

10 millions \$ d'amende pour négligence sur la sécurisation des data

La très redoutée FTC (Federal Trade Commission) vient de faire un exemple: et elle a eu la main lourde! Il est vrai que le cas est sérieux: vol d'informations confidentielles, sur des comptes bancaires, des cartes de crédit, etc.

La présidente de la FTC, Deborah Platt Majoras, a souligné que c'était là la plus forte amende jamais infligée. La commission fédérale a également exigé le versement de 5 millions de dollars à un fonds destiné à indemniser des victimes de ce genre d'incidents. La firme devra également se plier à un contrôle d'audit sur ses procédures de sécurisation, tous les deux ans durant les 20 prochaines années! « *C'est une victoire importante pour les consommateurs* », a estimé la présidente, citée par le Wall Street Journal. « *Cela signifie aux compagnies qu'elles doivent protéger les données sensibles dont elles ont la garde. Elles doivent protéger la porte d'entrée comme la porte de derrière contre les 'hackers' [pirates de systèmes informatiques]* » On se souvient que ChoicePoint héberge les données de fournisseurs de crédits: agences gouvernementales, études notariales ou autres instances détenant des informations personnelles et confidentielles nécessaires à l'obtention de prêts ou de divers financements. ChoicePoint avait reconnu publiquement en février 2005 avoir été victime d'un acte de piraterie sur des fichiers contenant des informations concernant 160.000 consommateurs. En fait, l'incident s'était produit quelques mois auparavant, durant l'automne 2004. La firme avait alors cherché à minimiser les faits en évoquant un « *petit nombre de criminels très bien organisés, se présentant comme des compagnies officielles afin d'avoir ainsi accès à des informations confidentielles* ». Depuis lors, on a appris que ChoicePoint a modifié ses structures de bases de données, procédant notamment au masquage et au tronçonnage d'informations sensibles, comme les numéros de sécurité sociale ou de permis de conduire! De source sûre, on sait que la firme détient également des numéros de comptes bancaires et cartes de crédit. Judiciairement, l'amende s'applique en vertu du non respect du *Fair Credit Reporting Act* (FCRA). Au delà des défaillances dans son système de sécurisation des données, il était reproché à ChoicePoint d'avoir fait de fausses déclarations sur ses procédures internes. **Un 'back-up' sur 350.000 patients volé dans une voiture...**

Après CardSystems, ChoicePoint, la série noire continue... Computerworld révèle ce 26 janvier qu'un lot de disques et de bandes de sauvegarde contenant des informations confidentielles portant sur 365.000 patients des Etats de l'Oregon et de Washington, a été dérobé dans la voiture d'un employé d'un centre de soins. Le transfert, en voiture, de ces data au domicile de l'employé faisait partie de la procédure de sécurité. Le vol qui s'est déroulé à son domicile, le mois dernier, a été déclaré le 31 décembre 2005. L'annonce en a été faite par l'organisme Providence Home Services, filiale de Providence Health Systems, basé à Seattle. Les données dérobées concernent une partie de l'activité du centre de soins, celle des soins à domicile. Les informations sauvegardées n'étaient pas encryptées, mais enregistrées dans un format propriétaire « *difficilement lisible* », ont argué les responsables du centre de soins. Ces informations contenaient les noms, adresse, date de naissance, nom du médecin traitant, références sur les assurances sociales, les prescriptions médicales, les diagnostics ou résultats d'analyses en laboratoire. Les deux tiers des enregistrements comportaient le numéro de sécurité sociale et, pour un certain nombre d'entre eux (non encore établi), des informations bancaires. La déclaration de l'incident a été faite dans le

délai de 4 semaines imposé par la nouvelle réglementation aux Etats-Unis. Cette semaine, un **incident similaire** a été rapporté: un employé d'une société de conseil en financement, Ameriprise, à Mineapolis, s'est fait voler en décembre dernier, dans sa voiture garée dans un parking, son PC portable. Celui-ci contenait des informations confidentielles (numéros de comptes, numéros de sécurité sociale) sur 158.000 clients, et 68.000 conseillers financiers.