

Les banques, victimes ou complices de la fraude dans le commerce en ligne ?

Par Jean-Luc Wernoth, fondateur Store Factory.

Sujet majeur pour le commerce en ligne car directement lié au résultat net des e commerçants, la fraude poursuit sa progression en France. L'observatoire de la sécurité des paiements chiffrait **le taux de fraude sur les paiements à distance sur Internet en 2007 à 0,28%** sur l'ensemble des transactions nationales, pour un montant de 26,4 millions d'Euros, multiplié par deux par rapport à 2006. Les premiers chiffres annoncés récemment par la Fevad indiquent **une poursuite de la hausse des transactions frauduleuses, à la fois en nombre et en valeur**. Cette hausse est directement liée bien sûr à la croissance continue du volume et de la valeur des paiements à distance via Internet, au rythme actuel de 30% par an. Mais elle témoigne aussi d'un problème récurrent de sécurité, non réglé à ce jour.

Pour arriver à leurs fins, les fraudeurs emploient essentiellement deux techniques : l'usurpation d'identité, qui consiste à utiliser un numéro de carte bancaire à l'insu de son détenteur légitime, et la répudiation des transactions après réception de la marchandise. Cette possibilité leur est offerte par la loi, comme c'est le cas dans la plupart des pays d'Europe du Sud et en Amérique du Nord. En effet, la législation française actuelle sur la vente à distance protège efficacement le consommateur en cas d'utilisation frauduleuse de sa carte bancaire, en lui garantissant un remboursement dans la grande majorité des cas. Et c'est le commerçant qui supporte intégralement la charge d'une fraude éventuelle, dans la mesure où le consommateur n'a pas saisi de code secret lui permettant de s'identifier avec certitude comme il pourrait le faire avec un terminal de paiement physique dans un magasin. Les banques ne sont exposés qu'indirectement au risque, en cas de défaillance du commerçant lui-même.

Généraliser 3D Secure d'ici Juin 2010

Pour régler ces problèmes de sécurité, la communauté bancaire mondiale, comme le GIE Carte bancaire en France par exemple, recommande depuis le début des années 2000 la mise en place d'une authentification forte des acheteurs pour les transactions à distance.

Après plusieurs années de gestation, la solution se présente enfin avec la mise en œuvre effective en ce début 2009 d'un nouveau protocole de paiement sécurisé connu sous le nom de 3D Secure.

Imaginé à l'origine par Visa en 2003, puis adopté par Mastercard, son principe est simple : lors de la transaction, l'internaute doit saisir en plus un code personnel, comme il le ferait sur un terminal de paiement classique, qui garantit qu'il est bien le porteur de la carte.

Concrètement, le protocole 3D Secure introduit, en plus du site marchand et de l'acheteur, une troisième partie – d'où son nom – dans la validation d'une transaction sur Internet : la banque du porteur. La cinématique d'un paiement sur un site marchand s'en trouve donc changée : validation du panier ; saisie du numéro de CB dans la fenêtre ad hoc ; saisie d'un mot de passe complémentaire dans une nouvelle fenêtre, affichée par la banque du porteur.

En contrepartie, l'acheteur ne peut plus faire jouer son droit de répudiation (le paiement est effectif dans un délai de trois jours maximum), et le commerçant est assuré de bien toucher quoiqu'il arrive la totalité de la transaction. En cas de litige, c'est désormais la banque qui supporte l'ensemble du risque.

L'utilisation effective du protocole 3D Secure a débuté en France à l'automne 2008, et l'objectif de la Banque de France est de généraliser son usage par l'ensemble des banques françaises d'ici Juin 2010.

Une mise en œuvre laborieuse

Or, neuf mois après son introduction, force est de constater que le bilan de l'adoption de 3D Secure, tant du point de vue de la mise en œuvre du protocole que des solutions techniques choisies, est loin d'être satisfaisant. Ce qui éveille déjà des craintes quant au réalisme de la date butoir de Juin 2010.

Les banques françaises ont commencé à mettre 3D Secure en application depuis Octobre 2008, et tous les grands établissements ont sauté le pas au cours du dernier trimestre de l'année dernière. Mais elles l'ont fait le plus souvent en catimini, sans réelle politique de communication tant auprès des commerçants que des cyberacheteurs sur les avantages qu'ils pouvaient tirer du nouveau système.

D'autre part, certaines banques parmi les plus importantes ont adopté en fait de code d'authentification la simple date de naissance de leurs clients. Cette solution permet certes aux internautes de se familiariser facilement avec le paiement 3D Secure, mais offre une garantie de sécurité pour le moins aléatoire.

Du côté des e commerçants, la migration vers le nouveau protocole de paiement s'est fait en ordre dispersé, ce qui a clairement désavantagé les premiers adeptes du nouveau système. En effet, imposant à leurs clients une étape supplémentaire de saisie du code personnel, perçue comme contraignante, ceux-ci ont constaté lors de l'activation de 3D Secure une baisse du taux de transformation (abandon de l'achat au niveau du panier) allant jusqu'à 30%.

D'autre part, la responsabilité des fraudes étant transférée à la banque avec 3D Secure, la plupart de celles-ci ont prévu de nouvelles dispositions contractuelles leur permettant de mettre fin très rapidement à un contrat de vente à distance avec un commerçant en cas de taux de fraude « anormal ». Celui-ci court donc le risque de se voir supprimer les moyens de paiement de son site marchand de façon soudaine et aléatoire.

Enfin, beaucoup d'internautes ne comprennent pas pourquoi on leur demande un code personnel sur certains sites et pas sur d'autres, faute d'une réelle communication des banques sur ce sujet.

Par conséquent, beaucoup de sites marchands aujourd'hui encore traînent les pieds et refusent d'adopter le nouveau protocole, en arguant que *'la résolution de 0,2% de leurs problèmes ne vaut la perte de 20% de leurs commandes'*. De même, les professionnels du secteur recommandent de conserver les systèmes de 'scoring' comme Fia Net pour limiter les fraudes.

Sites marchands et banquiers se renvoient la balle

Alors à qui la faute ? Sites marchands et banquiers se renvoient la balle, chacun considérant que c'est à l'autre d'expliquer au client final les avantages de 3D Secure.

Beaucoup de sites marchands ont clairement adopté une stratégie attentiste, et n'adhéreront à 3D Secure que lorsqu'il sera suffisamment généralisé, en limitant les risques avant.

Les banques, de leur côté, se hâtent lentement, ce qui est compréhensible dans la mesure où 3D Secure leur fait supporter l'ensemble du coût de la fraude. Pourquoi pousserai-elles un système qui les défavorise ?

Les banques doivent s'engager

In fine, tous les acteurs, banquiers, commerçants et internautes, ont intérêt à une généralisation la plus rapide possible de l'usage de 3D Secure, seule capable de limiter la fraude à un niveau « maîtrisable ».

Responsables en pratique de la mise en œuvre du nouveau protocole, les banques sont seules capables de donner l'impulsion et doivent s'engager rapidement et sans réserve en faveur de 3D Secure. Elles doivent le faire d'une part via une politique de communication énergique en direction de leurs clients. Et d'autre part en mettant en place de processus à la fois simples et parfaitement sécurisés pour les consommateurs, qui tiennent compte dans le même temps des contraintes des commerçants.

Contacts Presse :

Agence HL.COM

Shamina Peerboccus: 01.45.00.97.14 / speerboccus@hl-com.com

Hervé Lobry : 01.45.00.97.11 / hlobry@hl-com.com

Store Factory

Jean-Luc Wernoth : 01.78.94.28.12 / jean-luc.wernoth@store-factory.com