Chambre des communes
CANADA

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

ETHI • NUMÉRO 047 • 1re SESSION • 39e LÉGISLATURE

TÉMOIGNAGES

Le mardi 15 mai 2007

Président

M. Tom Wappel

Aussi disponible sur le site Web du Parlement du Canada à l’adresse suivante :

http://www.parl.gc.ca

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

Le mardi 15 mai 2007

● (0905)

[*Traduction*]

Le président (M. Tom Wappel (Scarborough-Sud-Ouest, Lib.)): Bonjour. Je déclare cette 47e réunion du comité ouverte.

Mesdames et messieurs, je tiens à vous informer que le comité de direction a tenu une réunion hier en fin d'après-midi afin de discuter d'un plan de travail relatif à la motion qui a été adoptée jeudi. Je tiens également à ce que vous sachiez que la première question à aborder jeudi matin sera le rapport du comité de direction, qui vous sera présenté aux fins de délibérations et d'approbation.

Nous essaierons de rassembler des témoins, et avec un peu de chance, ceux-ci pourront témoigner si le rapport du comité de direction est accepté. Bien entendu, dans le cas contraire, je les renverrai. Mais je ne veux tout simplement pas perdre une journée si nous pouvons l'éviter.

Alors voilà comment nous procéderons.

Aujourd'hui, nous continuerons notre étude sur le vol d'identité, avec l'aide de témoins que nous avons déjà entendus sur d'autres questions.

Bienvenue.

Voici M. John Lawford, conseiller juridique de l'Initiative canadienne des consommateurs. Et voici la directrice exécutive de la Clinique d'intérêt public et de politique d'Internet du Canada, Philippa Lawson, accompagnée de M. Mark Hecht.

Je présume qu'il y aura deux déclarations préliminaires, n'est-ce pas? Oui, très bien.

Nous commencerons donc par Mme Lawson puis nous continuerons avec M. Lawford pour finir par la période de questions.

Mme Philippa Lawson (directrice exécutive, Clinique d'intérêt public et de politique d'Internet du Canada): Merci, monsieur le président.

Bonjour mesdames et messieurs.

Je vais parler en anglais ce matin.

Je vous remercie de me donner la chance de parler aujourd'hui d'un problème très grave qui touche directement un nombre croissant de Canadiens et qui par le fait même, nous concerne tous.

Mon nom est Philippa Lawson. Je suis directrice de la CIPPIC, la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa. En décembre dernier, j'ai eu le plaisir de témoigner devant vous sur la LPRPDE, ou Loi sur la protection des renseignements personnels et les documents électroniques.

Je suis aujourd'hui accompagnée de Mark Hecht, professeur en droit et principal chercheur de ce projet sur le vol d'identité de la CIPPIC.

Nous avons remis un mémoire au greffier qui, je crois, sera traduit avant de vous être présenté.

La CIPPIC participe à un projet de recherche pluri-institutionnel sur le vol d'identité financé par l'ORNEC, ou Ontario Research Network for Electronic Commerce, un partenariat public-privé regroupant quatre grandes banques canadiennes et quatre universités ontariennes. Un certain nombre de chercheurs de ces universités étudient les diverses questions entourant la définition et l'évaluation du vol d'identité, les méthodes de gestion et les solutions techniques à ce problème.

À la CIPPIC et à l'Université d'Ottawa, nous examinons les solutions juridiques et politiques au vol d'identité, et nous avons entrepris une vaste analyse comparative des mesures appliquées dans les autres provinces et territoires et là où la loi canadienne est en vigueur.

Nous avons publié une série de documents de travail portant sur divers aspects du vol d'identité, la plupart pouvant être consultés sur notre site Web — www.cippic.ca —, et nous en publierons quelques autres sous peu.

Comme vous le savez, nous avons aussi publié un livre blanc sur la notification des atteintes à la sécurité, et nous avons été très heureux de voir que nos recommandations à ce sujet ont été mentionnées dans votre dernier rapport sur la LPRPDE.

Nous avons également créé une page Web sur le vol d'identité comprenant une foire aux questions et diverses ressources pour le public.

Nous avons l'intention, après avoir effectué des recherches et des analyses plus fouillées au cours de l'été et de l'automne, de publier un livre blanc comportant de nombreuses recommandations sur la réforme des lois et des politiques. Et nous avons l'intention de le terminer d'ici la fin de l'année.

Vous nous avez devancés par ces audiences, et c'est pourquoi nous vous présentons certaines recommandations dès maintenant. Toutefois, nous en formulerons de plus détaillées plus tard, notamment dans le domaine du droit pénal, que, d'après ce que je comprends, vous n'abordez pas dans ces audiences.

Je sais que je dispose d'environ dix minutes. Ai-je moins de temps que cela? D'accord, très bien.

Le président: Il vous reste moins de dix minutes, évidemment.

Mme Philippa Lawson: Le terme « vol d'identité » est quelque peu trompeur, dans la mesure où l'activité dont nous parlons ne couvre pas seulement la collecte non autorisée ou le vol de renseignements mais bien l'utilisation frauduleuse qu'on en fait. Vous vous rendrez compte que de nombreux experts parlent de fraude d'identité lorsqu'ils font référence à l'utilisation non autorisée de ces renseignements. Ce crime comporte en fait deux volets. Il porte à la fois sur la collecte non autorisée de renseignements et sur leur utilisation frauduleuse. Nous utilisons le terme « vol d'identité » de façon générale comme on s'en sert habituellement pour faire référence à ces deux volets.

Les voleurs d'identité ont recours à de nombreuses techniques pour recueillir des renseignements personnels. Il existe des méthodes relativement simples comme fouiller les poubelles, intercepter les courriels, soudoyer des employés et se faire passer pour une personne autorisée à obtenir les informations. Il existe également des techniques autrement plus complexes comme l'écrémage, l'hameçonnage, le détournement de domaine, l'enregistrement des touches du clavier et le piratage des grandes banques de données.

Une seule personne peut faire l'objet de nombreuses fraudes avant de s'en apercevoir. En effet, il arrive souvent que les victimes de vol d'identité l'ignorent jusqu'à ce qu'elles fassent une demande de crédit et se la voient refuser ou commencent à recevoir des appels d'une agence de recouvrement des créances. Entre-temps, leur cote de solvabilité s'en trouve ruinée et elles risquent d'avoir beaucoup de difficulté à la rétablir. Les victimes font face à une myriade de difficultés pour restaurer leur réputation et recouvrer les pertes encourues, souvent sans qu'elles aient fait preuve de négligence.

Je sais que vous vous préoccupez des tendances. Une tendance qui vaut la peine d'être mentionnée est l'utilisation que font les voleurs d'identité d'Internet afin de recueillir et d'échanger les renseignements volés. Il est très facile de trouver des sites Web qui vendent des données de cartes de crédit. Des lecteurs de disque dur contenant des informations personnelles sont vendus sur eBay, par exemple. Internet, comme je suis sûre que vous le savez, est également utilisé pour duper des consommateurs sans méfiance en les amenant à transmettre les renseignements relatifs à leur compte grâce à des techniques comme l'hameçonnage et le détournement de domaine. Je peux vous les expliquer plus tard si vous le désirez.

Malheureusement, il existe peu de données fiables sur le vol d'identité au Canada. PhoneBusters publie des données fondées sur les plaintes qu'il reçoit, mais celles-ci ne représentent qu'une fraction du problème. Certains sondages d'opinion publique fournissent un aperçu du problème, mais encore une fois, ils ne sont pas complets. Nous n'avons que peu d'autres sources sur lesquelles nous appuyer.

Notre première recommandation est de créer une stratégie nationale visant à recueillir des données fiables et autant que possible complètes sur la fréquence et les formes du vol d'identité au Canada ainsi que sur les frais qu'il occasionne.

En ce qui concerne la prévention du vol d'identité, nos recherches laissent voir que les voleurs d'identité profitent autant, si ce n'est plus, de la collecte, de la conservation et de l'échange superflus de renseignements personnels par les organismes que des lacunes dans l'application des lois pénales ou de la crédulité et de l'insouciance des consommateurs. Dans de nombreux cas, les consommateurs n'auraient absolument rien pu faire pour se protéger, si ce n'est d'éviter de faire affaire avec l'organisme qui a laissé échapper les renseignements en premier lieu.

Donc, si nous voulons aborder ce problème avec efficacité, il nous faudra agir dans quatre domaines cruciaux : l'application des lois sur la protection des données, la poursuite en justice des voleurs d'identité, les droits des consommateurs et les recours à leur portée, et la sensibilisation du public.

Nous disposons d'une loi sur la protection des données relativement efficace avec la LPRPDE. Cette loi interdit aux organismes de recueillir plus de renseignements qu'ils n'en ont besoin, de les conserver plus longtemps que nécessaire et de les utiliser ou de les divulguer à des fins autres que celles autorisées par la personne visée. Elle exige aussi que les organismes mettent en place des mesures de sécurité raisonnables afin de se protéger contre les accès non autorisés et les vols d'identité.

Le principal problème avec la LPRPDE n'est pas une quelconque lacune substantielle, comme nombre d'entre vous l'avez mentionné dans votre dernier rapport sur la LPRPDE, mais plutôt le fait que la LPRPDE n'a pas de mécanisme d'application efficace afin d'encourager les organismes à s'y conformer. Par conséquent, de nombreuses organisations recueillent beaucoup plus de données personnelles qu'elles n'en ont besoin et les conservent plus longtemps qu'elles ne le devraient, exposant ainsi les gens à un plus grand risque de vol d'identité. Je pourrais vous en donner plusieurs exemples.

Les organismes n'arrivent également pas à protéger les renseignements personnels qu'ils conservent au moyen d'un cryptage efficace, d'une sélection judicieuse de leurs employés et d'autres mesures. L'étude que nous avons effectuée l'an dernier auprès de 64 marchands en ligne et que nous vous avons présentée en décembre dernier confirme qu'il arrive couramment que même les exigences les plus simples de la Loi ne soient pas respectées.

● (0910)

L'obligation de notification des atteintes à la protection des données offre une certaine promesse de création de mesures incitatives, mais uniquement si cette notification est rendue publique et uniquement si les atteintes ne sont pas si fréquentes et répandues qu'elles amoindrissent l'atteinte portée à la réputation. Même alors, les règles de notification des atteintes doivent être complétées par un régime d'application qui suscite un risque réel de sanction pécuniaire en cas de collecte excessive de données personnelles ou d'autres infractions à la LPRPDE qui contribuent au problème du vol d'identité.

Dans notre présentation au comité en décembre dernier, nous avons formulé un certain nombre de recommandations visant à renforcer le régime d'application de la LPRPDE, notamment autoriser les recours collectifs contre les organismes qui enfreignent la LPRPDE, éliminer les obstacles financiers qui empêchent les victimes d'intenter des poursuites contre des organisations qui contreviennent à la LPRPDE et verser des dommages-intérêts punitifs en guise de recours possible en cas d'infraction à la LPRPDE.

Nous avons été déçus de voir qu'aucune de ces recommandations n'a été adoptée ou même mentionnée par le comité dans son rapport. À notre avis, il est indispensable de s'attaquer au problème des mesures incitatives — la plus importante lacune de la LPRPDE et un facteur décisif du problème croissant du vol d'identité — si nous voulons faire des progrès dans ce domaine.

En ce qui concerne la sensibilisation du public, il existe d'excellents sites Web et dépliants qui expliquent les tendances en matière de vol d'identité et offrent des trucs pour s'en protéger, mais le problème demeure. Les gens continuent d'être victimes de ces stratagèmes d'ingénierie sociale, tels que l'hameçonnage et le détournement de domaine. Des jeunes publient des renseignements détaillés sur eux-mêmes sur Internet, sans comprendre les risques qu'ils courent.

Nous recommandons que l'Agence de la consommation en matière financière du Canada soit mandatée pour entreprendre une campagne nationale de sensibilisation du public sur le vol d'identité, en consultation avec les institutions financières, les organismes d'application de la loi et les organismes de protection des consommateurs. Cette campagne devrait porter principalement sur les manœuvres les plus couramment utilisées par les voleurs d'identité pour obtenir des renseignements directement auprès des personnes, faire appel aux médias de masse et présenter des notices dans les communications du gouvernement, des affiches et des dépliants dans les comptoirs publics.

Sur la question de la protection des consommateurs, il convient d'abord de mentionner que les victimes de vol d'identité n'ont habituellement aucun moyen de savoir qu'un vol s'est produit avant d'en avoir subi les conséquences. Nous croyons que la notification des atteintes à la protection des données s'avérera très utile à cet égard.

Deuxièmement, même les victimes les mieux informées et les plus motivées font face à des obstacles extrêmement contrariants lorsqu'elles tentent de mettre fin aux préjudices et de se refaire une réputation. Si ces obstacles étaient supprimés, les victimes seraient capables de limiter les préjudices et de prendre des actions préventives plus rapidement. Dans certains cas, elles pourraient aussi aider la police à identifier et à poursuivre les criminels.

● (0915)

Le président: Pardonnez-moi, madame Lawson. Puis-je vous demander de conclure? Je suis persuadé que les éléments que vous n'avez pas abordés seront soulevés pendant la période de questions.

Mme Philippa Lawson: Bien sûr.

Notre mémoire mentionne un certain nombre de mesures de protection des consommateurs précises que nous croyons utiles pour amener ces derniers à se protéger.

Nous recommandons avant tout que tous les intervenants du Canada, organismes d'application de la loi, organismes de protection des consommateurs, institutions financières et groupes de défense des consommateurs, travaillent ensemble afin de corriger le problème. Il nous faut élaborer une stratégie nationale afin de combattre le vol d'identité, et j'ai sept recommandations à ce sujet.

D'abord, comme je l'ai déjà mentionné, modifier la LPRPDE afin de créer des mesures incitatives efficaces en matière de conformité.

Deuxièmement, nommer un organisme à l'échelle fédérale qui sera chargé de collecter et de divulguer des données sur le vol d'identité et de coordonner les efforts visant à combattre le vol d'identité dans l'ensemble du Canada.

Troisièmement, comme je l'ai déjà mentionné, mandater l'Agence de la consommation en matière financière du Canada d'entreprendre une campagne nationale de sensibilisation.

Quatrièmement, créer un bureau national d'aide aux victimes de vol d'identité, encore une fois avec le mandat de recueillir des données, d'analyser le problème et de formuler des recommandations en matière de réforme des lois et des politiques.

Cinquièmement, exiger des établissements de crédit qu'ils rapportent les cas de vol d'identité.

Sixièmement, accorder aux consommateurs des droits qui renforcent leur capacité à déceler et à prévenir le vol d'identité et à en réduire les effets. Ces droits doivent notamment permettre aux consommateurs d'accéder à la version de leur rapport de solvabilité sur laquelle s'appuient les établissements de crédit, ce qui constitue actuellement un problème parce qu'ils n'y ont pas accès. Il faut aussi donner le droit aux consommateurs à une limitation du crédit en leur permettant d'en faire la demande auprès des agences d'évaluation du crédit, ce qui encore une fois leur est interdit actuellement.

Finalement, nous devons réviser en profondeur les lois régissant les agences d'évaluation du crédit, les établissements de crédit et les services de police afin d'aider à prévenir, détecter et réduire le vol d'identité.

Merci.

Le président: Merci.

Nous vous remercions pour votre mémoire. Je sais que les questions que vous venez de soulever y sont également traitées. Dès que le document aura été traduit, il sera distribué et nous aurons l'occasion de l'examiner plus en détail.

Et voici maintenant la déclaration préliminaire de M. Lawford.

M. John Lawford (conseiller juridique, Initiative canadienne des consommateurs): Merci beaucoup.

Je suis ici aujourd'hui en tant que représentant de l'Initiative canadienne des consommateurs, dans laquelle sont regroupés six organismes qui défendent les droits des consommateurs, dont le Centre pour la défense de l'intérêt public, où je travaille, l'Union des consommateurs, Option consommateurs au Québec, l'Association pour la protection des automobilistes, et l'Alberta Council on Aging. Nous vous présentons aujourd'hui notre position commune à l'égard du vol d'identité, position sur laquelle nous nous sommes entendus au cours de la dernière année.

La chose la plus importante à retenir de notre présentation aujourd'hui est une observation qui rejoint les propos de Philippa, c'est-à-dire que nous croyons qu'il y a un grand rôle qui doit être joué par le gouvernement et le monde des affaires pour attaquer le problème que représente le vol d'identité, ce qui n'a pas été fait. Nous croyons aussi que les consommateurs doivent être informés. Mais les premières mesures que vous devriez prendre en tant que législateurs devraient permettre d'amener le gouvernement et les entreprises à s'unir pour mieux protéger les renseignements personnels, ce qui réduirait le nombre de vols d'identité.

Si vous le permettez, je vais vous faire part de quelques statistiques de PhoneBusters que votre recherchiste vous a probablement déjà fournies. L'année dernière, 16 millions de dollars en pertes ont été déclarés à PhoneBusters, pour un total de 7 000 à 8 000 plaintes formulées. Ce total représente environ le double de l'argent perdu, mais la moitié des victimes par rapport à l'année précédente. Je ne sais pas si cette tendance va se maintenir, mais c'est inquiétant puisque cela signifie peut-être que le vol d'identité est plus profitable qu'avant et qu'il y a davantage de façons de faire de l'argent par fraude liée au vol d'identité.

Nous voulons également vous rappeler que cette situation n'est pas inévitable. Il existe un vide à l'échelon fédéral. Les consommateurs ne savent pas à qui s'adresser. Lorsqu'il y a des appels concernant le vol d'identité, je dois vraiment réfléchir et me demander où devrais-je d'abord diriger ces personnes? Vers les services de police, pour remplir un rapport de police? Vers une agence d'évaluation du crédit, pour obtenir un rapport de solvabilité? Vers l'équipe de PhoneBusters, pour déclarer le vol d'identité? Vers leur institution financière? En fait, toutes ces démarches doivent être entreprises, mais il n'existe pas encore de service à guichet unique au gouvernement fédéral, et c'est ce qui devrait être fait.

La situation est différente aux États-Unis, puisque la Commission fédérale du commerce est responsable des dossiers relatifs à la protection des consommateurs. Cet organisme a mis en place certaines mesures visant la création d'un site Web pour répondre aux préoccupations des consommateurs et des entreprises en matière de vol d'identité.

Prenons, par exemple, le guide des affaires de la Commission fédérale du commerce. Aux États-Unis, il y a maintenant un règlement concernant la protection de l'identité. Si vous êtes en possession de renseignements personnels de nature financière, vous devez respecter ce règlement. Le règlement est plutôt simple, et, en fait, il est similaire à la Loi sur la protection des renseignements personnels et les documents électroniques. Vous devez savoir quels renseignements sont contenus dans vos dossiers, vous ne devez conserver que le minimum d'information nécessaire, vous devez protéger ces renseignements par l'entremise de mesures de sécurité adéquates, vous devez éliminer les renseignements dont vous n'avez pas besoin et vous devez avoir un plan en cas d'atteinte à la protection des données.

Nous avons aussi un règlement comme celui-là ici, et ce, dans la Loi sur la protection des renseignements personnels et les documents électroniques. Mais la Loi n'est tout simplement pas appliquée. Ce qui nous préoccupe, dans le cadre de l'Initiative canadienne des consommateurs, c'est que le Commissariat à la protection de la vie privée du Canada n'a pas mis ce règlement en avant, en grande partie parce que, conformément à la loi, seules des plaintes individuelles peuvent être reçues. Le Commissaire à la protection de la vie privée peut procéder à une vérification pour les entreprises pour lesquelles on a noté un grand nombre de fuites pouvant mener au vol d'identité, mais il ne l'a pas fait de façon marquée.

Dans ce cas, il nous est difficile de formuler des recommandations au-delà de celles avancées par Philippa, si ce n'est que d'accorder au Commissaire à la protection de la vie privée un plus grand pouvoir d'action et le pouvoir de donner des directives, mais ça ne fait pas partie des suggestions présentées par le comité.

Un point que nous voulions obtenir, et qui était suggéré dans le rapport sur la Loi sur la protection des renseignements personnels et les documents électroniques, était un règlement sur la déclaration des intrusions dans les données. Selon nous, un tel règlement permettrait de réduire de beaucoup le nombre de vols d'identité, puisque compte tenu du temps requis pour procéder au vol d'identité, bon nombre des pertes surviennent au cours des deux, trois ou quatre premiers jours. Si un processus pouvait être mis en œuvre par l'entreprise pendant cette période-là, les gens pourraient prendre les mesures nécessaires afin de bloquer leurs comptes en téléphonant à leur institution financière et en avisant l'agence d'évaluation du crédit.

● (0920)

Un autre élément que nous avons suggéré d'inclure à la législation, en plus de ce que je viens de mentionner, est la surutilisation des numéros d'assurance sociale, et ce phénomène perdure. Le numéro d'assurance sociale constitue un élément clé dans l'obtention de nouveau crédit, et certains des cas de vol d'identité se font par l'ouverture de nouveaux comptes au nom de la victime, processus qui requiert habituellement un numéro d'assurance sociale. Le problème ici, c'est que les entreprises utilisent le numéro d'assurance sociale comme identificateur unique de la personne, et, dans la position commune, nous demandons qu'il soit indiqué dans la législation que les entreprises cessent d'utiliser les numéros d'assurance sociale à des fins d'identification et que l'utilisation des numéros d'assurance sociale soit limitée à celle d'origine, c'est-à-dire pour les démarches liées à l'emploi.

Nous reconnaissons la difficulté liée à l'établissement d'un identificateur unique qui pourrait être utilisé pour l'octroi de crédit. Cependant, en raison de l'utilisation fort répandue du numéro d'assurance sociale et ce, à tant de fins différentes, le numéro d'assurance sociale constitue une invitation à la fraude. En fin de compte, notre position est que nous aimerions que le gouvernement examine en profondeur l'utilisation que font les entreprises des numéros d'assurance sociale, et qu'il en réduise l'utilisation au minimum.

Une autre suggestion présentée dans notre position commune est que les gouvernements provinciaux examinent la possibilité de mettre en œuvre un mécanisme de limitation du crédit, pour que si vous appreniez que votre identité a été volée, vous puissiez communiquer avec l'agence d'évaluation du crédit pour empêcher l'octroi de nouveau crédit sans la mise en place de mesures exceptionnelles. Ce n'est peut-être pas de votre ressort, mais cela soulève certaines questions sur l'utilisation, par les agences d'évaluation du crédit, des renseignements concernant l'identité.

Pour l'instant, vous n'avez pas à traiter de la question des actes criminels. Le simple fait d'accumuler des boîtes et des boîtes de documents concernant l'identité ne constitue pas un crime actuellement, mais nous appuyons les efforts déployés par le ministère de la Justice pour en faire un acte criminel.

Nous aimerions également aborder une question qui revient à celle de ne pas avoir de guichet unique en place pour les Canadiens en ce qui concerne les vols d'identité. Nous n'avons pas vraiment non plus de données statistiques très détaillées concernant ce phénomène. Nous avons les données consignées dans le cadre de PhoneBusters, mais, encore une fois, les plaintes reçues dans ce contexte proviennent seulement de personnes qui savent que PhoneBusters acceptent les plaintes en matière de vol d'identité, ce qui réduit de beaucoup le nombre de cas signalés. Et beaucoup d'autres personnes ne portent tout simplement pas plainte par l'entremise de PhoneBusters.

Je sais qu'à la GRC, on a tenté de créer une base de données, nommée Signalement en direct des délits économiques, et je ne sais pas ce qu'il en est actuellement, mais il s'agit vraisemblablement d'un bon point de départ pour la centralisation de ces données statistiques. Une idée intéressante qui a été présentée aux États-Unis est de demander aux institutions financières de signaler le vol d'identité de sorte que, lorsqu'elles reçoivent une plainte en matière de vol d'identité — et elles en sont généralement informées par les consommateurs lorsqu'il y a un problème — elles pourraient signaler le cas à la GRC ou à toute autre organisation dans le but de recueillir des données à ce sujet. Nous sommes d'accord avec cette idée, même si elle ne fait pas partie de notre position commune.

Le dernier élément que nous aimerions apporter est que, dans cette situation, nous ne voulons pas que les consommateurs soient encore plus affectés par ce problème, et nous avons constaté deux tendances qui ne disent rien de bon. L'une est que les institutions financières ou autres offrent maintenant des assurances contre le vol d'identité, et nous ne croyons pas qu'il s'agit d'une bonne protection ni d'une bonne solution. Nous, au Centre pour la défense de l'intérêt public, avons produit un rapport concernant ce phénomène. Cette protection ne couvre que le temps réel passé à l'extérieur des heures de travail pour régler le problème. Elle ne couvre pas la fraude liée au vol d'identité comme tel, c'est-à-dire l'argent que vous perdez. Elle offre un certain nombre d'autres protections qui ne sont pas de grande importance, mais, à la base, nous pensons que c'est une façon d'imposer aux consommateurs les coûts et les responsabilités liés au vol d'identité, et ça va à l'encontre de ce que nous visons pour les entreprises, c'est-à-dire une protection plus complète des renseignements personnels.

La deuxième tendance qui nous préoccupe, c'est la volonté de créer une carte d'identité nationale ou d'autres identificateurs biométriques dans le but d'identifier absolument une personne. Puisque le vol d'identité est davantage un crime de nature sociale impliquant des facteurs comme la facilité d'obtention du crédit et la surcollecte de données, nous ne pensons pas que le fait d'avoir un identificateur unique lié à toutes les données améliorera la situation. En fait, ça pourrait même l'empirer.

Alors voilà ce que nous voulions présenter au comité aujourd'hui, et c'est avec plaisir que je répondrai aux questions, en anglais ou en français. Merci.

● (0925)

Le président: Merci beaucoup, monsieur Lawford.

Avant de passer aux questions, pour lesquelles nous allons commencer avec M. Pearson, pourriez-vous, madame Lawson, définir les concepts d'hameçonnage et de détournement de domaine?

Mme Philippa Lawson: Bien sûr. L'hameçonnage est l'acquisition frauduleuse de renseignements personnels par une personne qui se fait passer dans un courriel pour une entité de confiance, comme une banque ou eBay ou PayPal ou tout autre établissement financier. Le destinataire du courriel se voit demander des renseignements sur son compte sous prétexte, notamment, de corriger un problème ou de lui permettre d'avoir accès à son compte. Vous avez sûrement déjà reçu ce genre de courriel. J'en reçois tous les jours. Il s'agit d'un stratagème des fraudeurs pour acquérir les renseignements dont ils ont besoin pour accéder à des comptes en banque et en faire un usage frauduleux.

Le détournement de connexion est une technique de même genre par laquelle les voleurs redirigent un trafic légitime sur un site Web d'une institution financière de confiance vers de faux sites qui l'imitent de façon très convaincante. Ils invitent aussi les gens à entrer des renseignements sur leur compte, qu'ils utilisent ensuite pour se livrer à la fraude.

Il existe une troisième tendance, l'hameçonnage vocal, qui se fait au téléphone, par communication directe ou par des messages automatisés. Le consommateur répond au téléphone. Un message automatisé, soi-disant d'une banque ou d'une institution de confiance, l'avise alors qu'une complication est survenue concernant son compte et lui demande de composer un numéro 1-800 en vue de régler ce problème. Lorsque la personne appelle ce numéro, une boîte vocale interactive lui demande de fournir tous les renseignements sur son compte. C'est une autre façon de recueillir les renseignements.

● (0930)

Le président: Merci.

Monsieur Pearson.

M. Glen Pearson (London-Centre-Nord, Lib.): Merci, monsieur le président.

C'est beaucoup d'information. Je n'avais jamais entendu parler d'hameçonnage téléphonique avant aujourd'hui.

J'ai plusieurs questions, mais avant d'aller plus loin, n'avez-vous pas dit dans votre rapport que le nombre de vols d'identité diminuait?

Mme Philippa Lawson: John en a également fait mention.

Les données de PhoneBusters semblent corroborer cette affirmation. Mais selon moi, ces statistiques ne sont pas fiables. PhoneBusters est le fruit d'une collaboration entre la GRC, la PPO et le Bureau de la concurrence. Je suggère que vous fassiez comparaître une personne travaillant chez PhoneBusters sur ces statistiques.

M. Glen Pearson: Cela me semble un peu confus. L'ensemble des témoins a, tout comme vous ce matin, fait état de l'augmentation rapide de ce phénomène, sous différentes formes. On nous affirme cependant qu'il serait plutôt en train de perdre de l'ampleur. Je crois que nous avons la responsabilité de ne pas nous immiscer dans un dossier si celui-ci ne pose plus problème. Il est difficile de faire la juste part des choses.

Madame Lawson, vous parliez d'une stratégie nationale de cueillette de renseignements — Croyez-vous vraiment que cette stratégie soit nécessaire. Qui devrait s'en charger?

Mme Philippa Lawson: Nous croyons qu'il faut désigner un organisme responsable. Il faut, dans un premier temps, demander aux organismes aux prises avec des vols d'identité dans le cadre de leurs activités — et ce, même si leur charge de travail s'en trouve alourdie — de faire un suivi et de produire un rapport annuel sur les vols d'identité dont leurs clients ou eux-mêmes ont été victimes, ainsi que sur les tentatives dont ils ont fait l'objet et qu'ils ont pu bloquer.

Je crois qu'en procédant ainsi, nous aurons une bien meilleure idée de l'étendue du problème.

M. Glen Pearson: Est-il question d'un organisme gouvernemental?

Mme Philippa Lawson: Quelqu'un doit en prendre la responsabilité.

Comme John le soulignait, il y a ici une lacune à combler. Il n'existe pas d'organisme de protection du consommateur au fédéral. Seul le Comité sur les mesures en consommation d'Industrie Canada intervient dans ce secteur de manière restreinte, notamment en ce qui a trait à la coordination des stratégies provinciales. Le Bureau de la concurrence ne se définit pas comme un organisme de protection du consommateur. Il ne semble pas s'intéresser à ce problème précis.

M. Glen Pearson: Lors de son passage il y a deux ou trois semaines, la Commissaire à la protection de la vie privée a mentionné, entre autres, que le réel problème réside dans le fait qu'il n'existe aucune base de données sur l'ensemble de ces questions. Il faudra donc se pencher sur la meilleure façon d'y arriver.

Vous avez formulé un ensemble de recommandations. Bien que nous n'ayons pas votre rapport, nous savons que vous en avez fait un grand nombre. Laquelle de ces recommandations devrait être suivie en priorité? Je sais que c'est un exercice difficile, mais nous avons besoin de votre avis, puisque nous ne disposons pas de votre rapport — quelle orientation voudriez-vous que le comité suive?

Mme Philippa Lawson: Cette question est complexe. Il serait probablement utile de mettre sur pied un groupe de travail comme celui qui a été créé il y a deux ou trois ans sur les pourriels. J'en faisais partie. J'ai participé à deux ou trois groupes de travail et je peux attester l'utilité de ce processus, qui, en réunissant les différents intervenants, a permis de s'attaquer à des problèmes difficiles et de formuler un ensemble solide de recommandations, qui n'ont malheureusement pas encore été suivies.

Je ne voudrais pas pour autant retarder la mise en œuvre de certaines mesures qui pourraient être prises dès maintenant. J'ai en suggéré quelques-unes. Mais je crois que, dans l'ensemble, cette question requiert la création d'un groupe de travail.

Sans vouloir remettre en question l'enquête et l'examen que vous avez déjà menés, je suis fermement convaincu de la nécessité de mesures incitatives pour faire respecter la loi sur la protection des données par les entreprises.

M. Glen Pearson: Merci.

Monsieur Lawford, je travaille comme bénévole dans une banque alimentaire. Auparavant, nous demandions systématiquement les numéros d'assurance sociale. La plupart des organisations caritatives ont pu omettre de le faire, car personne n'était tenu de donner quoi que ce soit. Pourtant, selon vous, les établissements de crédit, notamment, n'emploient pas le numéro d'assurance sociale comme mode d'identification de base.

Vous avez également affirmé que vous n'étiez pas à l'aise avec l'idée de la carte biométrique, mais qu'il fallait également restreindre la nécessité d'identification par NAS ou par d'autres moyens.

Comment y parvenir? Pouvez-vous nous donner un exemple?

M. John Lawford: C'est une question délicate. L'identificateur unique, s'il est nécessaire, ne doit pas s'appliquer à tout. Pourquoi ne pas en prévoir un pour les agences d'évaluation de crédits, avec un numéro du type de celui employé par l'agence d'évaluation de crédit? Chacun recevrait une longue série de chiffres uniquement aux fins d'identification pour le crédit, qui ne remplacerait par le NAS, utilisé à d'autres fins. Le NAS pose bien sûr un problème, parce qu'il sert de mot de passe à trop d'activités.

Nous craignons que ce problème double d'ampleur si vous créez une carte d'identité nationale, car cette carte sera requise pour toutes les activités. Il faudrait peut-être maintenir un certain cloisonnement, même si je ne sois pas sûr qu'il s'agisse de la meilleure solution, faute d'études sur ce mode d'utilisation et sur sa mise en œuvre. Il n'en demeure pas moins que l'idée d'un identificateur pour l'ensemble de la population et servant à plusieurs fins me semble inquiétante.

● (0935)

M. Glen Pearson: Selon vous, il faudrait donc créer différents identificateurs pour différents groupes. Cela semble plutôt difficile à gérer.

M. John Lawford: Ma suggestion s'inscrit plutôt dans l'esprit de la législation sur la vie privée, voulant que les renseignements personnels ne puissent être utilisés à d'autres fins que celles prévues lors de leur collecte. Le numéro d'assurance sociale donne accès à trop de renseignements provenant de sources diverses.

Mme Philippa Lawson: J'ajouterai que l'authentification est au cœur du problème, auquel s'attaquent l'industrie, les entreprises privées et le gouvernement. Je siège à un groupe de travail présidé par Industrie Canada sur les principes en matière d'authentification électronique. C'est un énorme défi.

On reconnaît en principe que l'authentification à un facteur, avec un simple mot de passe, est insuffisante. Cette protection est trop facile à forcer. Nous devons donc suivre l'exemple des entreprises et passer à l'authentification à facteurs multiples.

Autre problème d'envergure: les gens font souvent appel à une forme simple d'authentification constituée d'un ensemble de renseignements personnels. Les technologues, les ingénieurs et les experts en informatique sont parvenus à des modes fiables d'authentification, sans qu'il soit nécessaire d'enregistrer un ensemble de renseignements personnels, notamment au moyen d'algorithmes informatiques. Le défi consiste donc à convaincre l'industrie de délaisser la forme simple d'authentification au profit de mesures qui réduisent la collecte de données personnelles.

M. Glen Pearson: Dernière question : si je —

Le président: Non, je suis désolé. Vous disposerez de tout le temps nécessaire au troisième tour de questions.

Madame Lavallée, sept minutes.

[*Français*]

Mme Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Merci beaucoup, monsieur le président.

Bonjour. Vous nous avez dit au tout début de votre allocution à quel point on ne faisait pas état de la situation. En vous écoutant parler, je constate que plusieurs types de fraude se font par l'entremise d'Internet. Il y a aussi de la fraude qui se fait au moyen du téléphone. J'en ai entendu parler chez moi, dans mon milieu. Des gens se sont fait prendre de toutes les façons imaginables. Dans certains cas, on leur demandait des renseignements en se faisant passer pour des représentants de l'institution détenant leur carte de crédit. La copie des cartes de crédit ou de débit semble être une troisième façon de procéder à un vol d'identité. Y en a-t-il d'autres?

Mme Philippa Lawson: Oui, il en existe beaucoup. Nous avons publié un rapport sur les techniques de vol d'identité.

[*Traduction*]

Les différents procédés auxquels recourent les voleurs d'identité pour recueillir des renseignements personnels figurent sur notre site Internet. Je pourrais parler d'autres méthodes, si vous le désirez, mais, comme je l'ai déjà dit, il en existe un large éventail, allant de la fouille des vidanges au piratage de bases de données informatiques. Les voleurs d'identité emploient plusieurs de ces méthodes.

Une des méthodes classiques des voleurs de carte de débit est l'emploi d'un dispositif d'écrémage, la plupart du temps dissimulé sous un comptoir. Vous tendez votre carte de crédit au commis du magasin, le fraudeur, qui profite d'un moment d'inattention pour passer la carte à la fois dans la bonne machine et dans celle conçue pour un usage frauduleux. Ces dispositifs d'écrémage sont vendus librement sur le marché.

● (0940)

[*Français*]

Mme Carole Lavallée: Vous avez dit plus tôt qu'il y avait des moyens traditionnels, par exemple la fouille des poubelles et des boîtes aux lettres, Internet, où l'on retrouve des méthodes plus sophistiquées, ainsi que le téléphone et les magasins. Je pense que ce sont essentiellement les quatre moyens utilisés. J'essaie d'en faire le tour.

Mme Philippa Lawson: Le vol d'information se fait très souvent par des —

[*Traduction*]

Plusieurs vols d'identité ont été attribués à des employés travaillant au sein des organismes, qui se font graisser la patte pour remettre ces renseignements aux voleurs d'identité.

[*Français*]

Mme Carole Lavallée: Donc, il arrive régulièrement que des gens se fassent voler leur identité, et les tentatives pour y arriver sont nombreuses. J'ai moi-même reçu à la maison un courriel qui semblait provenir de mon institution financière. On me demandait de me réabonner à quelque chose. Vous connaissez sans doute cette technique. De plus en plus, on entend des gens dire que leur carte de crédit ou leur carte de débit a été copiée. Parallèlement, on entend dire que les banques deviennent plus frileuses et qu'elles annulent instantanément la carte de débit ou la carte de crédit des gens ayant fait une transaction à l'endroit où la carte d'un client de la banque s'est fait copier. Je comprends que les institutions financières deviennent de plus en plus frileuses, mais il est très difficile pour un consommateur de se faire retirer aussi bien sa carte de crédit que sa carte de débit la fin de semaine de Noël. Il y a donc un véritable problème.

Vous dites ne pas connaître le nombre de personnes qui se sont fait voler leur identité. Vous n'avez aucune donnée à ce sujet?

[*Traduction*]

Mme Philippa Lawson: Comme je l'ai dit précédemment, au Canada, nous ne disposons que de deux sources d'information à ce sujet: PhoneBusters, qui s'en remet aux quelques rares plaintes reçues, et quelques sondages d'opinion.

Mes collègues, M. Norm Archer et Mme Susan Sproule, qui participent au projet financé par l'ORNEC à l'Université McMaster, se sont penchés sur ce manque de données statistiques. Ils ont réalisé une enquête auprès des consommateurs et devraient bientôt rendre les résultats publics. Vous aimeriez peut-être les faire comparaître sur cette question. Il semble que nous ne disposons pas des données statistiques nécessaires.

Tout comme John, j'aimerais souligner qu'aux États-Unis, le FTC a été mandaté, dans le cadre de la législation en matière de vol d'identité, pour recueillir des données statistiques et les diffuser. Concernant l'ampleur du problème, le FTC aux États-Unis est donc une source d'information qui, bien qu'insuffisante, est plus complète que ce dont nous disposons au Canada.

[*Français*]

Mme Carole Lavallée: Les banques doivent quand même avoir des statistiques à ce sujet. On voit bien qu'elles réagissent et qu'elles deviennent plus frileuses. Elles gèlent les cartes de crédit beaucoup plus rapidement qu'avant. Elles doivent connaître l'ampleur du problème.

[*Traduction*]

Mme Philippa Lawson: Selon moi, les banques sont la meilleure source d'information sur l'étendue du problème. C'est pourquoi nous recommandons qu'elles soient tenues de produire des rapports sur cette question.

Le président: Merci.

En vue d'informer les membres du comité, nous avons invité des représentants de PhoneBusters et les chercheurs de l'Université McMaster à comparaître devant nous.

On retrouve des techniques de vol d'identité sur le site Internet de la CIPPIC : il s'agit peut-être ici d'une arme à double tranchant. Vingt-trois techniques y sont mentionnées. Avis à tous les amateurs de vol d'identité qui veulent savoir comme s'y prendre.

Une voix: Ces comités serviraient donc à l'apprentissage du vol?

Le président: Je ne crois pas que beaucoup de voleurs d'identité seraient prêts à écouter les délibérations de notre comité, mais qui sait.

Laissons la parole à M. Stanton, s'il vous plaît, pour les sept prochaines minutes.

● (0945)

M. Bruce Stanton (Simcoe-Nord, PCC): Merci, monsieur le président, et merci aux témoins de s'être déplacés ce matin pour nous fournir des explications sur ce problème déconcertant.

En premier lieu, madame Lawson, vous avez mentionné au cours de votre présentation, sans vous citer mot à mot, que plusieurs consommateurs victimes de vol d'identité n'avaient aucun moyen de se défendre, qu'ils se sont trouvés dans cette situation par inadvertance et qu'ils n'auraient rien pu faire pour s'en prémunir.

Parallèlement, la plupart de vos recommandations, comme celles d'autres personnes, font état de la nécessité de pallier le manque de renseignements pour les consommateurs.

On constate qu'il existe deux points de vue diamétralement opposés. Pourriez-vous nous faire part de votre opinion à ce sujet.

Mme Philippa Lawson: Ce problème comporte plusieurs facettes. Selon nous, le consommateur était souvent, sinon la plupart du temps, dans l'impossibilité de réagir. Mais il arrivait parfois qu'il en ait la possibilité; en effet, le consommateur aux prises avec un courriel d'hameçonnage ou un stratagème d'ingénierie sociale pouvait éviter de se faire prendre en ne répondant pas aux courriels provenant soi-disant d'une banque ou d'un établissement financier. C'est dans ce genre de sensibilisation que nous devons investir.

Les consommateurs peuvent prendre certaines mesures. Déchiqueter les documents contenant des renseignements personnels avant de les jeter. Ne pas répondre aux courriels suspects. Et s'assurer que l'adresse URL du site bancaire ou de l'établissement qu'ils utilisent pour leurs opérations financières en ligne est bien une adresse http; en effet, les sites d'hameçonnage ont rarement une adresse http.

Les consommateurs peuvent se défendre. Le problème réside en partie, mais pas totalement, dans la crédulité et la négligence du consommateur.

M. Bruce Stanton: Merci.

Monsieur Lawford, nous avons été extrêmement surpris d'apprendre que certains organismes utilisent les NAS comme identificateurs uniques. Si je ne m'abuse, vous avez cité en exemple l'ouverture d'un compte en banque. La nouvelle norme des établissements financiers n'est-elle pas désormais la présentation d'une carte d'identité à photo pour l'ouverture de tout type de compte financier, aux fins d'épargne ou d'investissement?

M. John Lawford: Oui, je sais que les établissements financiers les exigent souvent, pour ajouter une étape de vérification.

Le Centre pour la défense de l'intérêt public recommande notamment, dans le premier rapport, que les entreprises prennent certaines mesures simples, comme de s'efforcer de contrôler l'identité.

Il arrive qu'on vous prenne votre carte de crédit sans même lire le nom ou vérifier votre signature. Une mesure simple à réaliser consisterait à former les commis pour s'assurer, entre autres, qu'ils vérifient vraiment que les signatures correspondent.

Je ne dis pas que c'est une mauvaise chose, mais est-il vraiment nécessaire d'effectuer de nouvelles vérifications de la solvabilité? Certains exigent déjà une vérification de la solvabilité pour ouvrir un nouveau compte de téléphone cellulaire. Même si la vérification s'avère inutile, le NAS demeure dans la base de données de l'entreprise de téléphonie cellulaire. Si la sécurité de cette base de données est compromise, les numéros de carte de crédit peuvent tomber entre de mauvaises mains. Dans ce genre de situation, les demandes de crédits, qu'elles soient nécessaires ou non, se retrouvent intégrées aux activités commerciales types. Or les NAS sont systématiquement demandés lors de ces demandes.

Mme Philippa Lawson: Puis-je faire un court commentaire?

La Commissaire à la protection de la vie privée a conclu de manière décisive que la collecte de numéros d'assurance sociale, sauf si elle est nécessaire aux banques, aux employeurs et ainsi de suite, enfreint la LPRPDE. C'est une violation de la loi. Ce qui nous ramène au problème que j'ai déjà soulevé, à savoir que nous n'appliquons pas la loi.

M. Bruce Stanton: Merci.

C'est curieusement sur ce point que je veux intervenir.

Votre présentation de ce matin m'a aussi fait réfléchir sur la nécessité d'examiner la LPRPDE. Je partage votre opinion voulant que la LPRPDE soit le mécanisme par lequel les organismes et les entreprises seront tenus de se conformer à la loi et à un ensemble de pratiques. Vous avez très clairement démontré que les entreprises ont un rôle à jouer dans ce processus.

Mais le Commissariat à la protection de la vie privée et la Commissaire à la protection de la vie privée en personne, remettent résolument en question la nécessité des pouvoirs exécutoires et semblent convaincus que le modèle de l'ombudsman fonctionne efficacement. Elle souligne que les consommateurs sont de plus en plus sensibilisés aux questions relatives à la protection de la vie privée. Vous avez d'ailleurs suggéré dans l'un de vos commentaires, le deuxième si je ne m'abuse, de créer un organisme responsable de ces questions relatives au vol d'identité.

Je me dois d'insister. Comment se fait-il que votre point de vue sur ces questions soit si diamétralement opposé à celui de la Commissaire à la protection de la vie privée? Le Commissariat à la protection de la vie privée n'est-il pas tout désigné dans ce dossier?

● (0950)

Mme Philippa Lawson: Bien sûr. Je ne me l'explique pas non plus. Je ne saurais être plus en désaccord avec elle sur ce point.

M. Bruce Stanton: Vous êtes en désaccord. Vos points de vue sont différents. Restons-en là.

Pour en revenir aux lois sur la protection du consommateur, le Comité des mesures en matière de consommation a fait une présentation lors de notre dernière réunion. Cet organisme est en réalité un groupe d'encadrement par l'entremise duquel les différentes provinces collaborent. En effet, il est bien connu que les lois sur la protection du consommateur sont de compétence provinciale.

Cet organisme réalise donc dans les moindres détails le contenu de votre recommandation. Quelles lacunes existe-t-il encore? Si le Comité des mesures en matière de consommation est effectivement l'organisme responsable de ce dossier, qu'il constitue un programme d'éducation, qu'il contribue à rassembler les intervenants, quel est son point faible?

Mme Philippa Lawson: Oui, je crois que le Comité des mesures en matière de consommation fait un très bon travail, mais ce n'est pas suffisant. Il ne rassemble pas les intervenants en matière d'application de la loi. Les services de police détiennent beaucoup d'information et peuvent intervenir de nombreuses façons, en particulier auprès des victimes, qui sont une excellente source d'information sur la nature et l'ampleur du problème.

En joignant d'autres intervenants, nous nous sommes entretenus des banques et des établissements de crédit et nous avons discuté de leurs rôles. Les agences d'évaluation du crédit ont un rôle important à jouer dans ce dossier. Nous nous sommes rendu compte, en parlant aux victimes et en examinant les études de cas, que le système d'enregistrement des crédits de l'agence d'évaluation du crédit présente des lacunes. Il faut faire une étude plus approfondie de cette question.

En ce qui concerne les organismes de défense des consommateurs, il faut examiner l'ensemble des volets de ce dossier, dans les secteurs criminel, civil, privé et public, ainsi que dans les administrations fédérale et provinciales. Les travaux du CMC ne portent que sur une partie du problème.

M. Bruce Stanton: Il y a encore du travail à faire.

Merci, monsieur le président.

Le président: M. Pearson, puis M. Van Kesteren.

M. Glen Pearson: Merci, monsieur le président.

J'avais encore quelques questions sur le NAS, mais je vais les mettre de côté.

Monsieur Stanton, avez-vous obtenu des réponses suffisamment claires relativement à cette question?

M. Bruce Stanton: Oui.

M. Glen Pearson: Bien. Je ne poserai donc pas d'autres questions à ce sujet.

Madame Lawson, vous avez parlé de recours collectifs. Selon M. Lawford, vous voudriez notamment éviter d'imposer un trop lourd fardeau aux consommateurs. N'est-ce pas précisément ce qui arrivera si vous intentez un recours collectif? Qu'en dites-vous?

Cette mesure n'est pas aussi populaire au Canada qu'aux États-Unis? Pourriez-vous m'aider à comprendre?

Mme Philippa Lawson: Il existe plusieurs recours collectifs. La juridiction du Québec est avant-gardiste au Canada en matière de recours collectif. Plusieurs consommateurs ont ainsi pu obtenir un redressement.

Les recours collectifs sont précisément conçus pour la prise en charge des consommateurs, en vue de les encourager à abandonner les mauvaises pratiques et à se prendre en main: les consommateurs ont accès gratuitement à une représentation juridique et sont représentés automatiquement, même sans l'avoir réclamé, dans la mesure où ils font partie de la catégorie concernée.

Il suffit qu'une seule personne, représentant une catégorie de consommateurs, soit victime de pratiques illégales pour qu'elle puisse intenter un procès et retenir les services d'un avocat en recours collectif. Les avocats prennent en général la cause à leur compte et procèdent à la poursuite selon un régime d'honoraires conditionnels. Ce système libère le consommateur du fardeau de la poursuite et permet à tous les consommateurs de la catégorie d'obtenir un redressement.

M. Glen Pearson: Monsieur Lawford, vous avez parlé de la Federal Trade Commission aux États-Unis. Concernant notre échange à propos de ma dernière question sur le NAS ou la carte biométrique, vous affirmez qu'il y a plusieurs avenues possibles. Comment la Federal Trade Commission a-t-elle procédé?

● (0955)

M. John Lawford: Il me semble qu'actuellement, aux États-Unis, la FTC n'a pas donné son aval à un projet du même genre: la Real ID Act. En vertu de cette loi, les permis de conduire approuvés et comportant des données biométriques pourraient servir à de multiples usages. Il me semble que la FTC s'est prononcée contre ce projet. Il faudrait que je vérifie.

En ce qui concerne votre question, je ne suis pas certain d'en saisir le sens. Comment a-t-elle procédé pour —?

M. Glen Pearson: Comment l'identité des gens peut-elle être protégée si nous ne —?

Continuez.

M. John Lawford: La FTC dirige les gens vers un site unique; elle leur demande s'ils ont à se plaindre de vols d'identité aux fins de compiler des statistiques — et les gens collaborent. Si vous tapez « vol d'identité » dans Google, la page d'accueil de FTC figurera en tête de vos résultats de recherche.

C'est là que les gens vont. Ils savent ce qu'ils font. Ils prennent des mesures contre les entreprises, car ils peuvent faire appel à leur législation sur la protection des consommateurs. L'article 5 de la Federal Trade Act dit que les consommateurs doivent être protégés; ils ont d'ailleurs engagé des poursuites en vertu de cet article. Par exemple, Card Systems, aux États-Unis, aurait entamé des poursuites après avoir encouru des pertes avec ChoicePoint. Un organisme de cet ordre nous serait utile. Selon eux, l'entreprise a fait preuve de négligence lors de la collecte de données, ce qui contrevenait à la Federal Trade Act.

Voilà donc leur approche: ils appliquent la loi, recueillent de l'information et donnent des conseils aux consommateurs et aux entreprises.

M. Glen Pearson: Ont-ils des recommandations à faire en ce qui concerne, notamment, la carte biométrique et le numéro d'assurance sociale? Laquelle est la meilleure option? Vous avez suggéré d'autres possibilités. Ont-ils fait des recommandations?

M. John Lawford: Il faudrait que je vérifie. Je crois qu'ils se sont prononcés contre la Real ID Act, qui est une solution de type biométrique, mais je vais devoir m'en assurer.

M. Glen Pearson: D'accord.

Madame Lawson, j'aurais une dernière question si le temps me le permet. Vous dites que les entreprises doivent prendre plus de responsabilités, et ainsi de suite, de manière à ce qu'elles n'incombent pas autant aux consommateurs. Une chose qui préoccupe bon nombre d'entre nous, c'est l'accablant fardeau dont devraient se charger les petites entreprises pour être en mesure de le faire. Pouvez-vous commenter cette question?

Mme Philippa Lawson: Je crois que ce sont habituellement les grandes entreprises qui sont visées, ou du moins dans les cas dont nous entendons parler. Ce sont généralement les grosses banques de données, les grandes entreprises et les établissements de crédit qui ont des ennuis, je ne suis donc pas convaincue qu'on puisse parler d'une charge accablante pour les petites entreprises.

Encore une fois, lorsque nous considérons l'exécution de la loi sur la protection des données, nous parlons d'agir selon le gros bon sens de toute façon, de ce qui est bon pour le commerce et de ce qui l'est pour les consommateurs.

Le président: Merci.

Monsieur Lawford, est-ce que ça vous dérangerait de vérifier? Si vous pouviez obtenir ces réponses, peut-être pourriez-vous communiquer avec nos attachés de recherche et les leur transmettre.

Merci.

Monsieur Van Kesteren.

M. Dave Van Kesteren (Chatham-Kent—Essex, PCC): Merci, monsieur le président.

Merci à vous, mesdames et messieurs les témoins, pour vous être présentés de nouveau.

On dirait bien qu'il s'agit là d'une solution à trois volets.

D'abord et avant tout, nous devons sensibiliser les consommateurs, et je suis d'accord avec votre recommandation. Je crois que ce serait plus prudent ainsi et qu'il faudrait s'y mettre très bientôt, et nous devrions en prendre l'initiative.

Deuxièmement, oui, je crois que les sociétés et les institutions qui manipulent les informations sur le crédit devraient avoir une certaine responsabilité.

Troisièmement, nous ne devons pas négliger un élément qui doit être continuellement considéré en société, à savoir l'élément criminel. Il existe un projet de loi d'initiative parlementaire, le projet de loi C-299. Le connaissez-vous? Savez-vous qu'il porte sur l'hameçonnage et, je crois, sur la sollicitation téléphonique, qui vise à soutirer des informations personnelles. Qu'en pensez-vous? Sommes-nous sur la bonne voie? Sommes-nous trop enthousiastes à ce sujet?

Mme Philippa Lawson: Je suis tout à fait en faveur de ce projet de loi, mais je crois qu'il ne s'agit que d'une pièce du casse-tête. Ce n'est certainement pas la seule solution du côté du droit pénal, et je comprends que le ministère de la Justice examine toutes les modifications possibles au Code criminel qui pourraient offrir aux policiers les outils dont ils ont besoin pour poursuivre les voleurs d'identité. Nous savons d'après nos recherches qu'il existe de nombreuses autres façons dont le Code criminel pourrait être modifié pour aider à appliquer la loi contre les criminels de ce genre. Combattre l'imposture, vraiment, en est une, et nous appuyons le projet de loi C-299.

M. Dave Van Kesteren: N'oublions pas, et vous en avez parlé aussi, qu'il existe de nouvelles technologies tout à fait emballantes: la carte d'identité nationale, l'identification biométrique, comme vous l'avez mentionné, et les dispositifs d'identification par radiofréquence. Et puis j'ai lu votre mémoire et j'y vois une mise en garde. Vous semblez quelque peu hésitante à opter pour ces solutions: les cartes d'identité nationale, les identificateurs biométriques, les bases de données gouvernementales intégrées, toutes ces méthodes ont déjà été suggérées pour réduire le vol d'identité. Toutefois, ces initiatives soulèvent de sérieuses questions de confidentialité et nous ne devons pas les adopter sans avoir d'abord mené de solides consultations publiques, des débats et un examen approfondi des dangers qu'elles présentent pour les libertés civiles et l'affranchissement du contrôle gouvernemental.

Je me demande si vous pouvez élaborer à ce sujet. Vous semblez peu encline à suivre cette voie. Je me demande pourquoi.

● (1000)

M. John Lawford: Je crois qu'à la fin de votre déclaration, vous avez mentionné les effets que cela pourrait avoir sur les libertés civiles, et c'est là la principale préoccupation: ces solutions dépassent un peu le domaine du vol d'identité. Nous craignons aussi que ce ne soit pas forcément la solution miracle, si vous me permettez l'expression, en matière de vol d'identité, encore une fois parce que la situation ne se résume pas à l'obtention de vos données d'identification, c'est qu'il est également très facile d'obtenir du crédit par la suite. Les victimes ont beaucoup de difficulté à se débarrasser des taches laissées sur leur crédit et à restaurer leur cote de solvabilité. Alors notre objection à l'utilisation de la biométrie et des cartes d'identification nationale pour contrer le vol d'identité, c'est que d'un côté, encore une fois, la société civile ne croit pas que surveiller les gens à ce point constitue le bon moyen d'assurer la sécurité publique. Nous craignons que cela ne devienne un moyen de suivre pas à pas les gens dans leur vie quotidienne, si vous voyez ce que je veux dire, parce qu'il faudra présenter sa carte d'identité partout où on ira, et ce sera plus facile de suivre les gens, et c'est là que les implications sur les libertés civiles surviennent. Et puis, de l'autre côté, cela pourrait très bien ne pas résoudre le problème de vol d'identité du tout.

Mme Philippa Lawson: Puis-je ajouter quelque chose à ce sujet? Ces mesures pourraient en fait empirer le problème, comme John l'a dit. Les victimes ont déjà assez de difficultés à redresser leur situation lorsque leur numéro d'assurance sociale est compromis, par exemple. Imaginez si votre identité biométrique était compromise, et je peux vous assurer qu'elle pourrait l'être. Aucune de ces solutions technologiques n'est parfaite. Ce sera un véritable cauchemar pour les gens qui se verront usurper leur identificateur biométrique.

M. Dave Van Kesteren: Me reste-t-il du temps, monsieur le président?

Le président: Oui, 45 secondes.

M. Dave Van Kesteren: Nous tentons de trouver un juste milieu. Le consommateur aussi doit prendre une part de responsabilité.

John, vous avez mentionné que vous craigniez dans une certaine mesure que les gens soient surveillés, mais il reste quand même l'argent comptant. Je me soucie comme d'une guigne qu'on sache que je voyage d'Ottawa à Chatham, puis que je me dirige vers Détroit. Si ça me dérange, je peux toujours payer comptant. Certaines de ces méthodes semblent vraiment offrir des solutions prometteuses. Je ne crois pas que ce que j'ai entendu jusqu'à maintenant suffise à me convaincre que ce n'est pas la voie à adopter.

M. John Lawford: Très brièvement, je peux dire que je ne suis pas convaincu que c'est une bonne idée d'abandonner cette piste et qu'il reste d'autres préoccupations à ce sujet, en particulier si on fusionne les bases de données. Il est possible de brouiller ses dossiers d'appels et ses déplacements de toutes sortes de manières, et je crois que dans certaines situations, cela comporte plus d'implications négatives que nous ne pouvons l'imaginer.

En ce qui concerne l'argent comptant, on ne peut payer comptant sur Internet et il est impossible de payer en argent dans de nombreuses entreprises — elles préfèrent les cartes de crédit — on laisse donc des traces dans ces cas-là.

Je ne sais pas si j'ai répondu à votre question.

Le président: Madame Lavallée.

[*Français*]

Mme Carole Lavallée: Vous avez parlé à plusieurs reprises de PhoneBusters. J'imagine que l'image est très claire en anglais, mais je ne sais pas à quoi ça correspond en français.

M. John Lawford: En fait, les PhoneBusters, même en anglais, sont un concept un peu ancien. Au départ, ce groupe a été créé pour s'occuper des fraudes commises au moyen du téléphone. Il a évolué depuis et reçoit maintenant des plaintes concernant le vol d'identité. Le nom en anglais pourrait donc être remplacé par quelque chose de plus approprié.

Mme Carole Lavallée: Je veux simplement comprendre ce que c'est. Est-ce une agence, un organisme gouvernemental, un organisme sans but lucratif?

M. John Lawford: Il s'agissait d'une agence faisant partie de l'Ontario Provincial Police, mais je crois que maintenant, elle collabore aussi à un projet avec la GRC. Comme je l'ai dit, c'est un peu flou, ça a évolué au cours des dernières années. Il serait préférable de vérifier.

● (1005)

Mme Philippa Lawson: Le Bureau de la concurrence fait aussi partie de PhoneBusters .

Mme Carole Lavallée: Est-ce une association?

M. John Lawford: Je ne connais pas exactement le statut de l'organisme.

Mme Philippa Lawson: C'est une initiative.

M. John Lawford: En fait, ça pourrait disparaître demain.

Mme Carole Lavallée: Je suppose qu'il y a un numéro de téléphone que les gens peuvent utiliser. Visiblement, ça n'existe pas au Québec, car je n'en ai jamais entendu parler.

Mme Philippa Lawson: Peut-être que ça ne fonctionne qu'en anglais, je ne sais pas, mais il y a un site Web où on peut trouver de l'information : www.phonebusters.com, je crois.

Mme Carole Lavallée: Je ne comprends pas beaucoup de quoi il s'agit, mais est-ce qu'ils auraient des données sur le vol d'identité? Cela fait-il partie des questions pour les témoins que nous recevrons? Oui, d'accord.

[*Traduction*]

Le président: Ils pourront nous expliquer exactement qui ils sont, ce qu'ils font et quel est leur statut juridique.

[*Français*]

Mme Carole Lavallée: Parfait. Je vous remercie beaucoup, monsieur le président.

Au début de votre présentation, vous avez dit qu'il fallait changer des lois. Je voudrais savoir à quelles lois vous faisiez référence et comment on doit les changer exactement.

Je vous prierais de répondre l'un à la suite de l'autre, mais pas tous les deux en même temps.

M. John Lawford: Il y a la Loi sur la protection des renseignements personnels. Comme le comité l'a mentionné, il faudrait changer la loi pour qu'il soit nécessaire de dévoiler les fuites de renseignements.

En ce qui concerne le numéro d'assurance sociale, je ne sais pas s'il est inclus dans la loi que...

D'où ça vient?

Mme Philippa Lawson: C'est déjà contraire à la loi que d'utiliser le numéro d'assurance sociale si on n'a pas besoin de le faire. Le problème ne se situe pas dans cet aspect de la loi.

[*Traduction*]

Ces problèmes couvrent aussi l'application de la loi : il n'existe pas de mesures incitatives et de sanctions pour les organismes qui demandent le numéro d'assurance sociale alors qu'ils ne le devraient pas. On refuse aux consommateurs le droit de consulter leur rapport de solvabilité, malgré le fait que le droit relatif au respect de la vie privée le leur autorise. TJX et Winners scannent les cartes de crédit des acheteurs — Peut-être que tout le monde devrait utiliser de l'argent comptant, et peut-être est-ce là ce que nous devrions recommander. Mais cela irait certainement à l'encontre de la politique du gouvernement, qui tâche d'encourager le commerce électronique.

Ces magasins scannent les cartes de crédit et conservent les informations détaillées contenues sur la bande magnétique, alors qu'ils ne sont pas censés les garder et qu'ils n'y sont pas autorisés conformément au droit relatif au respect de la vie privée. Ils les conservent dans des bases de données aux États-Unis pendant des années, offrant ainsi une mine d'or aux voleurs d'identité.

Les grandes modifications qu'il nous faut vraiment apporter dans ce domaine touchent le régime d'application de la LPRPDE. Nous devons offrir aux plaignants des mécanismes plus efficaces pour porter leurs plaintes devant les tribunaux et obtenir des recours. Nous devons disposer de véritables sanctions en matière de finances et de réputation contre les organisations qui ne respectent pas la loi.

Nous devons également réviser les lois provinciales qui régissent les agences d'évaluation du crédit et qui assurent la protection des consommateurs. Le Comité des mesures en matière de consommation a déjà fait des progrès dans ce domaine, mais nous devons examiner comment nous pouvons améliorer les lois. Par exemple, elles devraient permettre aux consommateurs de limiter leur crédit dans leur rapport de solvabilité. Cela veut dire qu'aucun établissement de crédit ne pourrait avoir accès aux rapports de solvabilité sans le consentement explicite des consommateurs. Ça semble logique pour les victimes de vol d'identité et les gens qui ont de bonnes raisons de soupçonner qu'elles pourraient le devenir.

Le président: Merci.

M. Wallace est le suivant, puis ce sera le tour de M. Martin.

M. Mike Wallace: Merci, monsieur le président, et merci à vous, mesdames et messieurs les témoins, d'être venus.

J'aurais quelques questions pour m'aider à comprendre pour qui vous travaillez. J'ai ici un rapport que vous avez rédigé ensemble en 2003. C'était avec le Centre de défense pour l'intérêt public. Je vois maintenant que vous faites partie de deux organisations différentes. Travaillez-vous tous sous la même bannière?

Une voix: Ils se sont séparés.

M. Mike Wallace: Ils se sont séparés. Je vois qu'ils ont toutefois conservé la notion de droit dans leur titre.

● (1010)

Mme Philippa Lawson: C'est un peu une coïncidence. J'ai travaillé comme avocate pendant douze ans pour le Centre de défense pour l'intérêt public. La dernière chose que j'ai faite était le rapport sur le vol d'identité. Lorsque j'ai quitté en août 2003, le rapport était pratiquement, mais pas totalement, terminé. John l'a repris et l'a terminé.

En septembre 2003, après avoir quitté le Centre de défense pour l'intérêt public, je me suis jointe à la CIPPIC, la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa. Il s'agit d'organisations tout à fait distinctes.

M. Mike Wallace: Nous avons le rapport intitulé *Identity Theft: The Need for Better Consumer Protection*, qui a été terminé en 2003. Certaines des recommandations et des conclusions de ce rapport ont-elles été mises en œuvre? Le savez-vous?

M. John Lawford: Ce comité a recommandé la notification des atteintes portées à la protection des données. Je crois que c'est la principale pour l'instant. Je dois saisir mes recommandations à la base de tout cela.

M. Mike Wallace: Est-ce qu'Industrie Canada a financé cette étude ou une partie de celle-ci?

M. John Lawford: En effet, il l'a financée.

M. Mike Wallace: Il l'a financée en entier. D'accord. Mon attaché de recherche s'en est occupé pour moi et je ne savais si nous avions fait quelque chose à ce sujet ou non.

J'ai une autre question aux fins de clarification. Le groupe de consommateurs qui s'est présenté devant ce comité la dernière fois a indiqué dans son rapport qu'il n'existait aucune loi sur la protection des données aux États-Unis. Est-ce exact, ou les choses ont-elles changé depuis?

M. John Lawford: C'est exact. Toutefois, prenez par exemple la règle de la FTC que j'ai mentionnée… elle a un certain pouvoir relativement à l'exécution de la loi d'application générale sur la protection des consommateurs. En vertu de son pouvoir d'établissement de règles, elle a édicté une règle à l'égard des institutions financières qui oblige ces dernières à prendre des mesures semblables à celles de la LPRPDE en matière de sauvegarde des informations.

Mme Philippa Lawson: Puis-je ajouter quelque chose à ce sujet? Les États-Unis disposent d'un ensemble de lois sur la protection des données spécifiques à des secteurs et à des sujets donnés. Ils ne disposent pas d'une loi complète comme la nôtre. En fait, la principale recommandation des défenseurs des consommateurs et du respect de la vie privée des États-Unis est que le gouvernement adopte une loi comme la LPRPDE.

M. Mike Wallace: Madame Lawson, vous travaillez actuellement sur un projet. Est-ce exact? Qui le finance?

Mme Philippa Lawson: L'Ontario Research Network for Electronic Commerce, ou ORNEC, est un partenariat public-privé. Quatre des grandes banques du Canada le financent, à part égale avec le gouvernement de l'Ontario.

M. Mike Wallace: C'est bien.

La question qui nous préoccupe sur le vol d'identité — nous tentons d'éviter d'aborder le côté pénal de la chose. Le problème pour moi, c'est que si vous n'en entendez pas parler, que vous ne le voyez pas, vous n'en savez rien, n'est-ce pas? Nous tentons donc de nous pencher sur les questions de communication. Vous parlez de ces sites Web et ainsi de suite. Vous pourriez avoir le meilleur site Web, mais si personne ne le consulte, c'est très joli mais aussi fort inutile.

Pour faire partie d'une organisation et pour avoir travaillé dans ce domaine pendant des années, êtes-vous parvenue à quelque chose d'unique ou à quoi que ce soit qui permettrait aux gens d'être informés? Que nous recommanderiez-vous pour amener les gens à vraiment lire cette information?

Mme Philippa Lawson: Je crois qu'il faut faire appel aux médias de masse pour atteindre les gens.

Nous avons pensé à quelques moyens: utiliser les médias de masse, mettre des notes en pièces jointes avec les chèques du gouvernement, peut-être, et mettre des affiches et des dépliants efficaces dans les comptoirs publics du gouvernement, et puis travailler avec les banques. Les banques font un assez bon travail, et les agences d'évaluation du crédit aussi ont quelques bons dépliants de sensibilisation du public et autres outils sur ce sujet. Mais néanmoins, les gens continuent d'être victimes de vol d'identité.

Je crois que les banques se trouvent dans une situation délicate parce qu'elles ne veulent pas dissuader les gens d'utiliser les services bancaires en ligne. Elles voudraient donc dire que vous pouvez faire confiance à la messagerie électronique, mais elles doivent dire que vous ne pouvez pas faire confiance aux messages électroniques que vous recevez.

M. Mike Wallace: John.

M. John Lawford: Peut-être puis-je ajouter qu'on pourrait demander à l'Agence de la consommation en matière financière du Canada d'assumer ce rôle de sensibilisation du public, parce qu'elle remplit déjà cette tâche dans le système bancaire.

M. Mike Wallace: Cette semaine même, la banque avec laquelle je fais affaire, en grande partie par Internet, m'a fourni une nouvelle série de questions auxquelles j'ai mes propres réponses personnelles, et chaque fois que j'ouvre une session, on me pose une de ces questions: à quelle école secondaire j'ai étudié — je ne me rappelle pas de toutes. Il y a probablement entre 30 et 40 questions. Je dirais donc que cette banque prend la chose plutôt au sérieux.

Maintenant, en fin de semaine, j'ai reçu un courriel de mon fournisseur Internet, une entreprise de câblodistribution, m'avisant qu'il fermait mon adresse de messagerie parce que quelqu'un l'utilisait pour envoyer du pourriel. Est-ce du vol d'identité, à votre avis?

● (1015)

M. John Lawford: C'est un des problèmes de définition que j'espère que votre prochaine étude couvrira.

S'il y a fraude, par exemple si quelqu'un envoie ensuite des courriels d'hameçonnage et que cette personne peut ensuite avoir un accès à califourchon à votre compte, alors ça s'en rapproche beaucoup, mais si vous n'y perdez pas d'argent, ce n'est pas de la fraude d'identité, en tout cas. Mais je crois que cela devrait quand même être qualifié de vol d'identité.

M. Mike Wallace: Ce devrait être ma dernière question.

L'autre chose que j'ai faite —

Le président: Je suis désolé, monsieur Wallace, me voilà à converser avec notre attaché de recherche et notre greffier, et je vous ai laissé un peu plus de temps. Je dois donc vous interrompre maintenant.

Monsieur Martin.

M. Pat Martin (Winnipeg-Centre, NPD): Merci, monsieur le président.

Considérant que je n'ai pas pu me présenter plus tôt, est-il possible d'ajouter mes sept premières minutes aux cinq minutes qui me sont allouées?

Le président: Commencez avec vos cinq minutes et nous verrons par la suite.

M. Pat Martin: Merci, mesdames et messieurs. Je n'ai que deux questions assez brèves à poser, à part de vous remercier pour vos mémoires.

Le NPD craint que la nouvelle liste permanente d'électeurs puisse créer ce que nous appelons une « trousse de vol d'identité », en ce qu'elle se verra ajouter la date de naissance. Le nom, l'adresse, le numéro de téléphone et la date d'anniversaire constituent un bon paquet d'informations sur une personne, si vous avez l'intention d'utiliser ces renseignements. Elle est gratuitement distribuée. Dans une campagne électorale, vous pourriez avoir entre 200 et 300 personnes qui vont et viennent tout au long de la campagne, et si elles s'occupent des appels téléphoniques pour vous, vous déchirez une feuille de la liste d'électeurs et dites « Téléphonez à ces 50 personnes ». On la distribue donc au petit bonheur, gratuitement.

Que pensent vos organisations de l'utilisation de la date de naissance sur la liste électorale?

Mme Philippa Lawson: Nous nous y opposons, du moins dans la mesure où on la remet aux partis politiques.

Élections Canada a peut-être de bonnes raisons de recueillir cette information pour ses propres fins internes, de la conserver en sécurité et de veiller à ce qu'elle ne soit utilisée à aucune autre fin. Mais il n'y a absolument aucune raison, selon nous, pour que la date de naissance soit inscrite sur la liste fournie aux partis politiques, et ce ne devrait pas être le cas. Cela va totalement à l'encontre des principes du droit sur la protection des données et des pratiques équitables en matière d'information reconnues dans le monde entier.

M. Pat Martin: Avez-vous entendu cela, Mike?

M. Mike Wallace: Je ne sais pas si la liste contient les numéros de téléphone. Je ne le crois pas.

M. Pat Martin: Bien entendu, qu'ils y figurent.

Quoi, nous les avons mis sur la liste.

M. Mike Wallace: Bien, oui, vous pouvez le voir.

Vous vous immiscez dans la vie privée des gens, monsieur Martin.

Le président: Notre approche est très collégiale aujourd'hui, mais peut-être pourriez-vous passer à votre prochaine question.

M. Pat Martin: Vous avez raison.

La prochaine question est également brève.

Je remarque que vous mentionnez l'obligation de notification comme un impératif dans votre mémoire. Nous avons amplement traité de cette question lors de la révision de la LPRPDE, et le secteur privé a grincé des dents et s'est arraché les cheveux parce qu'il y voyait un inconvénient écrasant. C'était intenable. Nous ne pouvions tout simplement pas en informer les gens, juste parce que nous avions commis une bourde et perdu leurs informations ou que nous les avions jetées aux ordures, ou que sais-je encore. Ce serait incroyable. Nous avons donc fini par émettre une vague recommandation sur l'obligation de notification, sans grande force.

Jusqu'où iriez-vous? Je remarque que vous dites qu'il faudrait aviser les gens en cas d'atteinte, ou même de possibilité d'atteinte.

M. John Lawford: Cette recommandation tient en ce que s'il y a eu atteinte et que vous avez récupéré votre lecteur de disque dur, ou s'il y a eu une tentative de piratage mais que vous n'êtes pas certain de ce qui est arrivé avec les données, vous devriez en aviser les gens. Nous n'avons pas changé d'idée à ce sujet, parce qu'on ne sait jamais, l'information circule tellement vite, elle pourrait se retrouver n'importe où.

M. Pat Martin: Vous dites donc qu'il faudrait aviser tout le monde, pas seulement l'agence d'évaluation du crédit ou les services de police, mais aussi les clients?

M. John Lawford: Oui, aviser les clients, parce que ceux-ci pourraient prendre des mesures immédiates auprès de leur banque pour bloquer l'octroi de crédit et éviter que leur compte se fasse vider. On pourrait mettre une alerte de fraude dans leur rapport de solvabilité, nous préférerions une limitation de crédit, mais bon. Ils pourraient prendre beaucoup de mesures, comme d'aller directement à la police dès qu'ils voient quelque chose d'anormal, plutôt que de dire « Tiens, c'est bizarre », et attendre pendant des jours que le problème prenne de l'ampleur.

M. Pat Martin: Madame Lawson.

Mme Philippa Lawson: Il y a deux fonctions, à notre avis, à la notification des atteintes à la sécurité. L'une est de donner aux gens la capacité de prendre des précautions si la situation le leur permet. Mais la deuxième raison, aussi importante, si ce n'est plus, est de fournir aux organisations ces mesures incitatives dont je parle depuis le début pour qu'elles prennent des mesures de sécurité au préalable afin de prévenir les atteintes à la sécurité dès le départ. L'incitatif, dans ce cas-ci, c'est que les médias en seraient informés et que les organisations verraient leur réputation entachée.

C'est pourquoi j'ai certaines réticences envers un régime qui exigerait que les organisations se rapportent uniquement au Commissaire à la protection de la vie privée mais n'obligerait pas forcément à ce que l'atteinte soit rendue publique. Si vous voulez mettre cet incitatif en place, l'information doit être rendue publique pour que les médias puissent décider si elle mérite d'être signalée et dans l'affirmative, de la divulguer.

● (1020)

M. Pat Martin: Je suis d'accord. De plus, je mentionnerais la pression exercée par le client, parce que même si je ne subis pas de pertes financières, si mes informations personnelles ont été compromises deux ou trois fois par la même entreprise, je ne ferais plus affaire avec elle. Je transférerais mes comptes chez ce groupe qui travaille un peu plus fort pour que mes informations soient en sécurité. Alors, cette mesure est très bien —

Mme Philippa Lawson: Absolument. Je dirais que ça complète les forces du marché, dans ce sens.

M. Pat Martin: Merci, monsieur le président.

Le président: Merci, monsieur Martin.

Quelqu'un d'autre? D'accord, je prendrai la relève.

Madame Lawson, vous avez dit qu'à votre avis, l'Agence de la consommation en matière financière du Canada, je le dis dans mes mots, devrait être mandatée pour lancer une campagne de sensibilisation massive. Cela s'inscrit en quelque sorte dans la même ligne de pensée que celle de M. Stanton.

D'abord et avant tout, peut-être pourriez-vous nous parler un peu de l'Agence de la consommation en matière financière du Canada, ce qu'elle est, qui la dirige, à qui elle rend des comptes. Nous avons entendu le groupe d'Industrie Canada la semaine dernière, le Comité des mesures en matière de consommation, qui semble avoir une bonne relation de travail avec ses équivalents provinciaux et territoriaux, parce que bien entendu il s'agit d'une situation intergouvernementale, un point que nous n'avons vraiment pas abordé avec vous. Si nous les avons déjà, et je crois vous avoir entendu dire qu'ils faisaient du bon travail, pourquoi faudrait-il que l'Agence de la consommation en matière financière du Canada intervienne?

Donc, deux questions. Qu'est-ce que l'Agence de la consommation en matière financière du Canada et pourquoi lui demander d'intervenir si le CMC fait du bon travail?

Mme Philippa Lawson: Je laisserai M. Lawford poursuivre parce que je crois qu'il a plus travaillé avec l'ACFC.

Il s'agit d'un organisme national responsable, d'après ce que je comprends, de la réglementation des banques sur la question de la protection des consommateurs. Ce qui est bien avec l'ACFC, c'est son aspect national. Elle n'englobe pas toutes les institutions financières, seulement les banques sous réglementation fédérale, mais elle a une couverture nationale, ce dont nous avons besoin.

Le Comité des mesures en matière de consommation fournit de bonnes informations sur son site Web. Il encourage les provinces à en faire autant. Certaines provinces ont fait de grands pas dans ce domaine, mais si on résume la chose, le CMC coordonne les mesures provinciales, alors les citoyens des provinces qui choisissent de ne pas prendre ces mesures sont perdants.

Du moins en ce qui concerne la responsabilité fédérale, je crois qu'il serait logique de recourir à une agence fédérale pour offrir aux consommateurs davantage de solutions d'achat polyvalentes.

Je laisse la parole à John.

M. John Lawford: L'Agence de la consommation en matière financière du Canada a pris quelques mesures expérimentales à ce sujet. Je crois qu'elle travaille sur les documents d'hameçonnage, il serait donc tout naturel qu'elle continue dans cette voie. Que cela plaise aux banques ou non, elles se trouvent au centre de cet enjeu, parce qu'inévitablement, le vol d'identité leur est rapporté.

L'Agence de la consommation en matière financière du Canada a pour mandat de sensibiliser le public sur des questions de prudence financière et de sécurité, et bien qu'elle fasse uniquement affaire avec les institutions financières fédérales, comme je l'ai dit, elle représente un carrefour dans ce domaine. C'est donc un organisme vers lequel on pourrait se tourner au sein du gouvernement fédéral, et c'est un choix logique, parce que le Commissaire à la protection de la vie privée ne semble pas intéressé à s'en occuper, ni le Bureau de la concurrence, d'ailleurs.

Le président: Est-ce une agence créée par les banques, une agence créée par le gouvernement du Canada, une coopérative, ou autre?

M. John Lawford: C'est un organisme indépendant, créé en vertu d'une loi, qui rend compte au Parlement chaque année. Mais il est financé par les établissements financiers plutôt que par les contribuables.

Le président: Le CMC, en passant, publie des brochures et autres articles fort intéressants.

Monsieur Lawford, vous avez mentionné la Federal Trade Commission des États-Unis, et le sujet est revenu à quelques reprises. Quels sont les pouvoirs législatifs de cette commission? On nous a dit qu'il existe une gamme de lois sur la protection des consommateurs dans chacun des cinquante États américains; certains en ont plus que d'autres, certaines lois sont plus strictes, d'autres plus faibles, et certains État n'en ont peut-être aucune. Je n'en sais rien.

Monsieur Lawford, si j'ai bien compris, vous recommandez que ces lois nous servent de modèle, et j'essaye simplement de comprendre quels sont les pouvoirs de cette commission aux États-Unis.

● (1025)

M. John Lawford: La mesure de protection dont je vous ai parlé découle de la Gramm-Leach-Bliley Act, qui oblige les institutions financières américaines à prendre des précautions pour préserver le caractère confidentiel des renseignements financiers personnels de leurs clients. C'est le fondement des pouvoirs de la commission, dans ce cas en particulier. Aux termes de la Federal Trade Commission Act, il est du ressort de cette commission de veiller à la protection des consommateurs. Je pense que c'est prévu à l'article 5. La commission utilise donc ces deux lois.

Je sais qu'il y a eu des poursuites intentées en vertu de l'article 5 concernant les pouvoirs des entreprises suite à une atteinte à la sécurité.

Le président: À vous, madame Lawson.

Mme Philippa Lawson: La FTC exerce une compétence plus vaste que notre Bureau de la concurrence en matière de protection des consommateurs. À mon avis, c'est là une des plus grandes failles du régime fédéral, le fait que le Bureau de la concurrence n'a pas la perception d'avoir le mandat de protéger les consommateurs.

Le président: Merci beaucoup.

Nous passons à M. Tilson. La seule autre personne sur ma liste est M. Van Kesteren. Si quelqu'un d'autre aimerait poser des questions, veuillez s'il vous plaît le faire savoir au greffier. Autrement, nous entendrons M. Tilson et puis M. Van Kesteren seulement.

M. David Tilson (Dufferin—Caledon, PCC): Merci.

Comme vous le savez, quand nous avons examiné la LPRPDE, la question de la notification a été soulevée à plusieurs reprises. Nous avons débattu entre nous et nous avons écouté des témoignages. C'était suite à des fuites de renseignements bancaires — soit qu'on pensait qu'il y avait eu fuite et que cela s'est avéré faux, soit que les données avaient quitté l'établissement pour se retrouver dans une décharge en quelque part aux États-Unis. Je pense que Winners a été cité en exemple. Différents témoins nous ont donné l'impression que ces sources d'information ne voulaient pas que le public sache que ces choses-là se passent, et qu'ils allaient prendre la situation en mains.

Les sociétés de cartes de crédit elles-mêmes, monsieur Lawford, vont vous dédommager si quelqu'un fait une transaction avec votre carte de crédit et si vous pouvez prouver que ce n'est pas vous qui avez fait l'achat. C'est probablement ce qui justifie leurs frais d'intérêts de 24 p. 100 ou quelque. L'impression qui se dégage de la plupart des témoignages que nous avons entendus est que ces groupes — soit les banques, les sociétés de cartes de crédit, les détaillants eux-mêmes, ou les avocats — ne veulent pas que les gens sachent que l'information est sortie, ou encore qu'ils ont été victimes de fraude. Les comptables ne veulent pas savoir cela — cela nuit à leur image — alors ils vont faire tout ce qu'ils peuvent.

Est-ce que toute la situation serait exagérée à outrance? C'est la question que je me pose.

M. John Lawford: C'est-à-dire que les commerces, tout comme les banques et les sociétés de cartes de crédit, font des efforts pour faire cesser le vol d'identité, cela ne fait aucun doute. D'autre part, comme vous l'avez dit, ils n'ont certainement pas intérêt à faire savoir au public que la sécurité a été compromise.

Serait-il acceptable de ne rien faire du tout? Non, nous ne le pensons pas, parce que les renseignements perdus peuvent maintenant servir à plusieurs fins, par exemple constituer un nouveau crédit ou frauder par d'autres moyens des personnes qui ne reçoivent aucune compensation. Les sociétés de cartes de crédit vous protègent de vos pertes moyennant une déduction de 50 $ aux États-Unis et parfois entièrement ici au Canada, mais ce n'est pas le cas lorsque quelqu'un utilise vos renseignements personnels pour prendre une hypothèque sur votre maison. Nous avons dû adopter une loi en Ontario à cet effet; il y a des personnes qui ont carrément perdu leur maison au profit de fraudeurs. C'est un exemple effrayant.

Nous n'en connaissons tout simplement pas les effets ultérieurs. La banque se chargera peut-être des conséquences immédiates, mais il pourrait y avoir d'autres effets pour lesquels les consommateurs n'auront aucun recours. C'est ce qui nous préoccupe.

M. David Tilson: En ce qui concerne la fraude hypothécaire, il y a eu une affaire devant tribunal aussi, je pense. J'ignore quelle cour l'a entendue, mais quelqu'un a dit aux banques, au créancier hypothécaire, ou je ne sais trop : « C'est votre problème. »

Ensuite vous commencez à vous poser la question. Votre exposé était bien intéressant, mais avec toute cette information, avec tout le monde qui reçoit cette information — le nom de jeune fille de votre mère, votre date de naissance et tout le reste — le jour où vous êtes victime de fraude, même si c'est vous qui avez donné ces renseignements, est-ce qu'il revient à eux de prouver — devraient-ils assumer la perte? Je fais une comparaison avec la situation du créancier hypothécaire. C'est peut-être impossible dans bien des cas, particulièrement si un voleur a puisé dans votre compte de banque, je suppose, mais généralement pourquoi le consommateur devrait-il souffrir, en particulier lorsqu'on l'oblige à fournir toute cette information aux différents intervenants?

● (1030)

Mme Philippa Lawson: C'est précisément pourquoi nous recommandons de rendre la vie plus facile aux consommateurs qui, par exemple, intentent des recours collectifs contre des entreprises qui ont été si négligentes que de grands nombres de consommateurs ont souffert. Il nous faut absolument prendre des mesures législatives pour faire en sorte que les organisations négligentes soient tenues responsables. Je ne pense pas que les démarches actuelles soient suffisantes.

M. David Tilson: Vous avez mentionné la possibilité que des vérificateurs visitent les entreprises pour faire des vérifications. Est-ce une intrusion excessive?

M. John Lawford: La Commissaire à la protection de la vie privée du Canada détient ce pouvoir en ce moment. Je suppose que le Parlement ne trouvait pas qu'il y avait intrusion lorsqu'il l'a mis en place. Elle est toutefois obligée d'avoir des motifs raisonnables de l'appliquer.

Je pense que quand une organisation a fait les manchettes deux, trois ou quatre fois, cela pourrait constituer un motif raisonnable. Il est certain que si nous compilons des statistiques ou si d'autres indicateurs objectifs et factuels laissent deviner une source d'inquiétude par rapport à un certain détaillant ou établissement financier, ou par rapport à un récidiviste, si vous me permettez l'expression, une vérification pourrait être utile si le problème est chronique.

M. David Tilson: Je sais que nous voulons éviter de parler du Code criminel, mais vous êtes tous les deux avocats.

Vous avez été silencieux jusqu'à présent; il serait intéressant d'entendre votre point de vue.

Pourriez-vous me dire ce que vous pensez des amendes? L'un ou l'autre?

Mme Philippa Lawson: Tout ce que je peux dire, c'est que nos recherches indiquent que les peines ne sont pas suffisamment élevées, et qu'elles ne sont que des dépenses de roulement pour les criminels.

M. David Tilson: Avez-vous des points à ajouter? Pourriez-vous faire une recommandation?

Mme Philippa Lawson: Nous avons publié un document de travail sur la jurisprudence, qui couvre je pense autant les affaires pertinentes en droit criminel que celles en droit civil. Je ne l'ai pas en ma possession en ce moment, donc je ne pourrais pas vous donner de détails. Nous allons en publier un autre sur l'application des lois criminelles ayant une incidence sur le vol d'identité.

Je peux simplement vous dire que selon notre conclusion, il est très clair et c'est un des problèmes auxquels se heurtent les policiers — et j'espère que vous allez entendre ce qu'ils ont à dire sur le sujet : à quoi bon dépenser des centaines de milliers de dollars et des heures de temps à enquêter sur ces crimes de col blanc souvent très complexes alors qu'en bout de ligne, on finit par trouver le coupable, l'enquête est bouclée avec succès et le tribunal n'impose qu'une sentence de quelques mois ou une amende qui revient en fait à la rançon des affaires?

Le président: On a peut-être l'impression de ne pas porter attention aux aspects criminels du sujet, mais à ma connaissance, le comité n'a pas encore pris de décision à cet effet, et en fait nous allons entendre un porte-parole du ministère de la Justice. Dans le cadre de nos délibérations, nous pourrons décider ou non de laisser tomber les aspects criminels, après que nous aurons entendu tous les témoignages. Je ne voudrais surtout pas que les gens pensent que nous avons déterminé à l'avance que notre examen ne portera pas sur les aspects criminels. Il se peut que nous prenions une décision en ce sens, mais rien n'a encore été arrêté.

Il me reste deux personnes: M. Van Kesteren et Mme Lavallée.

Monsieur Van Kesteren.

M. Dave Van Kesteren: Merci, monsieur le président.

J'ai quelques courtes questions seulement. Je voudrais revenir sur ce dont parlait M. Martin.

La raison que l'on a invoquée pour justifier l'hésitation à déclarer les intrusions et le type de législation ou de politique à adopter, ou du moins la principale raison du point de vue des témoins que j'ai entendus, était qu'une fois que nous commencerons à le faire, l'apathie des consommateurs s'accentuera et cela engendrera une perte d'intérêt. Jour après jour on se rendra compte que « Il y a eu une autre fraude chez Zellers et une autre à une telle banque », et l'on finira par ne plus y porter attention.

Qu'en dites-vous?

M. John Lawford: Il y a certainement le risque que le public se lasse. Cependant, je pense que ce que nous avons recommandé à la Commissaire à la protection de la vie privée à cet effet, c'est qu'il y ait une description dans la notification qui nous indique le degré de sérieux de la situation. Donc, il est à espérer qu'un certain nombre de ces avis ne seraient pas de nature sérieuse et indiqueraient essentiellement « Nous ne pensons pas que cela soit très grave » et que d'autres laisseraient entendre « Oui, c'est très sérieux, et vous devriez peut-être réagir ». C'est une façon d'aborder la question.

Une autre solution, que nous leur avons proposée, c'est la possibilité de compiler un registre des fuites. Les gens pourraient consulter le registre à la fin de l'année et dire, « Oh, on m'a réellement volé mon identité, regarde, ma compagnie est inscrite au registre trois fois », mais ne pas nécessairement recevoir d'avis, à moins que la commissaire à la protection de la vie privée, comme l'a recommandé le comité, juge la situation suffisamment grave pour recommander la diffusion d'un avis.

Ce sont deux solutions possibles. Autrement, je pense que ce qui nous préoccupe, c'est que si un si grand nombre d'avis sont diffusés, cela donne l'impression que nous sommes en présence d'un grave problème.

● (1035)

M. Dave Van Kesteren: Non, je ne suis pas d'accord.

Si nous rendons les compagnies responsables de par la loi... elles vont protéger leurs arrières, honnêtement, et pour n'importe quelle raison, elles vont commencer à — Je me demande comment nous pouvons éviter cela —

Mme Philippa Lawson: Excusez-moi. Nous avons en place aujourd'hui une loi selon laquelle les compagnies sont responsables. Le problème est que cette loi est insuffisante.

M. Dave Van Kesteren: Si nous lui donnons du mordant — À ce stade-ci, s'ils ne diffusent pas d'avis d'intrusion, ils sont responsables. Je peux vous assurer que nous allons être inondés de —

Mme Philippa Lawson: Si vous êtes sérieux dans votre analyse, je vous recommanderais de songer à inviter certains témoins ou à entendre des gens de la Californie, où l'on a mis en place une loi prescrivant la déclaration des infractions à la sécurité des données il y a au moins trois ans. Ils en ont fait l'expérience. J'ai entendu dire que les consommateurs se lassent de recevoir des avis.

Je pense que nous avons besoin, et moi-même j'aimerais voir, de bonnes études objectives sur la question. Malheureusement, il existe des études qui manquent nettement d'objectivité. Javelin Research, par exemple, a été embauchée pour réaliser des sondages et des rapports par des entreprises qui sont opposées à la déclaration des atteintes à la sécurité, et les rapports qu'elle a publiés sont de toute évidence biaisés.

Obtenir un rapport vraiment neutre et sans parti pris sur les résultats, sur le succès d'une méthode de communication des atteintes à la sécurité des données, dépend en grande partie des seuils que vous établissez en vue de la notification. Bien entendu, plus le seuil est élevé, moins on aura besoin de communiquer les fuites. Il y a différents moyens de le faire, comme vous le proposez dans votre rapport, et comme le dit John en ce moment, qui pourraient inclure un registre public, la commissaire à la protection de la vie privée servant de filtre en quelque sorte, et une vérification de la nécessité d'une notification dans une circonstance donnée.

M. Dave Van Kesteren: Pour revenir très rapidement sur la responsabilité des consommateurs, je ne lis nulle part et je me demande pourquoi — Pourquoi ne pas afficher des avertissements, comme cela se fait sur les paquets de cigarettes? Il s'agirait simplement de les faire paraître à l'écran, du genre : voici ce qui pourrait vous arriver? Est-ce possible? Est-ce une idée que vous —?

M. John Lawford: La question pourrait se poser entre autres pour les transactions bancaires électroniques, que vous pourriez qualifier d'activités à risque. J'ignore si le public viendrait à se lasser ou non de ces avertissements. Mais une de mes inquiétudes, c'est que les consommateurs acceptent des courriels, et quand ces messages proviennent d'un établissement financier présumé, comme l'a dit Philippa, les consommateurs ne savent pas que dans 99 p. 100 des cas, ce sont des messages frauduleux. Peut-être qu'ils devraient recevoir par la poste une fois par année, un envoi de leur banque leur disant de ne pas répondre quand ils reçoivent un courriel d'une personne qui cherche à connaître des détails de leur compte. Je ne sais pas si cela se fait ou non.

Pensez-vous à d'autres formes d'avertissements?

Mme Philippa Lawson: Je pense que le problème est que les banques et d'autres entreprises ne sont pas disposées à publier ce genre d'avis parce qu'elles ne veulent pas décourager les gens d'utiliser le commerce électronique.

M. Dave Van Kesteren: Mais si nous en faisions une obligation lorsqu'on accepte de l'argent sur Internet, quand les institutions le font, elles sont obligées de dire que ce genre de transaction comporte des risques. Cela aiderait à sensibiliser les consommateurs.

Mme Philippa Lawson: Je vois deux problèmes. Le premier, c'est que le fraudeur ne va pas faire ce genre d'avertissement. J'essaye d'imaginer comment cela pourrait se produire dans la pratique. Ce qui se passe, c'est que les gens ne transigent pas avec des organismes légitimes. Ils pensent que c'est le cas, mais ils ont affaire à des fraudeurs. Alors, comment est-ce que l'avertissement va les rejoindre au moment où c'est vraiment nécessaire? Je me demande comment cela pourrait fonctionner.

Deuxièmement, comme je l'ai déjà signalé, même si vous étiez en mesure d'alerter les clients — en réalité, si l'on pouvait empêcher tous les clients de tomber dans tous les pièges informatiques imaginables, cela ne réglerait qu'une fraction du problème. Nous avons l'impression, mais sans données statistiques à l'appui, que le problème se situe principalement au niveau des fuites d'entreprises, du piratage de bases de données et des vols par l'intérieur, par exemple, sur lesquels les consommateurs n'ont absolument aucun pouvoir.

Le président: Merci.

Mme Lavallée, puis une intervention de M. Wallace.

Monsieur Reid, un rappel au Règlement.

● (1040)

M. Scott Reid (Lanark—Frontenac—Lennox and Addington, PCC): Merci, monsieur le président.

Mes excuses à Mme Lavallée et à nos témoins de cette intrusion, mais je crains que nous allons manquer de temps pour terminer la séance.

Je crois comprendre que le sous-comité chargé d'examiner l'ordre du jour du comité a pris des dispositions afin de traiter de la motion soumise au comité et mise aux voix en ce qui concerne l'Afghanistan et ainsi de suite. Je suppose que cela implique la convocation de témoins dès jeudi, et je crains que nous n'ayons pas la chance d'en discuter avant. Cela poserait évidemment un problème pour l'obtention d'un consensus au comité quand aux personnes que nous allons convoquer.

J'espère que nous allons tous trouver le moyen de nous accorder assez de temps pour régler cela aujourd'hui.

Le président: Merci d'avoir soulevé le point. Je suis persuadé que nous n'allons pas épuiser le temps prévu, donc laissez-moi m'en charger. Ce n'est pas un rappel au Règlement, mais une question légitime. J'allais m'en occuper d'ailleurs.

Tout d'abord, c'est le comité qui décide de ce qu'il va faire, non pas le comité de direction. Le comité de direction formule des recommandations. Le comité de direction s'est effectivement réuni, et il a élaboré des recommandations, que nous allons faire circuler.

Le premier point à l'ordre du jour jeudi sera le rapport du comité de direction. Il reviendra au comité de décider s'il veut adopter ce rapport, dans sa forme présentée ou dans une forme modifiée.

Si jamais le comité décide d'adopter ce rapport du comité de direction, tel quel ou avec modifications, nous avons un témoin qui a confirmé sa présence — un seul jusqu'à maintenant — pour jeudi. M. Jeff Esau est un journaliste pigiste dont le reportage a été publié dans le *Globe and Mail*. Il a présenté deux demandes d'accès à l'information sur la question.

Bien entendu, il sera présent afin que nous ne perdions pas de temps. Si nous passons toute la réunion à discuter du rapport du comité de direction, qu'il en soit ainsi. Ce sera la décision du comité. Mais le témoin sera ici au cas où la décision se prend assez rapidement. Si nous n'avons pas le temps de l'entendre, il sera accessible une fois que le comité aura pris une décision finale.

À l'heure actuelle, la décision du comité est d'aller de l'avant en ce qui concerne le vol d'identité. Mais comme on a insisté sur le caractère pressant de cet examen, j'inscris le rapport du comité de direction au premier point à l'ordre du jour de jeudi matin à 9 heures.

Est-ce que cela répond à votre question?

M. Scott Reid: Oui, monsieur le président.

Le président: Merci.

Mme Lavallée, ensuite M. Wallace.

[*Français*]

Mme Carole Lavallée: Je n'ai pas nécessairement de questions. Je voulais parler de la liste d'invités éventuels pour discuter du vol d'identité. Je me demandais à quel moment il serait préférable de le faire.

[*Traduction*]

Le président: Pas maintenant. Nous avons nos témoins ici.

Vous pourriez transmettre vos suggestions à notre greffier. Il pourra discuter à savoir s'ils figurent déjà sur la longue liste de témoins. S'ils n'y sont pas, nous pourrons en discuter entre nous. Vous n'avez qu'à remettre la liste au greffier.

[*Français*]

Mme Carole Lavallée: Parfait.

[*Traduction*]

Le président: C'est bien. Avez-vous des questions?

[*Français*]

Mme Carole Lavallée: Oui. Nous avons commencé plus tôt à parler des lois qu'il fallait changer, et vous n'avez pas été suffisamment clairs, en ce qui me concerne, quant à savoir quelles sont les lois fédérales que l'on peut changer. Au cours des discussions, vous avez ajouté qu'il fallait exiger que les magasins soient plus vigilants dans le dépistage des fraudeurs. Vous avez parlé de faciliter les recours collectifs. Au Québec, on a tout ce qu'il faut pour intenter des recours collectifs; je ne sais pas comment ça se passe dans les autres provinces. Vous avez aussi parlé des lois provinciales.

Le vol d'identité, selon vous, relève-t-il d'une compétence fédérale, ou provinciale?

Mme Philippa Lawson: Les deux, fédérale et provinciale.

[*Traduction*]

En ce qui concerne les recours collectifs, nous recommandons des amendements à la LPRPDE. Si vous prenez les recommandations 1 à 7 de notre présentation du 28 novembre concernant la refonte de la LPRPDE, vous allez voir que nous disons que les provinces, en particulier le Québec, ont en place un régime très efficace de recours collectif. Le problème est que les plaignants aux termes de la LPRPDE n'ont aucun moyen de déposer ces plaintes sous forme de recours collectif au Québec à l'heure actuelle. Vous devez modifier la LPRPDE de manière à leur permettre de déposer leurs plaintes dans le cadre d'un recours collectif.

[*Français*]

Mme Carole Lavallée: Non, parce qu'au Québec, il y a une autre loi sur la protection des renseignements personnels, une loi qui relève du gouvernement du Québec. Les recours collectifs fonctionnent bien à l'intérieur de ce système, alors on n'a pas besoin, dans la LPRPDE —

● (1045)

Mme Philippa Lawson: Mais, si les problèmes surviennent avec une banque qui est régie —

Mme Carole Lavallée: Oui.

[*Traduction*]

Mme Philippa Lawson: Si l'institution est assujettie à la réglementation fédérale, l'affaire tombe sous le coup de la LPRPDE, par opposition à la loi du Québec.

[*Français*]

Mme Carole Lavallée: Ça mérite d'être vérifié, mais je pense qu'il y a même eu des recours collectifs au Québec contre le gouvernement fédéral. Alors, je pense que le système ou le programme de recours collectif n'a rien à voir avec la personne que l'on poursuit. Je ne suis pas avocate, mais je vous fais part de ce que j'ai vu et entendu.

Non seulement vous avez besoin d'un traducteur, mais aussi d'un interprète.

M. John Lawford: L'amendement suggéré vise à faire en sorte qu'il soit absolument clair qu'on peut poursuivre une telle action, un tel processus au Québec, selon vos règles.

[*Traduction*]

Mme Philippa Lawson: Si je peux me permettre d'ajouter un point, il est possible que dans la majorité des cas au Québec, les consommateurs disposent des mécanismes de recours dont ils ont besoin à l'échelon provincial. Ce n'est pas le cas de toutes les autres provinces. Nous avons encore besoin de corriger la loi fédérale pour le reste du Canada, même si les consommateurs du Québec bénéficient d'une protection suffisante.

[*Français*]

Mme Carole Lavallée: La semaine dernière, un des témoins — je crois que c'était l'avocate de la commissaire à la protection de la vie privée — nous a dit, en ce qui concerne le vol d'identité, que ce n'était pas un crime que de voler l'identité de quelqu'un, mais que c'était un crime que de se servir des informations obtenues.

Peut-on faire quelque chose pour légiférer afin que le vol d'identité devienne un crime?

[*Traduction*]

Mme Philippa Lawson: Cette modification au Code criminel est recommandée par un grand nombre de personnes. En effet, à l'heure actuelle, le fait de recueillir et de posséder des renseignements sur les cartes de crédit sans excuse légitime est une infraction au Code criminel. Je crois que c'est également possible dans d'autres situations.

D'après les organismes d'application de la loi, il est parfois possible de prendre une personne qui détient de vastes quantités de données non liées aux cartes de crédit et d'autres informations et documents de nature personnelle, comme des numéros d'assurance sociale, des noms, des adresses, que la personne avait clairement l'intention d'utiliser à des fins de fraude d'identité. Toutefois, comme la possession de ce type de renseignement sans excuse légale ne constitue pas une infraction particulière au Code criminel, il est impossible de porter des accusations.

Il s'agit de l'une des modifications au Code criminel que considère actuellement le ministère de la Justice; nous étudions également la question.

Par contre, je crois qu'il faut faire preuve d'une grande prudence avant de créer tout simplement de nouvelles infractions. Il existe bien des situations où des gens détiennent en toute légitimité des renseignements sur d'autres. Pour qu'il y ait infraction, l'intention criminelle est nécessaire. Il est toutefois clair pour l'instant que dans la plupart des cas, la cueillette non autorisée d'information n'est pas un acte criminel.

Le président: Merci, madame.

Madame Lavallée, lorsque vous parlez de témoins possibles avec M. Rumas, vous pensez peut-être au Barreau du Québec ou à une autre personne morale du Québec. Il ou elle pourrait venir préciser pour nous la situation concernant les recours collectifs, la façon de les enclencher au Québec et les règles actuelles.

Il y a lieu d'espérer que cela vous apporterait des éclaircissements sur un témoin particulier possédant de l'expérience en matière de droit québécois. D'accord?

[*Français*]

Mme Carole Lavallée: Parfait.

[*Traduction*]

Le président: Notre dernier intervenant est M. Wallace.

Monsieur Hecht, c'est votre dernière chance de faire enregistrer vos propos. Ensuite, ce sera terminé en ce qui vous concerne.

Monsieur Wallace.

M. Mike Wallace: Excusez-moi, monsieur Hecht. Cette question ne vous est pas vraiment adressée, mais vous êtes libre d'y répondre si vous le voulez.

Je veux être certain de bien comprendre. De ceci, nous tirerons un rapport sur les recommandations.

Madame Lawson, vous avez dit qu'un groupe de travail serait prioritaire sur votre liste. Nous avons produit le rapport en 2003, et c'est l'industrie qui a réglé la note. Combien cette étude a-t-elle coûté? En avez-vous la moindre idée? Est-il question de centaines de milliers de dollars ou plutôt de 50 000 $?

● (1050)

Mme Philippa Lawson: Je ne me souviens pas du montant. C'était entre 25 000 $ et 40 000 $.

M. Mike Wallace: D'accord. Le montant était inférieur à 100 000 $.

Le rapport a été achevé en 2003, et les recommandations et conclusions qu'il contenait n'ont pas eu vraiment de répercussions. Qu'en dites-vous?

Mme Philippa Lawson: Les travaux réalisés par le Comité des mesures en matière de consommation depuis que ce rapport a été produit sont en harmonie avec nos recommandations, comme celle de créer un affidavit normalisé pour les victimes.

M. Mike Wallace: C'est une question de rentabilité. Est-ce qu'un autre groupe de travail fera quoi que ce soit de différent par rapport au contenu du rapport de 2003?

Le président: Madame Lawson, c'est ma faute: j'ai laissé la rencontre se poursuivre. Par contre il est inutile d'appuyer sur ce bouton. Nous avons quelqu'un pour le faire.

M. Mike Wallace: Oh! Je croyais peut-être avoir posé la mauvaise question.

Le président: En réalité, c'est ma faute. Ne touchez pas au bouton. Elle s'en occupe toujours pour nous. Je n'aurais pas dû le laisser avant la dernière heure dont nous disposons.

Excusez-moi, monsieur Wallace.

Mme Philippa Lawson: La recommandation, pour ce qui est du groupe de travail, vise à réunir tous les éléments dans un même groupe afin qu'ils soient tous réglés. Je crois qu'il existe clairement un certain nombre d'initiatives et de modifications législatives et de réformes stratégiques qui sont possibles.

On m'a demandé ce qui serait le plus important. La création d'un bureau national d'aide aux victimes d'usurpation d'identité serait incroyablement utile, non seulement pour venir en aide aux victimes, mais aussi pour recueillir des statistiques et mieux comprendre le problème.

M. Mike Wallace: J'essaie seulement de bien comprendre; un groupe de travail n'est pas un organisme bénévole. L'industrie ou quelqu'un d'autre devra acquitter la facture d'une telle étude.

Mme Philippa Lawson: Je parle d'un exercice semblable à ce qu'a fait le groupe de travail sur le pourriel.

M. Mike Wallace: D'accord. Merci beaucoup.

Mme Philippa Lawson: Industrie Canada a encadré le processus et y a mis un grand effort.

M. Mike Wallace: Je voulais simplement que les choses soient claires, pour bien comprendre. Merci.

Le président: Excusez-moi, c'est un bureau national —

Mme Philippa Lawson: Il s'agirait d'un bureau national d'aide aux victimes d'usurpation d'identité.

Le président: — d'aide aux victimes d'usurpation d'identité.

Nous aurons une brève question pour M. Tilson.

M. David Tilson: Par hasard, vous avez mentionné la question que j'allais poser. En vous fondant sur le document que vous avez préparé en 2003, pouvez-vous expliquer brièvement votre concept de l'affidavit normalisé pour l'usurpation d'identité? C'est à la page 52 de votre rapport.

Mme Philippa Lawson: Oui. Il s'agit de faciliter les choses pour les victimes. À l'heure actuelle, les victimes doivent composer avec de nombreuses institutions différentes, chacune ayant ses propres formules et exigences concernant l'authentification et la preuve qu'il y a bel et bien eu utilisation frauduleuse des renseignements. Tout cela représente un incroyable cauchemar et une énorme tâche pour les pauvres victimes.

M. David Tilson: Quel est le rôle d'un affidavit? On pourrait utiliser un affidavit frauduleux.

Mme Philippa Lawson: Oui, cela fait partie du problème. Ils sont traités comme des suspects.

M. David Tilson: Je voulais seulement comprendre le fonctionnement de cette formule. Si vous vous donnez la peine de frauder, un affidavit frauduleux est du gâteau.

Mme Philippa Lawson: Oui, mais il s'agit également de faciliter le processus pour les victimes. Il existe des moyens de le faire.

M. David Tilson: Merci.

Le président: D'accord. Merci beaucoup.

Je tiens à remercier nos témoins pour leur expertise ainsi que leurs points de vue et leurs recommandations. Nous attendrons avec impatience que M. Lawfield, je crois, nous revienne au sujet de la Federal Trade Commission, s'il le peut.

Nous reprendrons donc nos travaux jeudi à 9 heures. Nous nous pencherons alors sur le premier rapport du sous-comité du programme et de la procédure. La séance est levée.

M. Mike Wallace: Qui ajourne la séance?

The Chair: C'est moi.

Je suis désolé, monsieur Martin, aviez-vous levé la main? Je ne vous avais pas vu.

M. Pat Martin: Vous venez d'annoncer que jeudi, nous nous pencherons sur les recommandations du sous-comité au comité principal.

Le président: Effectivement. C'est le premier point à l'ordre du jour. Il est en outre confirmé que M. Jeff Esau viendra témoigner si le comité décide de se réunir.

La séance est levée.