CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 017 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 3 avril 2014

Président

M. Pat Martin

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le jeudi 3 avril 2014

● (1100)

[*Traduction*]

La vice-présidente (Mme Patricia Davidson (Sarnia—Lambton, PCC)): Bonjour à tous. La séance est ouverte.

Je souhaite la bienvenue à nos témoins d'aujourd'hui.

Nous recevons les représentants de la Gendarmerie royale du Canada: le directeur des Centres de coordination de la police fédérale, le surintendant Jean Cormier, et l'inspecteur Cameron Miller des Centres de coordination de la police fédérale, domestique.

Nous recevons également les représentants du ministère de l'Industrie: le directeur des dossiers spéciaux et conseiller stratégique du Bureau de la concurrence de la Direction générale des pratiques loyales des affaires, M. Thomas Steen, et le sous-commissaire adjoint intérimaire de la concurrence du Bureau de la concurrence de la Direction générale des pratiques loyales des affaires Division C, M. Morgan Currie.

Sans plus tarder, je vais céder la parole à nos témoins, qui feront leur déclaration préliminaire. Nous commencerons par les représentants de la Gendarmerie royale du Canada.

Monsieur Cormier, vous avez la parole.

Surint. Jean Cormier (directeur, Centres de coordination de la police fédérale, Gendarmerie royale du Canada): Madame la présidente, honorables membres du comité, bonjour et merci d'inviter la GRC à prendre la parole devant vous aujourd'hui.

J'ai à mes côtés l'inspecteur Cameron Miller qui, à la direction générale de la GRC, est l'officier responsable de superviser les activités et l'administration du Centre antifraude du Canada, le CAFC.

[*Français*]

Le CAFC est un partenariat entre la police provinciale de l'Ontario, le Bureau de la concurrence et la GRC. Il joue un rôle essentiel dans l'éducation du public en matière de fraude par marketing de masse.

[*Traduction*]

Je suis heureux d'être accompagné par l'un de ces partenaires, soit le Bureau de la concurrence, représenté par M. Morgan Currie, sous-commissaire adjoint de la Direction générale des pratiques loyales des affaires et M. Thomas Steen, directeur des dossiers spéciaux et conseiller stratégique, également au sein de la Direction générale des pratiques loyales des affaires.

[*Français*]

Je suis également heureux d'être ici aujourd'hui avec mes collègues pour vous dire quelques mots sur la GRC, sur son rôle au sein du CAFC et sur son rôle en ce qui a trait à la lutte contre le vol d'identité aux côtés de ses partenaires.

Le vol d'identité est un problème sérieux qui peut avoir de graves conséquences.

[*Traduction*]

Les groupes criminels exploitent les progrès technologiques pour détourner des renseignements personnels à des fins illicites. Bien que le vol d'identité ne soit pas nouveau, il a pris une ampleur considérable. Des groupes spécialisés peuvent percer des réseaux complets, infecter de nombreux ordinateurs personnels ou concevoir des sites Web frauduleux pour forer des données personnelles sur une vaste échelle.

Des millions de dossiers personnels peuvent être obtenus par une seule cyberattaque ciblée. Le vol d'identité a évolué: on ne se fait plus seulement passer pour une autre personne, on se crée dorénavant une identité de synthèse. Les criminels utilisent les renseignements personnels volés à diverses personnes pour se procurer des pièces d'identité légitimes sous un nom inventé — c'est ce qu'on appelle une identité de synthèse. On peut utiliser une identité de synthèse à plusieurs fins illicites: fraude, espionnage industriel, blanchiment d'argent et financement terroriste.

● (1105)

[*Français*]

Au cours des 10 dernières années, la hausse sans précédent de la criminalité associée aux renseignements personnels a fait du vol d'identité une préoccupation réelle pour toute la population canadienne.

[*Traduction*]

Les crimes contre l'identité n'ont pas sur les victimes les mêmes conséquences que d'autres crimes. L'identité est au coeur de pratiquement tous les aspects de la vie moderne. Une fois son identité compromise, la victime peut en subir des conséquences pendant longtemps. Outre les pertes financières, il faut penser aussi à l'atteinte à sa réputation de même qu'à la perte d'accès au crédit et à d'autres services. Certaines victimes doivent même répondre d'actes criminels qui ont été commis par d'autres en utilisant leur nom.

Il y a lieu de s'inquiéter aussi de l'activité accrue des groupes du crime organisé dans les crimes contre l'identité. Ces groupes fonctionnent au-delà des frontières nationales et internationales afin d'échapper à la détection de la police et aux poursuites judiciaires.

Par conséquent, les crimes contre l'identité se commettent simultanément dans plusieurs territoires de compétence, et traversent les frontières municipales et provinciales. La mondialisation et l'absence de cyberfrontières font en sorte que de nombreux cas ont des liens et des répercussions à l'échelle internationale, ce qui rend la situation encore plus complexe.

[*Français*]

En 2010, le gouvernement du Canada a reconnu la gravité croissante des crimes contre l'identité et a modifié le Code criminel par l'adjonction d'infractions liées au crime contre l'identité. En 2012, la GRC, de concert avec des intervenants des secteurs public et privé, a élaboré sa Stratégie nationale de lutte contre les crimes liés à l'identité.

[*Traduction*]

Si vous le voulez bien, mettons le problème en contexte.

En 2013, la GRC a ouvert 3 411 dossiers sur le vol d'identité ou la fraude. Pour cette même année, Norton, une sous-opération de Symantec, un fournisseur de solutions de sécurité, d'entreposage et de gestion de système, estime qu'il y a eu pour 113 milliards de dollars de pertes attribuables à la cybercriminalité à l'échelle mondiale, la part du Canada s'élevant à environ 3 milliards de dollars. Plus de 24 000 victimes de crimes contre l'identité ont communiqué avec le CAFC et fait état de pertes de 11 millions de dollars.

En 2012, Symantec a fait valoir qu'en moyenne, les atteintes à des données protégées entraînaient le vol de 604 826 identités et que ce sont plus de 93 millions d'identités qui ont ainsi été exposées. Une attaque ciblée contre la société Target a compromis les cartes de paiement de 100 millions de ses clients.

Ces données illustrent l'importance pour la police de travailler de près avec ses partenaires au pays et à l'étranger afin de prévenir et de détecter le crime, et de poursuivre ceux qui se livrent à de telles activités.

[*Français*]

Nous croyons que le partage d'informations entre les différents partenaires canadiens, les ministères du gouvernement du Canada et la GRC est vital afin de prévenir le vol d'identité et de s'attaquer au problème.

[*Traduction*]

Nous devons nous employer à éduquer, à prévenir, à détecter et à dissuader autant qu'à enquêter et à poursuivre ceux qui participent à de telles activités criminelles.

[*Français*]

Le vol d'identité a des répercussions réelles sur les particuliers, les entreprises et les collectivités, ainsi que sur la réputation du Canada à l'étranger.

● (1110)

[*Traduction*]

Chacun a la responsabilité d'apprendre à protéger son identité.

[*Français*]

Bien que de nombreux Canadiens soient maintenant sensibilisés aux différentes méthodes qu'utilisent les criminels pour voler des renseignements personnels, ils doivent maintenir une vigilance de tous les instants.

[*Traduction*]

La GRC s'engage à protéger le bien-être financier des Canadiens en continuant à contribuer aux efforts de détection et de dissuasion en matière de vol d'identité et d'utilisation de l'identité des victimes pour commettre des fraudes.

[*Français*]

Je vous remercie de l'intérêt que vous portez à ce sujet.

Nous sommes maintenant prêts à répondre à vos questions.

[*Traduction*]

La vice-présidente (Mme Patricia Davidson): Merci beaucoup, inspecteur Cormier, de votre déclaration.

Je cède maintenant la parole à M. Currie. Allez-y, monsieur.

M. Morgan Currie (sous-commissaire adjoint intérimaire de la concurrence, Bureau de la concurrence, direction générale des pratiques loyales des affaires Division C , ministère de l'Industrie): Merci, madame la présidente, de nous avoir invités aujourd'hui à vous parler du vol d'identité.

Je m'appelle Morgan Currie et je suis sous-commissaire adjoint à la Direction générale des pratiques loyales des affaires, qui est une direction générale chargée de l'application de la loi au sein du Bureau de la concurrence, lequel fait partie d'Industrie Canada.

Je suis accompagné de mon collègue, M. Thomas Steen, directeur des dossiers spéciaux et conseiller stratégique à la Direction générale des pratiques loyales des affaires. M. Steen a établi le régime d'application de la loi du bureau et est responsable de sa surveillance; ce régime vise à lutter contre la fraude par marketing de masse, qui est liée au vol d'identité, sujet qui fait l'objet de notre intervention devant vous aujourd'hui. Nous sommes également très contents d'être ici aujourd'hui aux côtés de notre partenaire, la Gendarmerie royale du Canada, qui est représentée par le surintendant Cormier et l'inspecteur Miller.

Je vais commencer par décrire le mandat et le rôle du Bureau de la concurrence. Ensuite, je parlerai de notre travail d'application de la loi dans le but de lutter contre la fraude par marketing de masse. Pour finir, je traiterai des partenariats auxquels participe le bureau, qui contribuent à renforcer les initiatives d'application de la loi dans ce domaine.

[*Français*]

Le Bureau de la concurrence, en tant qu'organisme indépendant d'application de la loi, veille à ce que les entreprises et les consommateurs canadiens prospèrent dans un marché concurrentiel et innovateur. Dirigé par le commissaire de la concurrence, le bureau est responsable de l'administration et de l'application de la Loi sur la concurrence, de la Loi sur l'emballage et l'étiquetage des produits de consommation, sauf en ce qui concerne les denrées alimentaires, de la Loi sur l'étiquetage des textiles et de la Loi sur le poinçonnage des métaux précieux.

Le fait que la concurrence soit profitable tant pour les entreprises que pour les consommateurs est la principale hypothèse opérationnelle sur laquelle se fonde le Bureau de la concurrence.

[*Traduction*]

II incombera aussi au bureau d'appliquer des parties de la loi canadienne anti-pourriel lorsqu'elle entrera en vigueur le 1er juillet 2014, de concert avec le Conseil de la radiodiffusion et des télécommunications canadiennes et le Commissariat à la protection de la vie privée. Grâce à cette loi, le Bureau de la concurrence sera en mesure de s'attaquer plus efficacement aux indications fausses ou trompeuses ainsi qu'aux pratiques commerciales trompeuses dans le marché électronique, notamment les renseignements faux ou trompeurs sur l'expéditeur ou dans l'objet d'un message, les messages électroniques faux ou trompeurs, ainsi que les renseignements faux ou trompeurs sur l'emplacement comme les URL et les métadonnées.

Le bureau fait la promotion de l'éthique publicitaire dans les marchés en décourageant les pratiques commerciales trompeuses et en préconisant la communication de renseignements suffisants qui permettent aux consommateurs de faire des choix éclairés. Les indications fausses ou trompeuses et les pratiques commerciales trompeuses peuvent avoir de graves conséquences sur le plan économique, en particulier lorsqu'elles visent un large public ou si elles se déroulent sur de longues périodes. Elles peuvent nuire tant aux consommateurs qu'aux entreprises concurrentes qui font une publicité honnête.

La Loi sur la concurrence contient des dispositions criminelles et civiles pour remédier aux indications fausses ou trompeuses ainsi qu'aux pratiques commerciales trompeuses lorsqu'il s'agit de promouvoir la fourniture ou l'utilisation d'un produit ou des intérêts commerciaux. Aux termes des dispositions criminelles, la disposition générale interdit les indications qui sont fausses ou trompeuses sur un point important et qui sont données sciemment ou sans se soucier des conséquences. D'autres dispositions interdisent spécifiquement le télémarketing trompeur, la documentation trompeuse, le double étiquetage et le système de vente pyramidale.

Le vol d'identité, tel que le décrit la GRC, fait référence à l'étape préparatoire de l'acquisition et de la collecte des renseignements personnels d'une personne à des fins criminelles. Le Code criminel prévoit plusieurs infractions qui visent les comportements frauduleux. Le mandat du Bureau de la concurrence dans le contexte de la fraude par marketing de masse concerne les comportements qui ont une incidence sur la concurrence et les renseignements relatifs aux produits qui permettent aux consommateurs de prendre des décisions d'achat éclairées. Les infractions comme le vol d'identité et les cas de fraude où la promotion d'aucun produit ou intérêt commercial n'est faite ne relèvent pas du mandat du bureau.

La fraude par marketing de masse se commet par l'entremise des moyens de communication de masse, soit l'Internet, la poste ou le téléphone. Cette fraude coûte à l'économie 10 milliards de dollars par année, et c'est une menace criminelle qui prend de plus en plus d'ampleur à l'échelle mondiale.

● (1115)

Ce type de fraude a des répercussions négatives considérables sur l'économie et les marchés, car elle mine la confiance des consommateurs envers les entreprises légitimes. Le Canada et de nombreux pays partout au monde sont victimes d'activités criminelles à grande échelle de fraude par marketing de masse.

Les auteurs des activités de fraude par marketing de masse ont une grande faculté d'adaptation et changent rapidement leurs méthodes et techniques pour réduire les risques de détection et d'enquête par les autorités chargées de l'application de la loi, et pour contrer la sensibilisation des consommateurs et des entreprises à leurs méthodes du jour.

Le vol d'identité et le blanchiment d'argent demeurent des volets essentiels des diverses manoeuvres de fraude par marketing de masse. Les organismes d'application de la loi constatent une exploitation croissante des victimes de fraude pour recevoir et blanchir des fonds ainsi que pour recevoir et débourser des instruments financiers contrefaits. Même si la majorité des manoeuvres de fraude par marketing sont par nature non violentes, les renseignements des organismes d'application de la loi témoignent que certains groupes auteurs de fraudes se servent de menaces et de techniques coercitives contre les victimes récalcitrantes, les groupes rivaux et même les membres de leur propre groupe.

Le bureau fait souvent enquête sur les fraudes par marketing de masse, qui ont entraîné pour les consommateurs des pertes pouvant aller jusqu'à 500 millions de dollars. Voici certains types de fraudes par marketing de masse sur lesquels enquête le bureau: les fraudes ciblant les petites et moyennes entreprises et leurs annuaires, et les fraudes concernant les fournitures de bureau; les fraudes liées à l'économie numérique où l'information importante est cachée dans les modalités; les fraudes ayant trait aux possibilités d'emploi; et les fraudes liées à la santé.

Pour combattre efficacement la fraude par marketing de masse, les autorités chargées d'enquête, d'application de la loi et de réglementation de nombreux pays travaillent de manière concertée pour recueillir et échanger l'information sur les manoeuvres de fraude par marketing de masse et la façon d'y contrevenir; mènent de plus en plus des programmes de sensibilisation et d'éducation pour aider les particuliers et les entreprises à reconnaître les manoeuvres de fraude par marketing de masse et éviter ainsi les pertes; élaborent des mesures pour identifier plus rapidement les manoeuvres de fraude par marketing de masse et aider les victimes; et déploient des efforts coordonnés avec les organismes d'application de la loi, et renforcent ces efforts, pour lutter contre les manoeuvres de fraude par marketing de masse.

À titre d'exemple de notre collaboration, soulignons que le bureau est membre du Groupe de travail international sur la fraude par marketing de masse, ainsi que du Réseau international de contrôle et de protection des consommateurs.

Le bureau joue également un rôle essentiel dans les sept partenariats Canada-États-Unis pour l'application de la loi en matière de fraude par marketing de masse dans l'ensemble du pays, dont le bureau est un membre fondateur. Établis dans les années 1990 pour combattre le télémarketing trompeur, ces partenariats regroupent maintenant des organismes d'application de la loi du Canada et des États-Unis, qui travaillent ensemble à l'application des lois visant la fraude par marketing de masse. Cette collaboration a donné lieu à des centaines d'enquêtes, de poursuites et d'accusations.

Le Centre antifraude du Canada, qui est géré conjointement par le bureau avec la GRC et la Police provinciale de l'Ontario, est au cœur du réseau national des partenariats en matière de fraude par marketing de masse. Le Centre fournit des renseignements et des informations sur les plaignants aux partenaires d'application de la loi en ce qui concerne une vaste gamme de crimes liés à la fraude par marketing de masse.

De plus, le CAFC, avec le bureau et ses partenaires dans le domaine de l'application de la loi et au sein du secteur privé, informent les consommateurs sur la façon de reconnaître, de signaler et d'enrayer diverses formes de fraude par marketing de masse. En fait, en mars chaque année, le Mois de la prévention de la fraude est organisé conjointement par les partenaires pour promouvoir la sensibilisation à la fraude.

Pour terminer, madame la présidente, mesdames et messieurs les membres du comité, j'aimerais vous remercier de m'avoir donné l'occasion de vous parler aujourd'hui du travail accompli par le bureau pour combattre la fraude par marketing de masse. Nous sommes conscients qu'il s'agit d'un problème mondial, et qu'à ce titre, il nécessite une approche coordonnée. Le bureau continuera de travailler avec les organismes d'application de la loi du monde entier pour défendre les consommateurs contre cette menace.

Je vous remercie et je serai ravi de répondre à vos questions.

● (1120)

La vice-présidente (Mme Patricia Davidson): Je remercie nos intervenants.

Nous entamons la première série de questions. Vous disposerez de sept minutes pour les questions et les réponses. J'espère ne pas devoir vous interrompre, mais je vous aviserai lorsque votre temps de parole tirera à sa fin, si vous n'avez pas fini de répondre aux questions.

Nous commençons par M. Ravignat, du NPD. Allez-y, monsieur.

[*Français*]

M. Mathieu Ravignat (Pontiac, NPD): Merci, madame la vice-présidente.

Je remercie les témoins de leur présence parmi nous aujourd'hui. C'est gentil d'être ici parmi nous et je leur souhaite une bonne journée.

Je ne sais pas si vous le saviez, mais mon parti, le NPD, a déposé les projets de loi C-475 et C-580, qui visent à renforcer les lois régissant la vie privée des Canadiens. Ces projets de loi représentent une solution à l'important retard juridique qu'accuse le Canada dans l'ère numérique actuelle.

Ma question est d'ordre plus général.

En tant que service de police national, la mission de la GRC est, entre autres, d'assurer le respect de la loi. Croyez-vous que le Canada est bien équipé aujourd'hui pour lutter contre le vol d'identité? Le cadre juridique est-il assez robuste pour vous aider dans votre travail?

[*Traduction*]

Surint. Jean Cormier: Comme je l'ai dit dans ma déclaration préliminaire, le gouvernement du Canada a reconnu le problème croissant du vol d'identité, et certaines lois ont été adoptées pour y remédier. Nous accepterions volontiers de nouveaux outils ou de nouvelles lois pour améliorer les méthodes de lutte contre le vol d'identité utilisées par la police. Je crois que le Canada est doté d'un système efficace, mais, comme je l'ai dit, nous pouvons toujours ajouter des cordes à notre arc.

[*Français*]

M. Mathieu Ravignat: Si on exclut le CAFC, quelles mesures la GRC déploie-t-elle afin de lutter contre le vol d'identité et la fraude?

[*Traduction*]

Surint. Jean Cormier: Madame la présidente, ma réponse risque d'être longue, parce que nous réalisons plusieurs initiatives. Je peux en nommer quelques-unes. Si je prends trop de temps, vous m'en aviserez.

Bien sûr, la GRC s'engage à garantir la sécurité et la protection des Canadiens. Nous avons de nombreuses initiatives en ce sens.

En 2012, la GRC a mis sur pied une stratégie nationale sur le vol d'identité. La stratégie repose sur trois piliers: l'éducation et la prévention; les renseignements et l'application de la loi; et les poursuites. La stratégie vise à cibler les priorités et les risques émergents, et à analyser les tendances; à utiliser les données et les analyses émanant du volet sur les renseignements criminels; à accroître la portée du projet d'enquête fondé sur les renseignements et les efforts d'interruption coordonnés; et à élaborer une approche normalisée relative à la fraude d'identité — et donc aux enquêtes —, ce qui comprend la création et l'adoption d'un protocole d'enquête intergouvernemental; comme je l'ai dit, le crime traverse souvent les frontières.

[*Français*]

M. Mathieu Ravignat: Permettez-moi de vous interrompre. Ce que vous dites est intéressant, mais j'aimerais savoir où vous en êtes par rapport à l'élaboration de ces normes?

[*Traduction*]

Surint. Jean Cormier: La stratégie a été mise en oeuvre l'année dernière, et nous travaillons avec nos partenaires du secteur privé et du secteur public pour mettre en oeuvre ces éléments.

[*Français*]

M. Mathieu Ravignat: Vous pouvez poursuivre si vous voulez ajouter quelque chose à ce sujet.

[*Traduction*]

Surint. Jean Cormier: De plus, nous bâtissons des partenariats solides et nous collaborons avec nos partenaires des secteurs public et privé à l'élaboration et à la mise en oeuvre de la stratégie. Nous dépassons les frontières fédérales et provinciales et nous travaillons avec les services de police provinciaux et municipaux, de même qu'avec d'autres organisations. Nous sensibilisons la communauté judiciaire et les responsables du gouvernement du Canada et des autres pays à l'égard du vol d'identité.

Comme l'a dit mon ami dans son discours préliminaire, l'un des thèmes du Mois de la prévention de la fraude — le mois de mars — était le vol d'identité.

● (1125)

[*Français*]

M. Mathieu Ravignat: Je vous remercie

Pourriez-vous nous remettre des copies de vos notes dans le but d'accélérer le processus?

J'aimerais vous poser une dernière question. Ai-je le temps, madame la présidente?

[*Traduction*]

La vice-présidente (Mme Patricia Davidson): Oui.

[*Français*]

M. Mathieu Ravignat: D'accord.

On a récemment appris que, en 2013, la GRC n'a rapporté au Commissariat à la protection de la vie privée du Canada que seulement 26 % des cas d'atteinte aux données personnelles et que, dans les 10 années précédentes, seulement environ 4 % des cas ont été rapportés.

Il doit bien y avoir une raison à ce sujet. Je me demande pourquoi votre organisation ne rapporte pas systématiquement toutes les atteintes aux données personnelles?

Surint. Jean Cormier: Je ne sais pas si je peux répondre à votre question avec exactitude. Essentiellement, on continue d'identifier les cas de vol d'identité. Le fait est que le nombre de cas diminue, mais les valeurs en cause, elles, augmentent.

M. Mathieu Ravignat: Cela ne répond pas tout à fait à ma question.

Selon le Commissariat à la protection de la vie privée, la GRC ne lui rapporte qu'une partie des cas d'atteinte à la vie privée. Je ne comprends pas pourquoi ce problème existe.

Surint. Jean Cormier: Pour vérifier l'information, il faudrait que je compare mes notes à celles de mes partenaires du Bureau de la concurrence.

[*Traduction*]

Je ne sais pas. Je dis seulement que je devrais peut-être…

La vice-présidente (Mme Patricia Davidson): Je vais vous interrompre. Nous pourrions y revenir dans le cadre d'autres questions. Vous n'avez plus de temps.

M. Mathieu Ravignat: Bien sûr.

C'est bien. Si vous pouvez nous transmettre cette information, nous vous en serions reconnaissants.

La vice-présidente (Mme Patricia Davidson): Si vous avez des renseignements à nous transmettre, faites-le par l'entremise du greffier. Il les fera parvenir à tous les membres du comité.

Nous passons maintenant à M. Hawn. Vous avez sept minutes. Allez-y, monsieur.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Je vous remercie tous de votre présence.

Je suppose que la GRC exerce un certain jugement pour désigner les cas de violation qui doivent être référés, par exemple. Est-ce bien cela?

Surint. Jean Cormier: Ce que vous dites est juste. Nous rapportons les cas pertinents au Bureau de la concurrence.

L'hon. Laurie Hawn: Bien sûr.

Monsieur Currie, vous avez parlé de votre collaboration avec diverses organisations internationales. Je suppose que vous échangez les pratiques exemplaires et autres. Est-ce qu'il y a des pratiques exemplaires que nous n'avons pas encore prises en compte ou mises en oeuvre? Est-ce qu'on devrait s'inspirer des autres?

M. Morgan Currie: Madame la présidente, je suis ravi de vous dire que nous entretenons des relations fréquentes et continues avec ces organisations. Bien sûr, l'un des plus grands enjeux associés à la fraude par marketing de masse, c'est que les criminels s'adaptent aux changements et utilisent les nouvelles technologies, mais nous participons régulièrement aux réunions des organisations d'application de la loi et aux forums internationaux, et nous croyons donc que l'échange des renseignements entre les diverses organisations est adéquat.

L'hon. Laurie Hawn: Vous avez parlé de l'adaptation des criminels au changement; ce sont des gens futés. Est-ce que vous embauchez certains d'entre eux pour tenter de garder une longueur d'avance sur les malfaiteurs? Des personnes qui peuvent nous expliquer comment elles procéderaient pour commettre un crime? Est-ce qu'on engage ce genre de personnes?

M. Morgan Currie: Ce que je peux dire, c'est qu'on doit avoir des méthodes de détection de haut niveau technologique. Je ne crois pas que nous ayons de telles personnes à notre emploi; je pourrais être surpris, mais j'espère que non. Toutefois, nous fouillons les sites de médias sociaux pour obtenir des renseignements ou des outils technologiques. De plus, notre collaboration avec les organismes d'application de la loi et même les organismes de protection des consommateurs nous permet d'obtenir plus de renseignements et de données probantes. Je crois que nous restons au fait des tendances et au-dessus de la mêlée.

● (1130)

L'hon. Laurie Hawn: Surintendant Cormier, vous avez parlé d'éducation. De toute évidence, l'éducation du public est très importante. Qui devrait s'en charger, à part bien sûr tout le monde, de façon générale? Quel est le rôle du gouvernement à cet égard?

Surint. Jean Cormier: En fait, le gouvernement joue un rôle très important. Le Conseil du Trésor mène actuellement une stratégie de lutte contre le vol d'identité et élabore des lignes directrices sur l'assurance identitaire, qui en sont à l'étape de la rédaction.

Comme je l'ai dit dans ma déclaration préliminaire, je crois que nous avons tous la responsabilité de nous informer, mais la prévention par l'entremise de publicités comme le Mois de la prévention de la fraude fait également partie de la solution. Le CAFC offre en quelque sorte un soutien entre pairs. Lorsqu'une personne nous appelle pour déclarer un vol d'identité, notre personnel compatit à sa situation et peut la conseiller sur les façons d'éviter qu'elle ne se reproduise.

Il existe également diverses pratiques axées sur l'éducation et la prévention, mais je crois que le gouvernement du Canada a un rôle important à jouer dans tout cela. L'achèvement de la stratégie serait une mesure importante.

L'hon. Laurie Hawn: Bien sûr, la participation du secteur privé est également importante; il se protège lui aussi. Avez-vous eu de la difficulté à obtenir la participation du secteur privé ou du secteur public?

Surint. Jean Cormier: Il n'est pas difficile d'obtenir leur participation. En gros, les défis auxquels nous sommes confrontés lorsque nous travaillons avec les secteurs privé et public et les organismes d'application de la loi ont trait à la capacité de communiquer les renseignements personnels, qui est restreinte dans certains cas par les lois en matière de protection des renseignements personnels, bien sûr, et par l'obligation au secret professionnel des entreprises.

L'hon. Laurie Hawn: Bien sûr, la Loi sur la protection des renseignements personnels est en place pour une bonne raison, mais elle nous met parfois des bâtons dans les roues. À quel point représente-t-elle un obstacle? Je veux dire, combien faut-il de temps pour contourner légalement la loi afin d'obtenir les renseignements dont vous avez besoin? Je sais que cela dépend de chaque cas.

Surint. Jean Cormier: Il n'y a aucune façon de contourner la Loi sur la protection des renseignements personnels pour obtenir des renseignements…

L'hon. Laurie Hawn: Je veux dire en fonction des paramètres de la Loi sur la protection des renseignements personnels.

Surint. Jean Cormier: Bien entendu, pour obtenir des renseignements de façon légale dans le cadre d'une enquête, il faut suivre le processus normal, soit demander une ordonnance judiciaire. Les secteurs public et privé veulent partager les renseignements qu'ils ont avec les forces de l'ordre, améliorer le renseignement et favoriser la prévention, et bâtir une base de données des victimes et des suspects. C'est sincèrement ce qu'ils souhaitent. Nous sommes à établir des relations avec le CAFC pour améliorer cet aspect.

L'hon. Laurie Hawn: Toujours en ce qui concerne la Loi sur la protection des renseignements personnels, rien dans cette loi n'empêche quelqu'un de vous fournir volontairement des renseignements, n'est-ce pas?

Surint. Jean Cormier: C'est exact.

L'hon. Laurie Hawn: Le projet de loi S-4, entré en vigueur en 2010, a ajouté au Code criminel des infractions liées à certains éléments du vol d'identité qui, à l'époque, n'étaient pas couverts par la loi. Savez-vous si cela a permis d'améliorer la capacité des autorités à poursuivre les individus qui commettent ce genre d'infraction? Évidemment, en raison du volume, les chiffres continueront d'augmenter.

Surint. Jean Cormier: Cela a eu un impact positif. Je vais vous donner quelques chiffres à cet égard. En 2012, 2 813 cas ont été rapportés et des accusations ont été portées dans 1 024 d'entre eux. Je n'ai pas les chiffres de l'année précédente, mais, par expérience, je sais qu'il s'agit d'une augmentation.

● (1135)

La vice-présidente (Mme Patricia Davidson): Merci beaucoup, monsieur Hawn. Votre temps est écoulé.

Monsieur Andrews, vous avez la parole pour sept minutes.

M. Scott Andrews (Avalon, Lib.): Une des choses que nous tentons de faire dans le cadre de cette étude, c'est de mieux comprendre comment le vol d'identité se produit afin de trouver des façons de le prévenir et de mieux éduquer la population.

Monsieur Cormier, dans votre exposé, vous avez dit que 3 411 dossiers liés au vol d'identité avaient été ouverts. Avez-vous une ventilation des types de vols d'identité?

Surint. Jean Cormier: Laissez-moi vérifier. Non, je suis désolé, je n'ai pas cette information avec moi. J'ai les statistiques du Centre antifraude du Canada et de la GRC sur le nombre total de vols d'identité, mais pas la ventilation par type.

M. Scott Andrews: Pourriez-vous nous donner une idée de la façon dont les gens s'y prennent pour voler une identité?

Par exemple, hier, nous avons accueilli des représentants de Passeport Canada. Je vais vous poser une question à ce sujet dans un instant. Ils nous ont dit qu'ils recevaient beaucoup de documents volés, que les gens essayaient de se forger une nouvelle identité grâce à des documents volés. Est-ce une façon habituelle de procéder pour ces fraudeurs?

Surint. Jean Cormier: Certainement. Dans nos exposés, mes collègues et moi avons parlé beaucoup de la cybercriminalité, en raison des progrès technologiques.

Bien entendu, l'hameçonnage — lorsque les gens reçoivent un courriel de quelqu'un qui prétend travailler pour leur institution financière et qui leur demande de fournir des renseignements personnels, des informations bancaires et des renseignements sur leurs cartes de crédit, par exemple — est encore très préoccupant. Cela se produit encore très souvent.

Le vol de courrier est encore une source de préoccupation. Des documents personnels volés dans le courrier peuvent mener à un vol d'identité. D'ailleurs, Postes Canada a participé, en collaboration avec plusieurs autres intervenants, à l'élaboration de la stratégie pour la GRC. Vous avez parlé de Passeport Canada. L'organisme dispose d'un des meilleurs systèmes de prévention de la fraude au monde. Ce serait un bon exemple à suivre pour la mise en oeuvre de systèmes de prévention de la fraude.

M. Scott Andrews: Ils nous ont dit également, hier, qu'en 2013, si je ne m'abuse, 70 individus ont tenté d'obtenir un passeport en utilisant une fausse identité, et que Passeport Canada a transmis cette information à la GRC. Que faites-vous lorsque Passeport Canada, par exemple, vous informe qu'un individu a tenté d'obtenir un passeport à l'aide d'une fausse identité?

Surint. Jean Cormier: C'est considéré comme un cas de fraude et il y a enquête. Bien entendu, on tente de définir l'intention, la raison derrière ce geste. Il pourrait s'agir d'un immigrant illégal au pays ou d'un individu voulant participer à des activités criminelles. Il faut examiner toutes les possibilités. Tout commence par une plainte. On obtient d'abord la déclaration des témoins, puis on suit les indices pour trouver le suspect.

Parfois, lorsqu'on nous transmet ces informations, il est difficile d'identifier le suspect, car les responsables de Passeport Canada n'ont que de faux documents à nous donner. Ils ne connaissent pas l'identité du suspect. Mais, lorsqu'on peut retrouver le suspect, on mène une enquête pour fraude.

M. Scott Andrews: Comment dites-vous à une victime qu'un individu a tenté d'utiliser son identité? Y a-t-il un processus en place pour informer la victime que ses renseignements personnels sont compromis? Y a-t-il un modèle pour cela? Est-ce une priorité d'informer les victimes?

Surint. Jean Cormier: Si l'identité d'une personne a été utilisée frauduleusement, cela fait partie du processus d'enquête. On informe les personnes concernées qu'elles ont été victimes de fraude et que quelqu'un a tenté d'utiliser leur identité.

On les informe aussi sur les conséquences possibles qu'un tel geste peut avoir pour eux, car, si un individu a tenté d'utiliser leur identité, cela signifie que leur identité a peut-être déjà été utilisée à leur insu ou à l'insu des forces de l'ordre. Il est nécessaire de communiquer avec les victimes. Cela fait partie du processus normal d'enquête. Aussi, en plus d'être une victime, ces personnes sont également des témoins. Elles peuvent confirmer qu'elles n'ont pas tenté d'obtenir un passeport ou un prêt bancaire ou autre, selon le cas.

● (1140)

M. Scott Andrews: Lorsqu'une personne est victime d'un vol d'identité, quelle mesure doit-elle prendre pour récupérer son identité si la fraude est assez importante? Y a-t-il beaucoup de victimes qui, après un an, subissent encore les conséquences d'une telle fraude?

Surint. Jean Cormier: Certainement. Comme je l'ai dit dans mon exposé, ces activités peuvent avoir des conséquences à long terme pour les victimes. Il est difficile de rebâtir son crédit et de faire corriger ses antécédents en matière de crédit lorsqu'on est victime de fraude ou de vol d'identité. C'est un processus complexe et difficile. J'ai entendu dire que, dans certains cas, les victimes ont dû attendre plusieurs mois avant que leur dossier soit réglé.

M. Scott Andrews: Est-ce que le problème se situe principalement au niveau du rétablissement des antécédents de crédit? Est-ce habituellement là qu'il y a problème?

Surint. Jean Cormier: Je crois que c'est un des dossiers les plus complexes et problématiques pour les victimes à régler. Le type de fraude commise avec l'identité volée peut également compliquer la situation.

M. Scott Andrews: Je crois que nous sommes censés accueillir des agences d'évaluation du crédit. Que pourrait-on leur demander pour aider les victimes à corriger leurs antécédents de crédit plus rapidement? Comment devrait-on procéder à ce chapitre?

Surint. Jean Cormier: J'ignore quel est le processus exact. Je suis convaincu que ces agences doivent faire preuve de toute la diligence requise, car n'importe qui ayant un mauvais crédit pourrait communiquer avec elles, dire qu'elles ont été victimes de fraude et qu'elles ne sont pas responsables de leurs mauvais antécédents de crédit.

Je suis convaincu que le processus est assez rigoureux. Parfois, l'attente peut être une source de frustration pour les victimes, mais c'est nécessaire. Il serait difficile pour moi de dire à une autre agence comment procéder.

La vice-présidente (Mme Patricia Davidson): Merci beaucoup, monsieur Andrews.

Monsieur Zimmer, vous avez la parole pour sept minutes.

M. Bob Zimmer (Prince George—Peace River, PCC): Merci d'avoir accepté notre invitation.

J'aurais quelques questions à poser. Je vais d'abord m'adresser à la représentante du Bureau de la concurrence. En quelques mots, quel est le mandat officiel de votre organisation?

M. Morgan Currie: Notre mandat consiste à veiller à ce que les entreprises et les consommateurs canadiens prospèrent dans un marché concurrentiel et innovateur. Nous nous concentrons beaucoup sur la concurrence pour les Canadiens et la santé économique. De façon générale, nous avons des règles pour mener des enquêtes sur des activités criminelles, comme la fixation des prix. Nous analysons les fusions proposées pour voir si elles risquent de limiter la concurrence pour les Canadiens relativement aux produits et services concernés. Nous avons une direction qui se penche particulièrement sur l'abus de position dominante, soit lorsqu'une entreprise dominante se livre à des agissements qui réduisent la concurrence.

Notre direction, la Direction générale des pratiques loyales des affaires, enquête principalement sur les indications fausses ou trompeuses et les pratiques commerciales trompeuses faisant en sorte que les consommateurs obtiennent des informations imprécises au moment d'orienter leurs décisions d'achat.

M. Bob Zimmer: J'ai entendu ce que vous avez dit plutôt, et ça concorde avec ce que vous venez de dire.

Pourriez-vous nous donner un exemple d'une fraude commerciale importante, et peut-être quelques exemples d'autres types de fraude? Pourriez-vous nous donner un exemple d'une fraude survenue au Canada? De quel type de fraude s'agissait-il? Comment le Bureau de la concurrence a-t-il réglé le dossier? Qu'a-t-on fait pour reconnaître les victimes?

M. Thomas Steen (directeur des dossiers spéciaux et conseiller stratégique, Bureau de la concurrence, direction générale des pratiques loyales des affaires , ministère de l'Industrie): Je peux répondre.

Ma collègue, Mme Currie, a parlé de quatre types de fraudes commerciales importantes que traite le bureau.

La première catégorie concerne les arnaques qui ciblent habituellement les petites et moyennes entreprises, qu'elles soient au Canada ou à l'étranger. Si les auteurs du crime sont au Canada, la loi s'applique, que les victimes soient au Canada ou à l'étranger.

La fraude de l'annuaire est un exemple typique de ce genre d'arnaque. Celle-ci est commise soit par télémarketing ou par télécopieur, et comprend toujours un volet Internet. Habituellement, les auteurs de ce crime utilisent ce qu'on appelle la technique de vente présumée. Il s'agit de communiquer avec une société — en fait, il peut s'agir d'une organisation, d'un organisme de bienfaisance, d'une église, d'un organisme gouvernemental ou de quiconque a un bureau — et de lui laisser croire qu'elle fait cette inscription chaque année et qu'on veut simplement renouveler cette inscription et mettre à jour leurs informations. Les arnaqueurs utilisent parfois des noms qui ressemblent aux Pages jaunes, ou à d'autres sociétés semblables. Les gens ne réalisent pas qu'il s'engage à un paiement au téléphone — parfois, les arnaqueurs envoient des formulaires aux sociétés par télécopieur leur demandant de mettre à jour leurs informations, de signer le formulaire et de le leur retourner. Mais, dans les petits caractères, la victime s'engage à débourser 1 500 $ par année pour l'inscription proposée.

Il y a bel et bien un produit; il s'agit habituellement d'une inscription dans un annuaire électronique, mais l'inscription n'apparaît pas. Je vous donne un exemple. Si je suis propriétaire d'une entreprise de remorquage, j'aimerais que les consommateurs puissent faire une recherche Google des entreprises de remorquage à Ottawa et que le nom de ma société apparaisse. C'est probablement ce qui se produit avec les Pages jaunes ou le Canada411, mais pas avec ces sites frauduleux. Il n'y a donc aucune valeur commerciale pour les sociétés ciblées.

Comment fait-on pour enquêter ce genre de fraude? Nous recevons des plaintes par l'entremise du Centre antifraude du Canada et de nos partenaires, puis nous les évaluons. Nous avons des priorités en matière d'application et, à un certain moment, nous décidons de mener une enquête. À ce moment, nous avons plusieurs mécanismes d'enquête à notre disposition, y compris des mandats de perquisition et des articles de loi qui nous permettent d'obliger des individus à nous fournir des renseignements, des déclarations écrites, des dossiers ou des témoignages sous serment. Avant de pouvoir exercer ces pouvoirs, on doit d'abord demander la permission aux tribunaux et démontrer que tout laisse croire que les infractions soupçonnées ont été commises. C'est lorsque nous obtenons l'autorisation d'utiliser ces pouvoirs et que nous analysons les renseignements que nous avons recueillis que notre enquête se met vraiment en branle. Lorsque celle-ci est terminée, nous remettons le dossier au Service des poursuites pénales et recommandons que des accusations soient portées. Il revient ensuite au service de décider de porter ou non des accusations contre les individus ou les sociétés concernés.

● (1145)

M. Bob Zimmer: J'aimerais poursuivre sur ce point. Combien de ces groupes font l'objet d'une poursuite judiciaire et quelle réparation les victimes obtiennent-elles? Des victimes ont-elles déjà été dédommagées? Qu'obtiennent habituellement ces victimes?

M. Thomas Steen: Pour répondre à votre première question, des poursuites ont lieu dans bon nombre des cas que nous renvoyons au Service des poursuites pénales. Nous entretenons une très bonne relation avec ce service. Nous collaborons tout au long du processus, ce qui explique qu'il y a très rarement des surprises dans notre technique d'enquête ou concernant les informations que nous recueillons. C'est la raison pour laquelle des poursuites ont lieu dans plus de 90 % et même 95 % des dossiers que nous renvoyons aux services.

En ce qui concerne les prochaines étapes, d'abord, il faut préciser qu'en vertu de la Loi sur la concurrence, ce genre d'agissement est criminel. Donc, les accusés sont passibles d'une amende par procédure sommaire pouvant atteindre 200 000 $. La plupart du temps, dans nos dossiers, des accusations sont portées et les accusés se voient imposer, à la discrétion de la cour, des amendes très élevées et une peine d'emprisonnement pouvant atteindre 14 ans.

Les victimes peuvent également obtenir réparation.

M. Bob Zimmer: Ce qui peut survenir et la réalité sont deux choses différentes.

Qu'arrive-t-il habituellement aux victimes en fin de compte? Sont-elles dédommagées, oui ou non? C'est une tache importante à leur dossier, alors, que se passe-t-il habituellement? C'est ce que je vous demande.

M. Thomas Steen: Plusieurs choses se produisent.

Souvent, les fraudeurs sont reconnus coupables et se font imposer une amende considérable de quelques centaines de milliers de dollars, sinon de quelques millions de dollars, ainsi qu'une peine d'emprisonnement. Jusqu'à maintenant, la peine la plus sévère a été de trois ans et demi, mais ce n'est qu'en 2009 que la peine maximale pour ce crime est passée à 14 ans. Donc, nous nous attendons à des peines d'emprisonnement plus sévères à l'avenir.

En ce qui concerne la réparation, le Code criminel laisse cette décision à la discrétion des juges. Parfois, nous portons aussi des accusations liées aux produits de la criminalité ou en vertu du Code criminel.

La plupart du temps, cela dépend du genre de preuve que nous avons recueillie dans le cadre de nos enquêtes. Comme on l'a déjà souligné, les criminels sont intelligents et, bien souvent, ils déplacent et cachent leur argent. Lorsque nous réussissons à le trouver, nous faisons ce que nous pouvons. Notre efficacité à trouver ces biens s'améliore.

● (1150)

La vice-présidente (Mme Patricia Davidson): Je vais devoir vous interrompre, car le temps est écoulé.

Merci, monsieur Zimmer.

Ceci met fin à notre première série de questions. Nous allons maintenant amorcer la deuxième série. Chaque intervenant disposera de cinq minutes. Monsieur Angus, vous avez la parole.

M. Charlie Angus (Timmins—Baie James, NPD): Un soir, je me suis rendu à un guichet automatique à Ottawa pour y faire un retrait. Le lendemain, ma caisse populaire dans le nord de l'Ontario a communiqué avec ma conjointe pour lui dire qu'il y avait eu une fraude. Ils avaient découvert que ma carte avait été compromise et, le lendemain, mes mots de passe ont été changés.

C'était extraordinaire, mais ça ne se déroule pas toujours ainsi. J'ai réalisé qu'il aurait pu s'écouler un mois avant que je m'en aperçoive. Les fraudeurs auraient pu vider mon compte en banque, car je suis sur la route et je ne prête pas attention.

Monsieur Cormier, à quel point est-ce important pour les victimes d'un vol d'identité… quand informez-vous les victimes afin qu'elles puissent prendre des mesures préventives? À quel point est-ce important d'agir rapidement?

Surint. Jean Cormier: Bien entendu, c'est très important, mais tout dépend de ce qui a été compromis.

Dans l'exemple que vous venez de donner, vous avez été informé le lendemain. C'est très rapide, ce qui a probablement permis de minimiser… Plus la fraude est identifiée rapidement et plus on réagit rapidement, moins l'impact sur la victime sera sévère. C'est très important.

M. Charlie Angus: Nous avons parlé plusieurs fois à la commissaire à la vie privée. Elle a exprimé sa frustration à propos de la désuétude des lois canadiennes sur la protection des renseignements personnels, qui permettent encore, par exemple, au secteur privé de déclarer les brèches de sécurité de façon volontaire. Évidemment, les entreprises ne veulent pas ameuter leurs clients quand une telle chose se produit. Il est arrivé que 40 et 50 millions d'adresses et de données aient été subtilisées à des entreprises. Les renseignements d'un demi-million d'étudiants ont été perdus, et il a fallu plus d'un mois avant qu'on réagisse.

Est-ce important, selon vous, que la commissaire à la vie privée soit informée des brèches de sécurité au gouvernement et au secteur privé, afin qu'on s'assure que des mesures soient prises au cas où ces atteintes aient été commises dans un but criminel?

Surint. Jean Cormier: Que la commissaire à la vie privée soit mise au courant des brèches, ou que les services de police et d'autres partenaires en soient informés pour limiter les dommages envers les victimes?

M. Charlie Angus: Le rôle de la commissaire est de décider si la brèche est suffisamment importante pour qu'elle doive être signalée. Inutile de faire peur à tout le monde si les données ont été enregistrées dans la mauvaise filière, mais c'est à la commissaire de déterminer s'il y a effectivement eu brèche de sécurité et si des personnes ont été touchées par elle.

Surint. Jean Cormier: Dans ce cas, il serait évidemment très important que la chose soit signalée promptement et que l'information soit analysée le plus rapidement possible. La loi sur la protection des renseignements personnels est bien sûr nécessaire. Je tiens autant que quiconque à mon intimité, mais il faut trouver un équilibre pour aussi être en mesure de protéger les victimes d'actes criminels.

M. Charlie Angus: On assiste maintenant à des tentatives d'espionnage international. En 2011, les ordinateurs du Conseil du Trésor et du ministère des Finances ont été piratés par quelqu'un qui essayait d'aller chercher des mots de passe et des données confidentielles. L'intrusion provenait de la Chine. Était-ce une tentative d'espionnage? Le pirate avait-il des intentions criminelles?

Compte tenu de la puissance incroyable que détient le monde de l'espionnage et du piratage, qui utilise des algorithmes pour recueillir toutes sortes de données, qu'il serait tout simplement impossible pour une seule personne de recueillir, est-ce bien réaliste de croire que les services de police ont ce qu'il faut aujourd'hui pour toujours demeurer à l'affût? Combien de formation faut-il suivre? Est-ce suffisant? J'ai l'impression qu'on a affaire à des activités criminelles d'une envergure sans précédent, éclipsant tous les cas de fraude 419, du temps où les escrocs étaient uniquement armés de télécopieurs.

Surint. Jean Cormier: Il est bien sûr très important d'avoir un agent de police bien formé pour faire enquête sur ce type de crimes. Il est aussi très important d'assurer un partenariat adéquat entre le secteur public et le secteur privé pour contribuer aux enquêtes à cet égard. D'autres organisations du gouvernement du Canada sont également responsables du monde virtuel. Il faut absolument avoir la bonne formation. Au Canada, la GRC peut compter sur des agents très compétents dans ce domaine. Nos compétences sont reconnues à l'échelle mondiale et nous n'avons pas à envier nos partenaires de ce côté. Parce que la technologie évolue constamment et rapidement, nous devons toujours parfaire nos connaissances.

● (1155)

M. Charlie Angus: Est-il très important d'assurer des interventions transnationales? Ces groupes montent des entreprises très sophistiquées dans des domaines où il est possible de mener ce genre d'activité en prétendant que c'est tout à fait légal. Sont-ils intouchables du point de vue de la loi canadienne? Devons-nous établir un groupe d'intervention transnational?

La vice-présidente (Mme Patricia Davidson): Votre temps est écoulé, monsieur Angus, mais nous pourrions entendre une réponse brève.

Surint. Jean Cormier: Certainement.

C'est important, mais c'est aussi tout un défi pour les forces de l'ordre, car les lois diffèrent d'un pays à l'autre, et cela nous empêche parfois de prendre les mesures que nous aimerions prendre pour prévenir les cas de fraude.

C'est important, mais aussi un de nos plus grands défis.

La vice-présidente (Mme Patricia Davidson): Merci beaucoup.

Merci, monsieur Angus.

Nous passons à Mme O'Neill Gordon, pour cinq minutes, s'il vous plaît.

Mme Tilly O'Neill Gordon (Miramichi, PCC): Je tiens à remercier les témoins d'être ici aujourd'hui.

Votre témoignage nous sera certainement très utile et nous poussera à réfléchir aux nombreuses erreurs que nous commettons en cours de route. Nous ne prenons pas soin d'effacer nos traces, notamment en ce qui a trait aux guichets automatiques. Nous les utilisons tous. Comment est-ce que cela se produit? Y a-t-il un facteur principal qui fait que quelqu'un peut entrer dans notre compte pour voler notre argent? Quelle est l'erreur la plus courante?

Surint. Jean Cormier: Je vais renvoyer la question à l'inspecteur Miller.

Insp. Cameron Miller (Centres de coordination de la police fédérale, domestique, Gendarmerie royale du Canada): Madame la présidente, la principale méthode employée pour obtenir de l'information des guichets automatique est une technique appelée « écrémage ». Un faux dispositif est inséré dans la fente du guichet automatique, et les gens croyant qu'il s'agit d'une machine tout à fait légitime, entrent leur numéro d'identification personnel. Les données sont traitées normalement, mais elles sont aussi stockées sur le dispositif.

Vous remarquerez que le clavier des guichets bancaires est muni d'un petit écran protecteur pour cacher le NIP entré. Dans le passé, des gens installaient des caméras dans les vestibules où sont placés les guichets automatiques, de façon à pouvoir capter le numéro entré au clavier, tandis que la bande magnétique était copiée par le dispositif d'écrémage.

À la fin de la journée ou le lendemain matin, avant l'ouverture de la banque, les criminels retournaient sur les lieux pour retirer le dispositif et télécharger toutes les images captées sur vidéo. Ils pouvaient alors produire des clones à l'aide des NIÉ et des données qu'ils avaient recueillies à partir des bandes magnétiques. Ils clonaient de nombreuses cartes, à la manière d'une usine, et tentaient par la suite de vider autant de comptes qu'ils le pouvaient.

Mme Tilly O'Neill Gordon: C'est très effrayant, mais également c'est très utile de le savoir.

Monsieur Cormier, vous avez parlé de sensibiliser les gens pour leur faire comprendre qu'il est de la responsabilité de chacun de protéger son identité. Quelles sont les ressources offertes à la population pour en savoir plus sur le vol d'identité? Je crois que j'ai beaucoup à apprendre à ce sujet.

Surint. Jean Cormier: Il existe différents moyens pour aider un consommateur ou un particulier à se protéger contre le vol d'identité. Il y a bien sûr différentes publications offertes sur le sujet. Tous les postes de police affichent sur leur babillard des brochures sur le vol d'identité. De nos jours, Internet est aussi une bonne source d'information.

On dit souvent qu'Internet est un endroit risqué pour les renseignements personnels, mais cela demeure une très bonne source d'information. Par exemple, le Centre antifraude du Canada a un bon site Web qui présente différents moyens pour se protéger contre le vol d'identité et d'autres types de fraude.

Mme Tilly O'Neill Gordon: Nous savons que ce genre de fraude est endémique, et elle l'est de plus en plus. Avez-vous une idée de la raison derrière cette montée?

Surint. Jean Cormier: Je crois que les avancées technologiques y sont pour quelque chose, car elles mettent le monde à la portée de tous. C'est évidemment un crime transnational. Les criminels ne sont pas nécessairement au Canada. Ils peuvent accéder au Canada de partout dans le monde, alors les victimes ne peuvent être que plus nombreuses.

Je n'ai pas de tableau comparatif, mais je suis sûr que si on comparait le nombre d'internautes à la hausse du nombre de victimes, on verrait une corrélation entre les deux.

● (1200)

Mme Tilly O'Neill Gordon: C'était ma prochaine question. Quelle est la proportion de cas de fraude sur papier par rapport aux fraudes commises en ligne?

Surint. Jean Cormier: On m'a posé cette question autrement tout à l'heure, mais comme je le disais, je n'ai pas de pourcentages pour les différents types de vol d'identité.

Mme Tilly O'Neill Gordon: Nous savons que bien des gens s'en font beaucoup avec cela. Est-ce que les victimes de vol d'identité s'aperçoivent qu'elles ont été ciblées, et si oui, comment s'en aperçoivent-elles?

Surint. Jean Cormier: Oui, lorsqu'on nous confie une enquête, nous prenons soin d'informer la victime, mais si la fraude ne nous a pas été signalée, il est possible que la victime ne s'en rende pas compte.

J'ajoute également que seuls 5 % des cas de fraude sont signalés au Centre antifraude du Canada. C'est donc dire que 95 % des victimes ne le signalent pas à la police, ou du moins pas au Centre antifraude du Canada.

C'est pourquoi il est primordial de faire savoir à l'ensemble de la population que le Centre antifraude du Canada est le registre central pour ce genre d'information. Plus on en saura, plus on sera en mesure d'élaborer des stratégies et des outils efficaces pour prévenir ce genre de crimes.

La vice-présidente (Mme Patricia Davidson): Merci beaucoup, madame O'Neill Gordon.

Je n'ai pas d'autres intervenants sur ma liste.

Voulez-vous prendre la parole, monsieur Andrews?

M. Scott Andrews: Oui, j'aurais quelques questions à poser.

Ma question s'adresse à vous deux. Quelles sont les informations dont les criminels ont besoin pour voler l'identité de quelqu'un? Que doivent-ils savoir sur nous? Ont-ils besoin de notre adresse, de notre date de naissance? De quelles informations ont-ils besoin pour forger une nouvelle identité?

Surint. Jean Cormier: Je peux y répondre rapidement, mais je vais laisser l'inspecteur Miller vous donner plus de détails.

En gros, il y a différentes données qui sont absolument essentielles.

Insp. Cameron Miller: Quand on veut se créer une identité, évidemment, plus on a d'information, mieux c'est. On peut commencer avec un document source, comme un passeport ou un certificat de naissance.

Pour créer une identité synthétique, il suffit d'un nom pour commencer. À partir de là, on décide de l'âge à donner à ce faux profil, puis on fabrique un certificat de naissance et on forge d'autres documents. Créée à l'aide de faux documents, l'identité synthétique peut permettre d'obtenir plus de documents encore.

Pour répondre à votre question, les fraudeurs peuvent partir de rien ou s'assurer d'avoir tout sous la main. Plus ils ont de renseignements, mieux c'est et plus c'est facile.

Cependant, avec les méthodes de production actuelles, il suffit d'imaginer un nom, une identité et une tranche d'âge.

M. Scott Andrews: Cela peut être un nom fictif. Il n'est pas nécessaire que ce soit un nom véridique.

Insp. Cameron Miller: Oui, une identité synthétique ne renvoie pas à une vraie personne. On pourrait donc l'appeler John Doe ou Jane Doe, comme vous voulez, et imaginer une identité, une adresse — au 123, rue Untel, dans n'importe quelle ville, n'importe où dans le monde.

M. Scott Andrews: Monsieur Currie, comment est-ce que cela se passe en ligne, avec le marketing de masse, entre autres? Voyez-vous plus d'identités synthétiques ou y a-t-il plus de vols d'identité de vrais consommateurs?

M. Morgan Currie: Les criminels emploient évidemment des moyens de plus en plus sophistiqués, et c'est un gros problème pour nous qu'aussi peu de cas soient déclarés. Nous tentons donc d'appâter les criminels à l'aide de cartes de crédit. Nous créons de fausses identités dans le but de susciter ce genre de comportement. Nous essayons des abonnements pour voir si cela cache des activités frauduleuses.

Tom pourrait m'aider à répondre à la question et aurait sans doute plus de détails à vous donner. Quand vous faites des achats par carte de crédit ou que vous donnez votre numéro de carte de crédit pour profiter d'une période d'essai gratuite, vous vous exposer immédiatement au risque d'être facturé pour des produits dont vous n'avez jamais entendu parler, et il est difficile d'annuler ce genre de service avant qu'on ne vous ait imposé des centaines de dollars en frais. C'est ce que notre loi définit comme une pratique trompeuse grave.

● (1205)

M. Thomas Steen: Nous avons récemment vu plusieurs cas de ce genre. Un produit est offert pour une période d'essai gratuite; il suffit de payer quelques dollars, peut-être 3 ou 4 $, pour couvrir les frais de port et de manutention, et le tout est porté à votre carte de crédit. En tout petits caractères, difficiles à voir et à lire, on indique que le consommateur accepte en fait d'acheter un plan à 80 $ par mois pour ce produit. Pire encore, deux autres produits, qui n'ont absolument rien à voir avec le premier, s'ajoutent à la commande et sont facturés sur la carte de crédit du client avec une description obscure.

Comme M. Currie le disait, il est très difficile de se sortir de ces attrapes, parce que les numéros de téléphone donnés sont ceux de centres d'appel, qui bien souvent laissent sonner sans jamais répondre. On tombe sur des messages en boucle qui nous disent d'appeler à un autre numéro. Bien des fois, le seul recours qui s'offre aux consommateurs est de faire annuler leur carte de crédit, et il ont beaucoup de mal à récupérer leur argent.

M. Scott Andrews: Merci.

La vice-présidente (Mme Patricia Davidson): Merci beaucoup.

J'en profite pour remercier nos témoins d'aujourd'hui.

Nous avons certainement entendu des renseignements très intéressants, parfois inquiétants, mais nous vous sommes reconnaissants d'avoir pris le temps de venir nous parler.

Comme nous n'avons pas d'autres témoins, la séance est levée.