également stimuler l'utilisation des technologies sans contact, qui paraissent particulièrement attrayantes alors même que le secteur cherche à encourager

Émergence de nouvelles leçons

L'évolution constante des méthodes de fraude aux guichets automatiques permet de tirer de nouvelles leçons.

- La fraude et la criminalité ne connaissent pas de frontières, qu'elles soient nationales ou internationales.
- De plus en plus, la solution à certains de ces problèmes implique une importante coopération sectorielle, dans des domaines tels que la conscientisation du client ou le déploiement des cartes à puce qui ont notamment eu lieu au Royaume-Uni, et récemment au Canada.
- Les transferts frauduleux de fonds ont attiré l'attention des pouvoirs législatifs, et les utilisateurs de guichets automatiques doivent être sensibilisés aux questions de conformité.
- Les multiples facettes des fraudes impliquent la nécessité d'une approche intégrée de la sécurité aux guichets automatiques.
- Toutefois, les mesures de sécurité peuvent être coûteuses et pas toujours opportunes lorsqu'elles sont généralisées. La vulnérabilité des guichets automatiques varie selon les régions, les pays, l'emplacement et la configuration.

Il est nécessaire d'élaborer des modèles de protection en fonction des guichets.

Une sécurisation intégrée combinée à des stratégies de hiérarchisation des risques constitue la clé du succès dans l'évolution de la sécurisation des guichets automatiques.

le recours aux cartes de paiement, et qui offrent à leurs utilisateurs des avantages concrets combinant confort et rapidité. Un rapport du groupe Aite montre que CVS, grande chaîne de drugstores aux États-Unis, a découvert qu'une transaction sans contact dure en moyenne 12,5 secondes, contre 26,7 secondes pour une transaction par carte de paiement à bande magnétique et à contact, et 33,7 secondes pour un achat payé en espèces.

En termes de sécurité, le fait que la carte ne quitte plus la main de l'utilisateur élimine les fraudes traditionnelles mentionnées plus haut. D'autres questions de sécurité restent d'actualité, comme la nécessité de garantir la conformité aux normes.

La même étude montre que dans les magasins CVS, la valeur d'un achat moyen avec paiement sans contact est actuellement 20 % plus élevée que celle d'un achat payé en espèces. L'enjeu sous-jacent consiste bien entendu à capter l'ensemble des petits achats (en liquide), qui représente une part importante des transactions. Ainsi, 86 % des paiements effectués dans les points de vente européens s'effectuent-ils en billets ou espèces, pour des montants variant, au Royaume-Uni, entre 2 et 20 euros dans 42 % des cas.

Selon Datamonitor, ce marché est estimé à 226 milliards de dollars US. Fin 2005, Frost & Sullivan estimaient à 15 000 le nombre de détaillants aux États-Unis qui acceptaient les paiements par carte Visa sans contact, et à 25 000 le nombre de détaillants qui acceptaient le paiement par PayPass MasterCard. Quelque 4,3 millions de cartes PayPass sont aujourd'hui en circulation. L'adoption massive de la technologie sans contact par les détaillants, les marchands et les consommateurs aux États-Unis engendre un intérêt croissant pour les paiements par carte sans contact.

L'attitude des consommateurs

Afin de mieux appréhender la manière dont le consommateur perçoit la sécurité des guichets automatiques face à l'augmentation des fraudes, NCR a commandité une étude indépendante sur les attitudes des consommateurs dans des zones clés à travers le monde. Globalement, lorsqu'on leur demande de décrire les guichets automatiques, 73 % des consommateurs américains les qualifient de pratiques, 63 % les trouvant en outre faciles à utiliser. Un nombre appréciable de consommateurs américains (39 %) sont au courant de l'ajout de pièges, et 34 % ont entendu parler d'au moins un vol de données commis dans le cadre d'un paiement chez un commerçant à des fins de fraude au guichet automatique. Les consommateurs se disent ainsi inquiets à l'idée d'utiliser ce type de canal, même s'il est intéressant de constater que 19 % d'entre eux ne partagent toujours pas ce sentiment. Les consommateurs doivent être informés des risques, ainsi que des contre-mesures les plus adéquates à adopter pour protéger leur code confidentiel et leurs coordonnées bancaires.

Interrogés sur une éventuelle adaptation de leur comportement, 68 % des consommateurs conscients des fraudes aux guichets automatiques ont répondu ne pas avoir changé leurs habitudes, tandis que 32 % ont avoué utiliser ce canal moins souvent qu'auparavant.

> *« En termes de sécurité, le fait que la carte ne quitte plus la main de l'utilisateur élimine les fraudes traditionnelles. D'autres questions de sécurité restent d'actualité, comme la nécessité de garantir la conformité aux normes. »*

Une étude menée en Australie montre que 92 % des consommateurs se sentiraient plus rassurés s'ils savaient que les guichets automatiques intègrent des dispositifs anti-fraudes. De quoi faire réfléchir les banques, qui voient l'intérêt à promouvoir auprès de leurs clients les mesures de sécurité prises en la matière. ■