

Série des maîtres

Il s'agit d'un des articles d'une série préparée pour Gestion privée de patrimoine CIBC^{MC}. Ces articles sont rédigés par des experts de divers domaines, dont la fiscalité, les fiducies et les successions.

PROTÉGEZ-VOUS CONTRE L'USURPATION D'IDENTITÉ

Par Norman D. Inkster, O.C., BA (spéc.), C.St.J, LL.D, président, Inkster Group

Il y a dix ans, l'usurpation d'identité était à peu près inconnue. Par contre, en 2004, ce crime insidieux a coûté aux Canadiens près de 19 millions de dollars selon les statistiques de PhoneBusters, une agence nationale de détection des fraudes exploitée par la Police provinciale de l'Ontario.

L'usurpation d'identité est un phénomène inhabituel en ce sens que les victimes ne se rendent compte qu'elles ont été volées que bien après le fait. La Federal Trade Commission aux États-Unis signale que 26 % des victimes d'une usurpation d'identité ne se rendent compte du méfait qu'après un à cinq mois, tandis que 12 % des victimes ne le constatent qu'après plus de six mois. D'ici

à ce que vous constatiez le vol, votre cote de crédit pourrait être ruinée, et il vous faudra peut-être des années pour remédier à la situation.

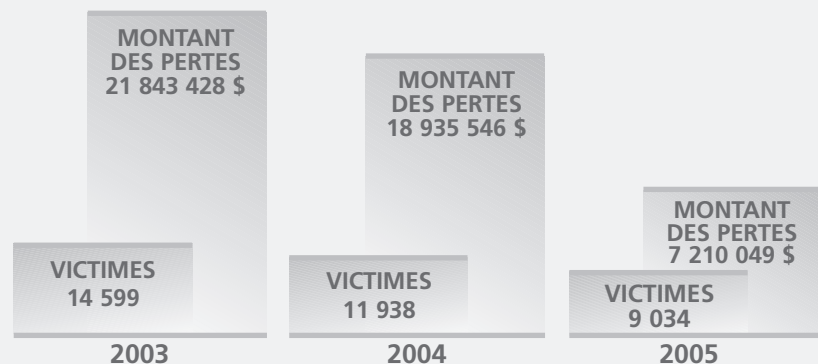
Heureusement, vous pouvez prendre des mesures pour protéger votre réputation et votre cote de crédit et empêcher l'usurpation de votre identité par des criminels. La protection de vos renseignements personnels et la sécurité de votre ordinateur et de votre accès Internet sont prioritaires. Vous devez en outre vérifier soigneusement tous vos relevés de comptes bancaires et de cartes de crédit.

Que recherchent les voleurs?

Un usurpateur d'identité vole des renseignements personnels à votre sujet lui

Le coût élevé des fraudes

Bien que le nombre de victimes et le montant des pertes attribuables à l'usurpation d'identité tendent à diminuer, ils demeurent tout de même très élevés.



Source : PhoneBusters, 1^{er} novembre 2005 (www.phonebusters.com)

Norman D. Inkster, président de Inkster Group, une division de Gowlings Consulting Inc., qui offre des services professionnels, comme des enquêtes, des services de renseignements et des évaluations de la sécurité et du risque. M. Inkster a occupé le poste de commissaire à la Gendarmerie royale du Canada de 1987 à 1994 et de président d'Interpol de 1992 à 1994. Avant de rejoindre les rangs de Gowlings, il a agi comme associé directeur mondial au sein du service de juricomptabilité d'un grand cabinet d'experts-comptables à l'échelle internationale.

Fraude : un crime d'envergure internationale

Les fraudes, les escroqueries et les usurpations d'identité font des ravages partout dans le monde. Dans le cadre d'un récent incident, la police espagnole a mis au jour une fraude ayant contribué à soutirer des millions de dollars à environ 500 Canadiens et Américains.

Dans la plupart des cas, les victimes avaient reçu une lettre leur faisant croire qu'elles avaient gagné un lot de la fameuse loterie espagnole de Noël «El Gordo». Pour avoir la possibilité d'encaisser leur prix, les gagnants devaient envoyer une somme d'argent destinée à couvrir les taxes et les frais de manutention, atteignant dans certains cas jusqu'à 26 000 \$.

Nul besoin de préciser que les «fameux lots» ne se sont jamais matérialisés. Conclusion : n'envoyez jamais d'argent et ne donnez jamais de renseignements personnels en vue d'obtenir un prix potentiel.

permettant de se faire passer pour vous. Les usurpateurs d'identité sont intéressés par votre numéro d'assurance sociale (NAS) et votre permis de conduire, ainsi que par les renseignements sur vos comptes bancaires et cartes de crédit. Vous pouvez même ne pas vous rendre compte qu'on vous a volé quelque chose puisque, contrairement à un vol habituel, le voleur recherche les renseignements accessibles par vos pièces d'identité, plutôt que les pièces d'identité elles-mêmes.

Grâce à ces renseignements, le voleur peut utiliser votre carte de crédit et votre compte bancaire pour faire des achats et des retraits, allant même jusqu'à vous dérober toutes vos économies. Certains criminels font pire encore, utilisant votre identité non seulement pour avoir accès à vos comptes existants, mais pour ouvrir de nouveaux comptes de carte de crédit à votre nom. À une occasion, le criminel a même utilisé l'information pour obtenir un prêt hypothécaire grevant la maison de la victime (consultez l'étude de cas n° 1).

Bien que nous puissions tous être victimes d'une usurpation d'identité, les mieux nantis représentent des cibles plus intéressantes. Les gens ayant une valeur nette élevée ont habituellement une marge de crédit plus importante et ils sont

plus susceptibles de détenir des biens considérables non grevés d'une hypothèque, notamment des biens immobiliers.

Ils peuvent également être moins à l'affût des fraudes, surtout si leur argent est géré par des tiers. Et plus une personne est aisée, plus elle a à perdre aux mains d'un usurpateur d'identité.

Comportement criminel

Afin de bien vous protéger, vous devez avant tout comprendre comment les usurpateurs d'identité procèdent. Voici quelques scénarios que préfèrent les escrocs.

Écrémage. Lorsque vous réglez une addition au restaurant ou payez un achat dans un magasin avec une carte de crédit ou de débit, celle-ci est rapidement passée dans un «dispositif servant à l'écrémage» avant le traitement légitime de la facture. Le dispositif enregistre les renseignements personnels figurant sur la bande au verso de la carte. Les renseignements ainsi obtenus sont utilisés pour acheter des produits ou des services sur Internet ou par téléphone, ou utilisés de façon frauduleuse s'ils sont encodés dans de fausses cartes de crédit ou de débit. (Consultez l'étude de cas n° 2.)

Vols de cartes ou de documents de paiement. Les usurpateurs d'identité volent des nouvelles cartes de crédit ou des demandes de carte de crédit préapprouvées dans votre boîte aux lettres. Les «pêcheurs de poubelles» fouillent dans les

Étude de cas n° 1 – Fraude hypothécaire

Jean et Marie Dupont* ont vécu très heureux pendant des années, persuadés que leur maison était libre de toute dette hypothécaire. Lorsqu'ils ont décidé de la vendre, ils ont constaté avec stupéfaction qu'un fraudeur l'avait à leur insu grevée d'une hypothèque.

Les imposteurs avaient remis de fausses pièces d'identité à la banque, dont les numéros d'assurance sociale, et ils avaient imité les signatures de M. et Mme Dupont sur les documents hypothécaires. D'ici à ce que la fraude eût été constatée, les bandits étaient déjà bien loin.

*Les noms sont fictifs.

déchets à la recherche de relevés de compte bancaire ou de carte de crédit. Ils communiquent ensuite avec la banque émettrice, demandent un changement d'adresse puis commencent à dépenser aux frais de leurs victimes. Très souvent, la victime n'a nullement connaissance des sommes qui s'accumulent dans son compte, puisque les factures sont envoyées à une autre adresse.

Piquage de mots de passe. Cette escroquerie est simple, mais très efficace. Le voleur regarde par-dessus votre épaule lorsque vous entrez votre numéro d'identification personnel (NIP) à un guichet automatique bancaire (GAB) ou lorsque vous utilisez votre carte de débit pour régler un achat, puis il utilise ce numéro pour retirer des fonds de votre compte bancaire.

Mystification par courriel et site Web. Dans le cadre de cette fraude électronique, la victime ciblée reçoit un courriel semblant provenir d'une entreprise légitime et l'invitant à se rendre sur un site Web où des renseignements personnels sont demandés. En fait, une telle entreprise n'existe pas et le site Web en question n'a pour but que d'obtenir le NAS et les renseignements financiers personnels de la victime.

Comment pouvez-vous vous mettre à l'abri?

En moyenne, la victime d'une usurpation d'identité doit consacrer plus de 600 heures et dépenser plus de 1 500 \$ au rétablissement de la situation. Comme pour de nombreux crimes, la prévention représente la protection la plus efficace (et la moins coûteuse).

Protégez vos renseignements personnels. Assurez la sécurité de vos renseignements personnels, surtout votre NAS, mais aussi votre date de naissance et les numéros de vos cartes de crédit et de vos comptes bancaires. Votre employeur, l'Agence du revenu du Canada et vos institutions financières sont légalement autorisés à obtenir votre NAS, mais ils sont à peu près les seuls. Ne donnez aucun renseignement personnel à des tiers à moins d'être parfaitement convaincu de faire affaire avec une entreprise fiable et ne donnez jamais de renseignements personnels par l'intermédiaire d'un téléphone sans fil, d'un cellulaire ou d'un ordinateur portable, en raison des risques d'interception.

Protégez vos mots de passe. Utilisez des mots de passe différents pour votre carte de crédit, vos comptes bancaires et de téléphone. Choisissez des mots de passe difficiles à deviner (ne prenez pas votre date d'anniversaire, par exemple) et modifiez-les régulièrement, tous les mois si possible. Ne les

mettez pas par écrit et ne les divulguez à personne. Lorsque vous faites un achat par carte de débit ou un retrait à un GAB, vérifiez bien autour de vous pour vous assurer que personne ne cherche à connaître votre NIP.

Utilisez votre carte de crédit intelligemment. Ne gardez sur vous que les renseignements personnels et les cartes de crédit dont vous avez besoin. Faites annuler les cartes de crédit que vous n'utilisez pas et gardez une liste distincte de celles dont vous vous servez régulièrement.

Assurez la sécurité de votre courrier. Déposez toujours votre courrier sortant directement dans une boîte aux lettres afin que personne ne puisse l'intercepter. Déchiquez ou détruisez toute demande de carte de crédit préapprouvée dont vous ne voulez pas, de même que tout reçu de carte de crédit, facture de services publics ou autre document contenant des renseignements personnels ou sur vos comptes. Une déchiqueuse coûte moins de 40 \$ et vous protège contre les «pêcheurs de poubelles».

Assurez la sécurité de votre ordinateur et de votre accès Internet. Vous pourriez doter votre ordinateur d'un «coupe-feu» pour empêcher les intrus d'avoir accès aux données qu'il contient. Ne traitez qu'avec des entreprises fiables et bien établies lorsque vous faites des achats avec votre carte de crédit ou des opérations bancaires sur Internet et assurez-vous

Étude de cas n° 2 – Le «dispositif servant à l'écrouissage» du Sud

Alors qu'il était en vacances en Floride, Fernand Dubé* a utilisé sa carte de crédit pour régler une addition au restaurant. La serveuse a pris la carte et s'est éloignée de la table en vue d'obtenir une autorisation. Sans que M. Dubé en ait la moindre idée, elle a aussi passé la carte dans un «dispositif servant à l'écrouissage» avant de la lui remettre. Elle est ensuite partie à l'assaut des magasins. M. Dubé ne s'est pas rendu compte que sa carte avait été utilisée frauduleusement avant son retour au Canada ni avant la réception de son relevé de carte de crédit.

*Les noms sont fictifs.

que leurs sites sont sécuritaires. Recherchez des signatures numériques, le chiffrement des données et d'autres outils technologiques contribuant à améliorer la sécurité des utilisateurs.

Revoyez vos dossiers régulièrement. Vérifiez vos relevés de comptes bancaires et de cartes de crédit dès leur arrivée pour découvrir et signaler toute irrégularité sans délai. Portez attention aux cycles de facturation – si vos factures n'arrivent pas à temps, il se peut que votre courrier soit détourné vers une autre adresse.

Vérifiez votre cote de crédit. Vous pouvez obtenir une copie de votre rapport de crédit pour vous assurer qu'il est exact. On compte deux agences nationales d'évaluation du crédit au Canada, soit Equifax Canada (1 800 465-7166, www.equifax.ca) et TransUnion Canada (1 877 525-3823, www.tuc.ca).

Que devez-vous faire si cela vous arrive?

Si vous pensez avoir été victime d'une usurpation d'identité, veuillez alerter la police, votre banque et vos créanciers sans tarder. Demandez à la police de vous remettre une copie de son rapport, car vos créanciers pourraient l'exiger comme preuve qu'une fraude a été commise. Prenez ensuite les mesures suivantes pour protéger votre réputation :

- Gardez un dossier de tous vos interlocuteurs et de toutes les dépenses que vous engagez pour blanchir votre nom et rétablir votre solvabilité.
- Annulez vos cartes de crédit et fermez vos comptes bancaires, puis remplacez-les par de nouveaux. Utilisez de nouveaux mots de passe et NIP pour chacun d'eux.
- Procurez-vous un nouveau permis de conduire.

- Communiquez avec Equifax et TransUnion et demandez-leur de placer un message d'alerte à la fraude dans votre dossier. Les fournisseurs de crédit sauront ainsi que vous pouvez faire l'objet de fraudes. Ces deux agences d'évaluation du crédit comptent des spécialistes chargés d'aider les victimes de fraudes qui vérifieront avec vous votre rapport de crédit par téléphone; vous aurez ainsi une liste complète de tous vos créanciers.
- Faites des vérifications auprès des agences d'évaluation du crédit après trois mois et demandez une copie à jour de votre rapport de crédit pour vous assurer que votre identité n'a pas été de nouveau usurpée.
- Communiquez avec Postes Canada si vous pensez que l'usurpateur a déposé un formulaire de changement d'adresse à votre nom en vue de faire acheminer votre courrier à une autre adresse.
- Avisez les sociétés de téléphone, de câblodistribution et d'autres services publics qu'un usurpateur utilise votre nom frauduleusement et qu'il pourrait tenter d'ouvrir de nouveaux comptes.
- Si vous pensez qu'un fraudeur a utilisé votre numéro d'assurance sociale pour obtenir un emploi, communiquez avec Ressources humaines et Développement des compétences Canada.

Cet article vise à donner strictement des renseignements généraux et il ne doit pas être considéré comme donnant des conseils précis convenant aux particuliers. Étant donné qu'il est essentiel de tenir compte des circonstances personnelles et de l'actualité, tout particulier souhaitant donner suite aux renseignements figurant dans cet article doit consulter un expert.

^{MC} Marque de commerce de la Banque CIBC.

Gestion privée de patrimoine CIBC représente des services offerts par la Banque CIBC et ses filiales.

Le logo CIBC est une marque déposée de la Banque CIBC.