Le vol d'identité : Les entreprises doivent également se prémunir contre ce fléau

1 décembre 2007

Auteur

Raymond Doray

Associé, Avocat

QU'EST-CE QU'UN VOL D'IDENTITÉ?

Le vol d'identité consiste à obtenir et à utiliser de façon frauduleuse l'identité d'une personne dans le but de commettre des fraudes ou d'autres activités criminelles. On peut notamment voler une identité en subtilisant le courrier d'une personne, en cambriolant sa résidence, en reproduisant des données personnelles relatives à une transaction par carte de crédit ou par chèque, en utilisant des « hameçons » sur Internet, en volant les ordinateurs d'une entreprise ou d'un gouvernement ou encore, en s'introduisant subrepticement dans leurs dossiers informatisés. On voit aussi de plus en plus de vols d'identité qui découlent de fraudes effectuées par téléphone alors que des renseignements (numéros de compte, numéros de carte de crédit, numéros d'identification personnels, etc.) sont obtenus sous de faux prétextes.

L'AUGMENTATION DES VOLS D'IDENTITÉ

Le vol d'identité est devenu l'une des formes de crime qui connaît la croissance la plus rapide au Canada et aux États-Unis. Le nombre de plaintes déposées à ce sujet auprès de la Federal Trade Commission des États-Unis a quintuplé entre les années 2000 et 2002, passant de 31 000 à plus de 160 000 plaintes. En 2006, près de 8 000 victimes ont déclaré des pertes de 16 millions de dollars à *PhoneBusters*, le centre d'appels anti-fraude du gouvernement du Canada. On estime que de nombreux autres cas ne sont pas signalés. Le Conseil canadien des bureaux d'éthique commerciale a estimé que le vol d'identité pourrait coûter aux consommateurs, aux banques, aux sociétés émettrices de cartes de crédit, aux détaillants et aux autres entreprises du Canada plus de 2 milliards de dollars annuellement.

Les données accessibles laissent croire que ce phénomène prend de l'ampleur et qu'au cours de la prochaine décennie, il sera un des éléments les plus importants de la criminalité transfrontalière et menacera des dizaines de millions de personnes et d'entreprises au Canada et aux États-Unis.

LES RISQUES DE POURSUITES POUR LES ENTREPRISES

Au-delà des coûts directs, le vol d'identité est susceptible de mettre en cause la responsabilité des entreprises s'il s'avère qu'une faute a été commise, notamment parce que les mesures adéquates n'ont pas été prises pour empêcher la divulgation de renseignements personnels. La rapidité et la nature de la réaction de l'entreprise dans le but d'atténuer les effets de ce type de crime pour les consommateurs pourraient également être considé- rées par les tribunaux, soit pour établir une faute, soit pour évaluer les dommages. Ceux-ci pourraient, du reste, s'avérer importants parce que le recours collectif est un moyen procédural utilisé de plus en plus par les victimes de vol d'identité dans le but de faire compenser par les entreprises ou les gouvernements les dommages qu'elles ont subis. Ces recours allèguent généralement que l'on n'a pas pris toutes les précautions raisonnables afin d'éviter que les renseignements personnels requis pour commettre des vols d'identité ne soient pas divulgués, que les victimes n'ont pas été averties avec diligence pour leur permettre d'annuler leurs cartes de crédit ou d'avertir leurs institutions financières ou que ces événements leur ont causé du stress et de l'anxiété.

UN RÉCENT CAS D'INTRUSION INJUSTIFIÉE

Récemment, le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information et à la protection de la vie privée de l'Alberta ont émis un rapport d'enquête conjoint sur la sécurité, la collecte et la conservation de renseignements personnels par la chaîne de magasin Winners. Le réseau informatique de la maison mère de Winners, TJX Companies Inc., avait fait l'objet d'une intrusion touchant des renseignements personnels d'environ 45 millions d'utilisateurs de cartes de crédit au Canada, aux États-Unis, à Puerto Rico, au RoyaumeUni et en Irlande à la fin de l'année 2006. Des numéros de cartes de crédit, y compris des dates d'expiration, des noms, des adresses et des numéros de client ainsi que des numéros de permis de conduire ont été illégalement obtenus par des tiers qui se sont introduits à plus d'une reprise, semble-t-il, sur les systèmes informatiques de TJX.

Au terme de leur enquête, les commissaires à la vie privée du Canada et de l'Alberta ont conclu que l'entreprise en question a contrevenu aux dispositions des lois canadienne et albertaine relatives à la protection des renseignements personnels en recueillant des numéros de permis de conduire et d'autres renseignements personnels non nécessaires lorsque les clients rapportent de la marchandise, et en conservant ces renseignements ainsi que des renseignements portant sur des transactions par carte de crédit durant une période excessive. Les commissaires ont cependant jugé que la nouvelle procédure mise en place par l'entreprise, après les évé- nements, qui consiste à décomposer par voie cryptographique les numéros d'identification des clients, notamment les numéros de permis de conduire, était adéquate et aurait pu éviter de mettre en péril la vie privée des consommateurs concernés ou de favoriser le vol d'identité si elle avait été adoptée plus tôt.

L'OBLIGATION D'ADOPTER LES TECHNOLOGIES LES PLUS SÉCURITAIRES

Ce qui est tout particulièrement intéressant et inusité dans ce rapport d'enquête, c'est que les organismes de surveillance fédéral et albertain ont reproché à TJX/Winners de ne pas avoir mis en place des mesures de sécurité informatiques adéquates, eu égard aux technologies existantes sur le marché. L'entreprise utilisait un protocole de chiffrement peu fiable selon les commissaires et n'a pas adopté une norme d'encryptage plus évoluée dans un délai raisonnable. Si elle avait suivi un protocole de chiffrement de niveau supérieur et surveillé ses systèmes de façon attentive, le risque de brèche aurait été atténué d'écrire les commissaires.

Autrement dit, il ne suffit pas pour les entreprises et les gouvernements d'avoir des systèmes de sécurité de leurs données informatiques et de leurs dossiers physiques. Ils doivent suivre les développements technologiques pour être à la fine pointe et empêcher les intrusions injustifiées, surtout lorsque les renseignements en cause ont un haut niveau de sensibilité. Les méthodes de chiffrement ou d'encryptage les plus performantes doivent donc être adoptées puisque les fraudeurs sont toujours à l'affût et qu'ils sont en mesure de s'introduire dans les systèmes qui sont plus

vulnérables, moins sophistiqués et moins avancés d'un point de vue technologique.

QUOI FAIRE ET QUOI DIRE AUX CLIENTS?

D'aucuns se demanderont s'il n'est pas préférable pour les entreprises qui font l'objet d'une intrusion injustifiée ou d'un vol de renseignements personnels de ne pas en informer les clients ou autres personnes concernées afin de ne pas les inquiéter indûment, de ne pas risquer de mettre en péril la relation de confiance qu'ils ont avec l'entreprise ou encore, pour éviter de fournir aux organisations de défense des consommateurs une occasion d'instituer des procédures judiciaires au nom d'un groupe de victimes.

Nous ne pouvons souscrire à une telle approche qui, du reste, contrevient au principe de transparence qui s'impose aux entreprises en vertu de la Loi sur la protection des renseignements personnels et des documents électroniques.

S'il y a effectivement eu intrusion injustifiée dans une base de données, vol de courrier, de dossiers ou de renseignements personnels, etc., les personnes concernées ont le droit d'en être informées afin de pouvoir se prémunir le plus rapidement possible contre les conséquences de ces actes, par exemple les fraudes. Les assureurs de l'entreprise devraient également être avisés dans les meilleurs délais.

Dans la plupart des cas, une lettre des dirigeants de l'entreprise devrait être transmise avec diligence à chaque client ou personne dont les renseignements personnels ont vraisemblablement fait l'objet d'une intrusion ou d'un vol, afin de les informer de la situation et de porter à leur attention différents moyens à prendre pour éviter de faire l'objet d'une fraude. Ces moyens sont notamment :

> les inviter à faire preuve de vigilance relativement aux transactions qu'ils ont faites dans les mois précédents ou qu'ils seraient appelés à faire à l'avenir;
> les encourager à obtenir régulièrement une copie de leur dossier de crédit pour s'assurer que des demandes de crédit n'ont pas été effectuées en leur nom et sans leur accord;
> leur suggérer d'aviser leur institution financière, compagnie émettrice de leur carte de crédit ainsi que le centre d'appels national *PhoneBusters* qui constitue le centre d'appels antifraude du Canada;
> leur proposer de consulter au besoin le site www.securitecanada.ca/identitytheft_f.asp pour obtenir des conseils afin de réduire les risques de vol d'identité ainsi que des réponses aux questions généralement posées par les consommateurs à ce sujet.

Pour sa part, l'entreprise qui a fait l'objet d'un vol de renseignements personnels ou d'une intrusion injustifiée devrait avertir les principales agences d'évaluation de crédit du Canada qui ont développé des protocoles permettant de rapporter les vols d'information de manière à ce que les dossiers de crédit des consommateurs visés soient mis sous surveillance immédiatement. Un avis de fraude est alors inscrit au dossier de crédit de ces personnes et indique aux éventuels créanciers qu'ils doivent communiquer avec le consommateur lui-même avant d'accorder du crédit, d'ouvrir un compte ou de modifier les comptes existants. L'entreprise serait également bien avisée d'informer les corps policiers de l'existence du crime dont elle a fait l'objet.

La lettre transmise par l'entreprise aux clients visés pourrait d'ailleurs leur faire part des démarches qui ont été entreprises en ce sens. Il serait également opportun d'indiquer dans cette correspondance le nom et les coordonnées d'une personne responsable au sein de l'entreprise avec laquelle les clients pourront communiquer en tout temps.