CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 024 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 27 mai 2014

Président

M. Pat Martin

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

Le mardi 27 mai 2014

● (1105)

[*Traduction*]

Le président (M. Pat Martin (Winnipeg-Centre, NPD)): Bonjour, mesdames et messieurs.

La réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique est ouverte. Aujourd'hui, nous poursuivons notre étude du problème grandissant du vol d'identité et de ses répercussions économiques.

Nous avons le plaisir d'accueillir aujourd'hui un groupe de trois experts du domaine. Ainsi, la compagnie Equifax Canada représente les agences d'évaluation du crédit. C'est M. John Russo, je crois, qui fera l'exposé en son nom, et vous pourrez présenter vos collègues quand vous en aurez l'occasion.

De Forrest Green Group of Companies, nous entendrons M. Murray Rowe, président. Nous vous souhaitons la bienvenue, monsieur Rowe.

Il y a aussi M. Todd Skinner, président de TransUnion Canada. Il est accompagné, lui aussi, de collaborateurs.

Nous invitons normalement les témoins à d'abord faire un bref exposé de 5 à 10 minutes chacun, dans votre cas, après quoi nous aurions des questions à vous poser, à tous les trois. Nous procéderons dans l'ordre dans lequel ils figurent à l'ordre du jour, en commençant donc par Equifax Canada. Si j'ai bien compris, c'est M. Russo qui fera l'exposé.

Monsieur, vous avez la parole.

M. John Russo (vice-président, avocat et chef de la protection des renseignements personnels, Equifax Canada Co.): Je vous remercie, monsieur le président. Bonjour à tous.

Je m'appelle John Russo et je suis vice-président, avocat et chef de la protection des renseignements personnels à Equifax Canada. À ma gauche se trouve Mme Carol Gray, présidente d'Equifax Canada et à ma droite, Mme Tara Zecevic, vice-présidente des solutions de décision et des services de lutte contre la fraude.

Nous voulons d'abord remercier le comité de nous donner l'occasion de parler de notre étude sur le problème grandissant que représente le vol d'identité, ainsi que ses répercussions économiques. Nous tenons aussi à féliciter le gouvernement d'avoir adopté des mesures si positives et proactives pour aider à endiguer la croissance des crimes liés au vol d'identité au Canada. Les Canadiens bénéficient de stratégies coordonnées auxquelles participent le gouvernement, les forces de l'ordre, l'industrie, les consommateurs, et ce comité en est un excellent exemple. L'approche que nous avons adoptée face au vol d'identité ne touche pas que les personnes qui volent d'autres personnes, mais bien des façons plus profondes et générales de tirer avantage d'un système vulnérable — elles sont organisées, ciblées et, assurément, de nature globale.

Pensez-y un moment; pensez aux ramifications.

C'est dans cet esprit que j'aimerais soumettre au comité trois points, cet après-midi.

Tout d'abord, devant le nombre grandissant d'atteintes aux données personnelles, l'utilisation accrue des modes de livraison électronique et des réseaux, et l'influence des médias sociaux dans notre société, Equifax a pu constater que les crimes liés à l'identité ont augmenté de façon constante depuis 1998. De fait, le nombre de Canadiens victimes de vol d'identité a augmenté de 14 % en 2013, selon le Centre antifraude du Canada. Un autre exemple pertinent que je souhaite souligner aujourd'hui, c'est que nous estimons que les stratagèmes de fraude d'identité synthétiques ou fictifs coûtent aux Canadiens près de 1 milliard de dollars canadiens en pertes par année. Ces chiffres sont réels et se fondent sur de minutieuses analyses de coûts.

Ensuite, j'aimerais parler des types de vol d'identité — vrais et synthétiques — qui ont une incidence tant sur les entreprises que sur les consommateurs. Pour terminer, nous aimerions expliquer pourquoi les consommateurs et les entreprises du Canada devraient s'inquiéter et connaître les mesures qu'ils peuvent prendre pour prévenir les pertes financières dans l'avenir et d'autres problèmes associés au vol d'identité.

Avant qu'un crime lié au vol d'identité ne puisse être commis, il faut qu'il y ait vol de renseignements personnels pour monter et préparer le crime. Chez Equifax, nous avons remarqué une hausse importante de la quantité de renseignements personnels volés ou perdus, qui était imputable à diverses sources, comme des employés imprudents ou indisciplinés ou des accès non autorisés dans diverses institutions, allant des détaillants jusqu'aux fournisseurs de soins de santé en passant par les institutions financières et même le gouvernement. N'oublions pas non plus l'augmentation de vol d'identité qui découle des infractions aux données personnelles. Par exemple, à notre bureau de crédit, ces 18 derniers mois, nous avons protégé plus de 1,5 million de dossiers de crédit de Canadiens grâce à des alertes de crédit ou à une surveillance de crédit découlant directement d'infractions aux données personnelles, et ces chiffres sont constamment en hausse.

Selon des statistiques récentes, la majorité des menaces qui pèsent de nos jours sur les renseignements personnels viennent d'attaques malveillantes ou criminelles contre les bases de données des organisations; les infractions aux données personnelles sont en voie de devenir un trésor pour les fraudeurs. Selon d'importants résultats publiés dans le cadre d'une récente étude menée par le Ponemon Institute, 42 % des incidents mettent en jeu des attaques malveillantes ou criminelles. Dans le même ordre d'idées, les résultats démontrent que les infractions aux données personnelles attribuables à des attaques malveillantes ou criminelles coûtent aux entreprises de l'Amérique du Nord en moyenne 246 $ par dossier compromis, ce qui dépasse de loin la moyenne de 200 $. Enfin, plus de clients ont mis fin à leur relation avec les entreprises dont les données ont été volées; le taux de roulement moyen a augmenté anormalement de 15 % entre 2013 et 2014.

En matière de prévention contre le vol d'identité, les entreprises canadiennes ont pris bon nombre de mesures pour réduire les effets de ce crime, mais le transfert électronique de renseignements personnels joue un rôle déterminant dans le traitement des transactions financières, et il y a des limites aux mesures que peut prendre l'industrie. En effet, des milliers de dossiers de crédit personnels sont transmis par voie électronique tous les jours, lesquels sont acquis, sécurisés et utilisés en toute légalité par nos membres. De plus, des milliers de demandes de crédit sont traitées au quotidien, allant des prêts bancaires aux crédits-bails automobiles.

Et pourtant, il y a eu de nombreux cas où d'employés indisciplinés, ou des « fantassins », comme on les appelle, ont pris l'information fournie dans la demande de crédit faite auprès de leurs employeurs pour, comme tout trafiquant, vendre les renseignements personnels que comportent ces demandes à des groupes criminels organisés.

Dans plusieurs de ces enquêtes sur le vol d'identité, les services de police ont rapporté que l'information personnelle volée est souvent trouvée lors de contrôles routiers ou d'autres perquisitions légales. Simplement dit, il n'y a guère de raisons légitimes pour qu'une personne ait en sa possession des piles de demandes de crédit de consommateurs, d'informations financières ou d'autres documents concernant l'identité.

J'aimerais donner un peu plus d'informations sur les statistiques et les tendances du vol d'identité au Canada. Depuis 1998, Equifax Canada fait état de la croissance exponentielle des crimes liés à l'identité. Entre 1998 et 2003, le nombre de vols d'identité signalés au Canada a augmenté de 500 %; il s'agit de cas où des demandes étaient soumises et pour lesquelles des consommateurs légitimes du Canada subissaient des dommages. De 2004 à 2005, le taux de croissance s'est stabilisé, mais en 2008, les chiffres sont remontés aux niveaux élevés de 2003 et des crimes d'identité fictive, ou synthétique, ont commencé à apparaître.

Qu'est-ce qu'un crime d'identité synthétique? Un crime d'identité fictive ou synthétique survient quand de l'information personnelle est volée — auquel cas des composantes de cette information sont utilisées pour créer une personne non existante — ou encore, quand de l'information sur une identité est tout simplement inventée. L'auteur du crime le fait souvent en prenant de l'information personnelle comme le numéro d'assurance sociale d'une personne qui est décédée ou qui ne fait pas encore partie d'un système d'octroi de crédit, comme un enfant, afin de créer une identité non existante. L'auteur suit ensuite les progrès de l'identité fictive en extrayant des dossiers de crédit et en effectuant des centaines de milliers de dollars en opérations financières avant d'abandonner l'identité de la personne qu'il a créée et de disparaître sans laisser de trace. Ce qui est encore plus inquiétant, c'est que nous voyons communément des dizaines, voire des centaines, d'identités fictives utilisées par le même groupe au même moment. Le crime organisé joue un grand rôle ici, puisque les produits de cette criminalité servent à financer une vaste gamme d'autres activités mondiales illégales, voire le terrorisme.

Récemment, j'ai participé à un reportage d'enquête de la CBC sur les identités synthétiques, à la suite du projet Mouse mené par les services de police de Toronto. Pour certains, ces crimes peuvent paraître comme ne faisant pas de victimes ou n'ayant pas de visages, mais les répercussions donnent froid dans le dos. De faux noms sur de vraies cartes de crédit, de vrais permis de conduire et de vrais passeports présentent une réelle menace à notre sécurité nationale, et même mondiale. Je vous encourage à visionner ce reportage de Rick MacInnes-Rae à l'émission *The National* de la CBC.

Sans aucun doute, la création d'identité fictive est en hausse et des dizaines de millions de dollars sont siphonnés par des groupes du crime organisé chaque année. D'ailleurs, Equifax voit, en moyenne, 1 300 dossiers de consommateurs fictifs créés tous les mois à l'échelle du pays par des fraudeurs et autres criminels organisés. Le fait est que les criminels n'arrêteront pas d'évoluer et que nos lois, notre sécurité et nos tactiques de prévention doivent changer en même temps. Des voleurs usurpent de vraies identités ou créent des identités fictives au moment même où l'on se parle, et ce problème ne disparaîtra pas sans la concertation des autorités réglementaires, des forces de l'ordre et des solutions proposées par des organisations telles qu'Equifax. Nous évaluons que ces activités représentent plusieurs milliards de dollars au Canada

L'industrie des services financiers et du crédit continuent de faire leur part en aidant les victimes de crimes d'identité et en investissant des millions de dollars chaque année pour détecter les fraudes d'identité le plus rapidement possible. Les crimes liés à l'identité ont augmenté à un point tel qu'ils touchent tous les Canadiens directement ou indirectement. Contrairement à il y a 15 ans, il me serait difficile de trouver aujourd'hui une personne qui n'ait pas été victime d'un crime lié à l'identité, qui n'ait pas vu sa carte de crédit ou de débit être clonée, qui n'ait pas connu un collègue de travail renvoyé pour un comportement malhonnête ou dont l'identité n'ait pas servi à obtenir du crédit ou à soumettre une demande crédit. Je suis certain qu'un grand nombre des gens que vous représentez ont fait l'expérience de telles situations.

Enfin, le combat contre les crimes liés à l'identité en est un qui transcende la politique et qui commence par l'éducation et la conscientisation de chaque consommateur et ménage au Canada, surtout à la lumière des derniers incidents d'infractions aux données personnelles, où ce n'est plus la personne qui perd son information, mais où ce sont des entreprises qui sont piratées ou attaquées avec malveillance en vue d'obtenir votre information personnelle de nature délicate et confidentielle.

Le hacktivisme est en hausse et selon une récente étude d'ABI Research, il représente maintenant 47 % de toutes les activités des groupes de cybermenace. Les activités de ces hacktivistes pourraient ne pas sembler être liées en surface; toutefois, la communication de toute information personnelle qui peut ensuite servir à créer une identité réelle ou synthétique présente un réel impact financier sur les consommateurs. L'expression « perte de données personnelles » est devenue une expression familière.

● (1110)

Selon une récente étude nord-américaine de Javelin Strategy and Research, un consommateur sur trois qui est touché par des pertes de données devient une vraie victime du vol d'identité. Ce chiffre était de 1 sur 4 en 2012. Les consommateurs, tout comme les entreprises, devraient s'inquiéter.

Alors, quelles mesures doivent-ils prendre pour prévenir ou du moins détecter le vol et limiter les dommages futurs?

Premièrement, les consommateurs devraient vérifier leur dossier de crédit au moins une fois par trimestre afin de détecter toute anomalie ou fraude possible dans leur dossier. Le slogan d'Equifax à l'intention des consommateurs, c'est « vérifier pour protéger ». Vous pouvez le faire gratuitement, 365 jours par année, à n'importe lequel de nos bureaux de crédit canadiens.

Deuxièmement, si vous êtes victime de perte de vos données personnelles, demandez à l'organisation de vous fournir, à ses propres frais, des services de surveillance de crédit pour au moins les 12 prochains mois. Selon notre expérience, c'est durant cette période que la plupart des crimes liés au vol d'identité sont commis.

Enfin, soyez vigilants quant à l'information que vous donnez aux institutions. Ont-elles vraiment besoin de connaître votre numéro d'assurance sociale ou votre date de naissance pour une simple opération au détail ou une location?

Monsieur le président et chers membres du comité, au nom d'Equifax, je salue vos efforts visant à régler le problème croissant que sont les crimes liés à l'identité au Canada et je vous remercie de nous avoir donné l'occasion d'aborder cette importante question d'actualité.

Merci.

● (1115)

Le président: Merci, monsieur Russo.

C'est un exposé qui donne froid dans le dos et qui fait réfléchir. Voilà exactement pourquoi nous faisons cette étude, parce que de tels problèmes existent.

Passons maintenant au prochain témoin. Nous accueillons M. Murray Rowe, président de Forrest Green Group of Companies.

M. Murray Rowe, Jr. (président, Forrest Green Group of Companies): Monsieur le président, mesdames et messieurs les membres du comité, merci de nous recevoir.

J'aimerais aussi présenter mon associé, Bob Groves, qui me conseillera peut-être plus tard, selon vos questions. J'utiliserai une approche différente aujourd'hui, puisque mes collègues d'Equifax et de TransUnion présenteront un point de vue plus général. Je me concentrerai sur un groupe qui, d'après moi, est particulièrement vulnérable: les communautés des Premières Nations.

Je vais vous présenter brièvement Forrest Green. Nous possédons beaucoup d'expérience pour ce qui est d'appuyer des organisations du secteur privé. Nous avons la cote de sécurité de niveau secret. Nous avons travaillé avec l'Assemblée des Premières Nations et AADNC.

Nous croyons que les communautés des Premières Nations sont parmi les plus vulnérables à la fraude et à l'exploitation financière. Le manque de données de crédit les rend plus sujets à la fraude. Dans de nombreux cas, ils ne comprennent pas le fonctionnement des bureaux de crédit. Ils vérifient rarement leurs rapports de solvabilité et, par conséquent, les gens à qui j'ai parlé sont surveillés de près; ils reçoivent des appels d'agences de recouvrement...

Un député m'a appelé vendredi pour me dire qu'il croyait avoir été victime d'un vol d'identité. Il s'en est rendu compte tout de suite à cause des processus qui se mettent en branle. Les gens dans les réserves, pour leur part, sont difficiles à trouver, et ils communiquent rarement avec les bureaux de crédit.

À la page suivante, je vous présente un exemple de rapport. Ce n'est pas un vrai rapport de solvabilité, et je dirais que nous avons extrêmement généreux lorsque nous avons indiqué que moins de 5 % des membres des Premières Nations avaient examiné leur rapport de crédit personnel. Je dirais que c'est plutôt 1 %. Par curiosité, les membres du comité qui ont examiné leur rapport de solvabilité au cours de la dernière année peuvent-ils lever la main? Bien, c'est impressionnant. On voit que près de la moitié des membres ne l'ont pas examiné, alors imaginez dans les collectivités éloignées. Nous croyons qu'elles sont particulièrement vulnérables à ce genre de crime.

Nous mettons en oeuvre des solutions pour l'authentification en ligne et nous collaborons avec les services policiers. La page suivante contient une capture d'écran du service de police d'Hamilton. Pour éviter de devoir se rendre sur place pour montrer une pièce d'identité avec photo, nous offrons une solution qui utilise les données des bureaux de crédit pour confirmer l'identité d'une personne; il s'agit donc d'une solution antifraude. De nombreuses communautés autochtones dans les régions éloignées ont un faible revenu, et ce sont ces personnes qui devraient avoir accès à des services en ligne pour qu'elles n'aient pas à prendre l'avion ou l'auto et faire des centaines de kilomètres pour aller montrer une pièce d'identité avec photo. Ironiquement, parce qu'elles n'ont pas accès à un bureau de crédit, ce sont ces personnes qui sont forcées de faire ce genre de choses. Je pense qu'il est important de comprendre les conséquences importantes de l'utilisation des données des bureaux de crédit.

La question de la vérification de l'identité est également intéressante, car lorsque les gens postulent surtout des emplois à faibles salaires, les données des bureaux de crédit sont souvent utilisées pour les analyses et la recherche d'emploi. C'est un peu ironique: les gens qui sont les plus vulnérables et qui ont le plus besoin d'un emploi peuvent être victimes de discrimination parce qu'ils ont une mauvaise cote de crédit. Ce n'est pas lié directement à notre sujet, mais je pense qu'il y a des liens intéressants entre le manque de données ou des données de faible qualité, la fraude, le vol d'identité et la vulnérabilité.

J'aimerais aussi faire quelques observations intéressantes en m'appuyant sur les conclusions du Comité permanent des affaires autochtones et du développement du Grand Nord. Lorsqu'on regarde certaines des statistiques ci-dessous, on constate que les communautés autochtones ont tendance à ne pas faire confiance aux organisations qui recueillent des données; 80 % des cessions familiales se font en marge de la Loi sur les Indiens et 50 % des baux des bandes ne sont pas enregistrés. Cela démontre que les communautés autochtones ne font pas confiance à l'idée de partager des données ou qu'elles ne l'ont pas acceptée.

S'il y a une chose à retenir à la fin de cette discussion, c'est que l'éducation aura un rôle à jouer si on veut régler le problème. Il faut en parler et on ne peut pas seulement se fier aux chefs d'aujourd'hui. Ils ne connaissent pas ce sujet. Ils ne peuvent pas expliquer à leurs enfants comment préparer de bons rapports de solvabilité parce que personne ne leur a dit comment le faire.

● (1120)

La dernière page montre encore la nécessité d'appuyer l'accès à l'information et les problèmes de ne pas avoir d'identité, de pièces d'identité avec photo ou de données de bureau de crédit. Non seulement cela mène à la fraude, mais il y a même eu un exemple intéressant, quoique franchement triste, d'une femme qui a reçu un règlement pour les pensionnats, qui a eu de la difficulté à ouvrir un compte de banque, qui a encaissé le chèque, a ramené l'argent à la maison et s'est fait voler et assassiner dans la réserve.

Je pense que cela démontre la vulnérabilité de ces gens, et nous devons commencer à examiner certaines des causes profondes. Au sujet de la fraude, il faut se rappeler que, d'après moi, lorsqu'il y a absence de documents sur l'identité, les gens sont plus vulnérables à la fraude que ceux qui peuvent s'en rendre compte en une semaine, comme c'est le cas pour de nombreux Canadiens. Mes collègues ne seront peut-être pas d'accord, et diront que c'est beaucoup plus répandu et plus difficile que ça, mais les gens que je connais qui ont été victimes de fraude ont réagi très rapidement.

Merci beaucoup de m'avoir donné la parole.

Le président: Merci, monsieur Rowe, d'avoir présenté cet aspect très important pour notre étude. Je suis certain qu'il y aura des questions à ce sujet plus tard.

Nous passons à M. Todd Skinner, président de TransUnion Canada.

M. Todd Skinner (président, TransUnion Canada): Monsieur le président, mesdames et messieurs les membres du comité, merci beaucoup de nous accueillir aujourd'hui. L'associée qui m'accompagne se nomme Chantal Banfield, et elle est l'avocate générale de TransUnion Canada.

Je parlerai un peu de TransUnion, puis du problème du vol d'identité.

TransUnion est un chef de file mondial dans la gestion du crédit et de l'information, et offre des avantages à des millions de personnes dans le monde en rassemblant, analysant et livrant les renseignements. TransUnion aide les entreprises à améliorer leur efficacité, à gérer les risques, à réduire les coûts et à accroître les revenus en offrant des données exhaustives et des analyses poussées pour la prise de décisions. Nous offrons aux consommateurs des outils, des ressources et de l'information pour les aider à gérer la santé de leur crédit et à atteindre leurs objectifs financiers. Ainsi, TransUnion, par l'entremise de son bureau à Toronto et de son siège social mondial à Chicago, participe au renforcement de l'économie mondiale.

TransUnion est régie par les lois sur la protection des consommateurs et de la vie privée. Notre activité principale est fondée sur le consentement; il faut le consentement pour obtenir un dossier de crédit. Nous effectuons des vérifications de nos membres pour des membres potentiels et des entreprises légitimes. Nous traitons des millions de données chaque mois et nous mettons à jour notre base de données régulièrement. Nous reconnaissons l'importance de protéger les renseignements, et nous sommes ravis d'annoncer que nous avons été des pionniers des alertes à la fraude au début des années 1990.

Le vol d'identité se divise en trois catégories: la perte ou l'atteinte aux données, le vol d'identité en tant que tel qui en découle, et la fraude qui s'ensuit. Une atteinte aux données, c'est lorsqu'un disque dur est volé, comme celui des dossiers de prêts étudiants, ou le vol qui a lieu à Revenu Canada.

Ce sont les consommateurs et les entreprises qui nous informent de ces atteintes aux données. Un des problèmes, c'est que les entreprises ne déclarent pas toujours ces atteintes, ainsi qu'il est recommandé par la commissaire fédérale à la protection de la vie privée dans « Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée ».

Il y a deux statistiques en particulier qui ressortent de celles présentées par TransUnion. Le nombre d'atteintes déclarées au cours des cinq dernières années a diminué de 30 %. Mais ce qui est alarmant, c'est que le nombre de victimes potentielles a augmenté de 600 %. On pourrait présumer que ces atteintes aux données ont lieu dans les institutions financières, mais ce n'est pas le cas. Seulement 8 % des atteintes déclarées viennent des institutions financières; 70 % viennent de l'industrie médicale, des services ou du détail. Pour les autres industries, le gouvernement, les compagnies d'assurances ou de finances, les chiffres sont très bas.

Quelles sont les conséquences? Le secteur financier est très conscient de ses obligations en matière de protection envers ses clients. Lorsqu'il y a des pertes dues à des atteintes dans le secteur financier, ces entreprises en paient le coût. C'est certainement attribuable, en partie, aux exigences du BSIF.

TransUnion offre des services à un grand nombre de ces institutions. Nous respectons les normes de l'industrie des cartes de paiement. Nous sommes également conformes aux normes ISO, et régulièrement...

● (1125)

Le président: Monsieur Skinner, pourrais-je vous interrompre brièvement? Les traducteurs n'ont pas copie de votre rapport, et ils demandent si vous pourriez ralentir un peu. Merci.

M. Todd Skinner: Certainement. Voulez-vous que je poursuive à partir de là où j'en étais rendu?

Le président: Oui.

M. Todd Skinner: Nous respectons les normes ISO, et régulièrement, nous sommes soumis à des vérifications en vertu des exigences SSAE 16.

Nos données semblent indiquer qu'à l'extérieur du secteur financier, les entreprises ne sont pas suffisamment sensibilisées aux problèmes et qu'il faudrait faire plus d'éducation dans ce domaine, non seulement sur les obligations découlant d'une atteinte, mais aussi sur les protocoles de sécurité pour empêcher ces atteintes.

Il sera utile d'être informé des atteintes aux données. TransUnion appuie les efforts du gouvernement dans le cadre du projet de loi S-4. Bien que nous ne voulions pas inonder les clients d'avis d'atteinte, lorsqu'il y a un risque de préjudice matériel, il y a des avantages à ce que les clients soient avisés.

Voici certaines statistiques sur les conséquences pour les consommateurs et TransUnion. Le nombre de victimes potentielles a augmenté de 600 % au cours des cinq dernières années. Le nombre confirmé de victimes de fraude a augmenté de 100 %. Une grande partie des consommateurs déclarent ces fraudes au Centre antifraude du Canada — PhoneBusters — et bien qu'il y ait eu une augmentation de 300 % du nombre d'alertes à la fraude publiées, nous avons encore du travail à faire.

Ces atteintes ont des conséquences à court terme pour TransUnion et Equifax, car elles augmentent le volume d'appels à nos centres et les demandes de divulgation d'alertes aux consommateurs. Nous avons investi dans des technologies pour rendre ce processus aussi efficace que possible et pour contribuer à cette augmentation de 300 % du nombre d'alertes à la fraude publiées par les bureaux de protection des consommateurs. Nous réduisons le nombre de fraudes, et nous sommes ravis de voir que ce nombre n'augmente pas au même rythme que celui des victimes potentielles.

Qui paie? Ce sont les consommateurs, à moins que les entreprises ou les organisations gouvernementales ayant causé l'atteinte soient prêtes à payer pour les dommages qu'elles ont créés. Nous croyons que ces coûts devraient être payés par les entreprises qui ont compromis des renseignements des consommateurs. Ce ne sont pas toutes les entreprises qui acceptent cette responsabilité et qui paient pour des solutions afin de réduire les préjudices possibles pour les consommateurs en réduisant les risques.

Que devrait-on faire? Premièrement, il faut aviser la commissaire à la protection de la vie privée. TransUnion appuie les modifications à la LPRPDE dans le projet de loi S-4. Lorsque la perte de données financières sensibles a été confirmée, les deux bureaux devraient être informés. Lorsque la perte de données financières délicates est confirmée, les deux bureaux devraient publier des alertes à la fraude, au moins, pour réduire la possibilité de vol d'identité. Par exemple, nous servons nos clients différemment; si une atteinte a lieu et que quelqu'un avise Equifax, la fraude pourrait toujours avoir lieu si les données subtilisées sont utilisées à une institution financière desservie surtout par TransUnion. Dans la plupart des cas, les deux bureaux devraient être avisés.

En ce qui concerne les identités synthétiques, mon collègue John Russo en a parlé, ainsi que des répercussions sur le marché canadien. Il s'agit vraiment de recréer une identité pour commettre de la fraude. Dans le cas de la fraude synthétique, personne ne peut se plaindre. Il n'y a pas de clients à qui parler. C'est un coût payé indirectement par l'ensemble des gens. En ce qui concerne la sécurité publique, la CBC en a parlé dans le cadre de quelques reportages, et John a mentionné les pertes de plusieurs milliards de dollars que les Canadiens absorbent sous la forme de différents frais et coûts. Chaque consommateur paie pour la fraude synthétique.

Comment en arriver à une solution? Nous collaborons avec les autorités policières pour déclarer les activités suspectes. Nous recevons ces renseignements, les entrons dans notre base de données sur la fraude et les transmettons aux institutions financières.

Pour prévenir ces crimes, il faut une meilleure technologie afin que les cartes d'identité ne soient pas facilement copiées et authentifiées. Si on veut vraiment s'attaquer au problème, il faut que les agences gouvernementales et le secteur financier mettent en commun leurs renseignements. Cette absence de partage crée des cloisons, et les fraudeurs en profitent.

Aujourd'hui, il n'y a pas de méthodes automatisées par lesquelles le secteur privé peut obtenir confirmation qu'une pièce d'identité a été émise par le gouvernement ou si cette pièce d'identité appartient à la personne qui dit en être le propriétaire. TransUnion et Equifax peuvent servir de courroies de transmission pour les institutions financières, puisque nous assurons déjà, par exemple, la vérification de l'identité pour l'analyse des profils de clients en vue de la lutte contre le blanchiment. Ces deux stratégies sont décrites dans le document de la GRC intitulé « Stratégie nationale de lutte contre les crimes liés à l'identité ».

En conclusion, TransUnion appuie l'initiative de s'attaquer au vol d'identité; premièrement, elle déclare les atteintes aux termes du projet de loi S-4 et avise les deux bureaux lorsqu'une atteinte aux données financières délicates est confirmée, et deuxièmement, elle s'assure que les entreprises responsables des atteintes en paient les frais, au lieu de les refiler aux consommateurs. Troisièmement, en ce qui concerne les lacunes en matière de sensibilisation à la sécurité et à la protection des données à l'extérieur du secteur financier, TransUnion appuie les avis d'atteinte aux données lorsque les circonstances le justifient comme moyen de sensibiliser les entreprises. Quatrièmement, nous appuyons également l'accent mis sur l'identification synthétique, en permettant le partage de renseignements entre le gouvernement et les institutions financières pour prévenir la fraude et le vol d'identité, et en investissant dans les mesures de sécurité pour des cartes d'identité que pourra utiliser le secteur privé afin de combattre le blanchiment d'argent et de prévenir la fraude.

● (1130)

Monsieur le président, mesdames et messieurs les membres du comité, merci beaucoup de nous avoir reçus aujourd'hui.

Le président: Merci beaucoup, monsieur Skinner. C'était très intéressant.

Nous allons maintenant passer aux questions des membres du comité. Nous allons débuter avec l'opposition officielle, le Nouveau Parti démocratique, représenté par Charmaine Borg.

[*Français*]

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Merci, monsieur le président.

Bonjour. Je vous remercie d'être parmi nous aujourd'hui. Vos témoignages sont très intéressants.

Ma première question s'adresse à M. Russo.

Vous avez mentionné que nous pouvions toujours avoir accès à notre dossier de crédit. Cependant, il est envoyé par la poste, ce qui est tout de même assez long. Pour l'obtenir gratuitement, c'est ainsi qu'il faut procéder. Si nous voulons avoir accès à notre dossier en ligne, il faut cependant payer. Pourquoi faut-il payer des frais? Serait-il possible de faire le contraire et de nous donner accès gratuitement à notre dossier de crédit en ligne? Selon moi, ce serait plus facile pour les consommateurs.

Me Chantal Banfield (vice-présidente et avocate générale, TransUnion Canada): Au Canada, depuis l'apparition des agences de crédit, la loi exige que nous ayons des bureaux dans certaines provinces. Nous avons donc une infrastructure qui permet à un consommateur de la Nouvelle-Écosse, par exemple, d'aller au bureau de TransUnion Canada pour obtenir une fiche de crédit. Parce qu'il s'agit des exigences de la loi, nous devons avoir une infrastructure qui soutient les bureaux que nous devons avoir à plusieurs endroits au Canada.

De plus, comme l'a mentionné M. Skinner, nous investissons dans des technologies téléphoniques comme les systèmes de réponse vocale interactive. Par exemple, les gens n'ont pas besoin d'envoyer de preuve d'identité par la poste. Ils peuvent tout simplement suivre un processus d'authentification au téléphone et recevoir leur dossier de crédit par la poste.

Vous avez l'exemple des États-Unis. En 2005 ou 2006, la Fair and Accurate Credit Transactions Act a été adoptée. En vertu de celle-ci, les consommateurs américains ont le droit de consulter leur dossier de crédit une fois par année, et la méthode choisie est l'accès en ligne.

Pour notre part, nous avons déjà une infrastructure que nous devons soutenir depuis le début des années 1990, au moment où les lois ont été adoptées dans la plupart des provinces. C'est une évolution un peu différente.

Mme Charmaine Borg: Monsieur Russo, je vous donne également l'occasion de répondre. Je suppose que votre réponse sera essentiellement la même.

[*Traduction*]

M. John Russo: Oui, je vais répondre. J'ajouterai quelques nuances à ce qu'a dit Mme Banfield.

Premièrement, au Canada, comme Mme Banfield l'a dit, vous pouvez recevoir votre dossier en personne dans les bureaux d'Equifax. Vous pouvez aussi recevoir votre rapport de solvabilité par téléphone en deux jours, grâce au système de réponse vocale interactive, de même que par Internet à peu de frais.

Comme Mme Banfield l'a indiqué, aux États-Unis, c'est une copie par année par personne. Ensuite, vous devez payer. Ici, vous pouvez avoir accès à votre dossier chaque jour, 365 jours par année, et nous avons en place l'infrastructure qui le permet, y compris les demandes par la poste et tout le reste. Nous payons ces coûts, c'est-à-dire les lettres, les enveloppes et les timbres qu'il faut envoyer à ces personnes dans le cadre des processus de vérification et de sécurité en place pour être certains que nous envoyons le bon dossier de crédit à la bonne personne.

Je ne vais pas répéter ce qu'a dit Mme Banfield. Elle vous a présenté un bref historique des lois.

Merci.

● (1135)

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Ma deuxième question porte sur un point soulevé auparavant par l'un des témoins experts. Cette personne a souligné que mettre en place un gel de crédit pourrait prévenir la fraude après un vol d'identité. En effet, la plupart du temps, lorsqu'une personne vole une identité, elle fait des demandes de cartes de crédit et fait toutes sortes de dépenses.

Cela serait-il possible dans votre cas? Réfléchissez-vous à l'idée de mettre en place un système de gel de crédit?

[*Traduction*]

M. John Russo: C'est une excellente question. Nous en avons parlé il y a environ 10 ans lorsqu'il y avait le projet de loi 152 en Ontario, qui aurait permis d'ajouter une alerte à votre dossier pour indiquer, par exemple, de contacter Mme Carol Gray avant d'accorder du crédit. Mme Gray aurait pu fournir son téléphone cellulaire afin qu'on communique avec elle immédiatement pour avoir la certitude que l'on fait affaire avec la bonne personne.

L'Ontario s'est éloigné de cette approche parce que les consommateurs voulaient une authentification en temps réel. Ils voulaient un accès immédiat au crédit. Disons qu'il y a un gel de crédit à votre dossier et que vous avez une urgence — disons un accident d'auto — et que vous devez payer certains frais pour faire réparer votre auto, ou que vous vivez une autre situation malheureuse où vous devez avoir accès à votre argent, à du crédit. Le gel vous empêcherait totalement d'avoir accès à du crédit immédiatement. L'accès aux fonds serait ralenti, surtout dans des situations d'urgence.

On constate qu'aux États-Unis, certains États s'éloignent de cette idée de gel de crédit.

[*Français*]

Mme Charmaine Borg: Merci.

Voulez-vous ajouter quelque chose, madame Gray?

[*Traduction*]

Mme Carol Gray (présidente, Equifax Canada Co.): Si vous me permettez d'ajouter un point, je pense qu'il y a de multiples approches pour en arriver à une solution, mais malheureusement, il n'y a pas d'approche qui convient à tous ou de solution magique. En plus de ce que John a dit, il y a des services de surveillance en temps réel qui n'empêchent pas le consommateur d'avoir accès à du crédit, mais qui les alertent immédiatement si quelqu'un a accès à leur dossier de consommateurs sans qu'ils le sachent, et ils peuvent réagir sur-le-champ.

[*Français*]

Mme Charmaine Borg: Merci.

Comme il ne me reste qu'une minute, je vais poser rapidement une dernière question.

Monsieur Rowe, vous avez démontré au moyen d'exemples que, finalement, très peu de personnes faisaient la demande pour avoir accès à leur dossier de crédit.

Je voudrais savoir si vous connaissez le pourcentage de Canadiens qui font une telle demande.

[*Traduction*]

M. Murray Rowe: Excusez-moi. Je n'étais pas certain si vous aviez dit Russo ou Rowe.

[*Français*]

Mme Charmaine Borg: En fait, n'importe qui peut répondre.

[*Traduction*]

M. Murray Rowe: Désolé. Pourrions-nous revenir un peu en arrière? J'essayais de suivre.

Mme Charmaine Borg: Je vais le dire en anglais et nous allons pouvoir laisser faire la traduction.

Je me demandais si vous, ou Equifax ou TransUnion, aviez des renseignements sur le pourcentage de Canadiens qui demandent leurs rapports de solvabilité.

Mme Carol Gray: Je n'ai pas les statistiques exactes, car bien que nous effectuions le suivi du nombre de demandes ou de consommateurs qui veulent voir leurs dossiers, la même personne peut le demander plus d'une fois pendant une année. Je dirais que c'est sûrement autour de 25 à 30 %. Il s'agit, tout au plus, de 30 % des consommateurs pendant une année; il y a donc beaucoup de progrès à faire.

Cela varie beaucoup selon l'âge. Les personnes âgées ont tendance à examiner leur dossier moins fréquemment que les jeunes qui bâtissent leurs antécédents de crédit.

Le président: Merci, madame Charmaine.

Est-ce que quelqu'un d'autre voudrait ajouter quelque chose à ce sujet?

M. Todd Skinner: Du point de vue de TransUnion, les pourcentages seraient probablement semblables à ceux d'Equifax pour ce qui est de la transmission de rapports aux consommateurs.

M. John Russo: Les dossiers de nos membres sont consultés 150 000 fois par jour; c'est donc dire qu'il y a des membres qui accèdent à des renseignements sur des particuliers comme vous et moi 150 000 fois par jour. Pour ce qui est de la mise à jour des comptes, pour vous donner un peu de contexte, 50 millions de comptes sont mis à jour chaque mois chez Equifax.

● (1140)

Le président: Monsieur Rowe, brièvement, s'il vous plaît...

M. Murray Rowe: Nous avons très peu de renseignements sur les collectivités autochtones, plus particulièrement celles des Premières Nations. Nous tentons, entre autres, de faire de la recherche sur le sujet et de recueillir des données afin d'éclairer des discussions empiriques. Je pense que ni mes collègues ni moi-même ne sommes en mesure de formuler des observations sur les pourcentages précis pour ce qui est des Autochtones. Selon moi, ils représenteraient une fraction des chiffres obtenus pour le reste de la société.

Le président: Merci beaucoup à tous.

Nous passons maintenant à Laurie Hawn, du Parti conservateur.

Vous avez sept minutes, s'il vous plaît, Laurie.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci, monsieur le président, et merci à tous nos témoins de leur présence.

J'aimerais commencer par Equifax. Proposez-vous des produits en matière de protection contre le vol d'identité et combien cela coûte-t-il?

M. John Russo: Oui. Il a deux types de protection que nous proposons. Il existe une alerte crédit que vous pouvez ajouter à votre dossier partout au Canada pour 5 $ plus taxes applicables. Cela reste dans votre dossier pendant six ans sauf si vous demandez de la supprimer.

Il existe aussi des services de surveillance du crédit, comme je l'ai indiqué dans mes notes d'allocution, en ce qui a trait à des programmes, qui vous permettent d'avoir accès en temps réel, 24 heures sur 24 et 7 jours sur 7, à vos renseignements. On vous fait savoir tout changement apporté à votre dossier, toute demande faite en votre nom, peut-être un changement d'adresse parce que quelqu'un essaie de la changer afin de faire expédier vos renseignements à une autre adresse, et d'autres cas comme ça. Il y a donc la surveillance du crédit et l'alerte crédit.

L'hon. Laurie Hawn: Au risque de donner l'impression de faire de la publicité pour Equifax, j'imagine que les gens qui ne bénéficient pas de cette protection sont moins protégés que les autres.

Mme Carol Gray: C'est exact. Il y a des services facultatifs que l'on peut ajouter aux services de base, comme une assurance pour portefeuille perdu, etc.

L'hon. Laurie Hawn: Ma prochaine question s'adresse à M. Rowe de Forrest Green. Pour les Premières Nations et pour un grand nombre de programmes auxquels ils participent, le défi est d'ordre culturel, ce qui entraîne un problème de confiance, etc. Avez-vous des chiffres sur le nombre de victimes chez les Premières Nations? Nous parlons d'une très faible participation au processus. A-t-on des chiffres sur les victimes qui sont membres des Premières Nations?

M. Murray Rowe: Je n'ai pas de chiffres à ce sujet. Nous avons fait des recherches approfondies sur le sujet et en fait, c'est quelque chose auquel nous nous intéressons. Selon moi, ce qu'il faut, c'est une culture dans les réserves, en particulier. Par exemple, dans mon exposé tout à l'heure, j'ai dit qu'environ 80 % des transactions ne sont pas enregistrées auprès du gouvernement fédéral. Ils ne paient pas d'impôt sur le revenu. Il existe un grand nombre de défis différents concernant l'enregistrement et ses avantages.

Je pense que, bien honnêtement, l'un de nos objectifs est de tenter de recueillir des renseignements afin de pouvoir fournir des rapports à des organisations comme la vôtre de façon plus claire. C'est un front sur lequel nous sommes actifs. Nous espérons que cela aura lieu au niveau des collectivités. On ne veut pas que cela soit imposé aux réserves. Cela prend plus de temps, mais notre approche consiste à s'assurer que les Premières Nations en prennent l'initiative afin que les chefs et leurs conseils appuient ce type de dialogue.

L'hon. Laurie Hawn: Cela m'amène à une deuxième question. Pour ce qui est de la participation des Premières Nations à tout le processus, pour ce qui est de la formation des gens — la formation du personnel, la mobilisation des gens — votre organisation...?

M. Murray Rowe: Ce n'est pas encore fait, mais nous avons parlé à plus de 20 bandes. C'est un long processus. C'est coûteux, mais nous savons qu'il s'agit du groupe démographique qui connaît la plus forte croissance au pays. Manifestement, il y a entre un demi-million et un million de personnes qui sont invisibles aux bureaux de crédit. C'est tout à fait frappant. À part les nouveaux immigrants, je ne connais pas d'autres groupes qui connaissent ces mêmes défis.

L'hon. Laurie Hawn: Je pense qu'il est juste de dire que ce haut degré de non-enregistrement, etc., peut s'expliquer par divers motifs. Mais si nous pouvons convaincre les Premières Nations — et il faudra du temps — qu'il vaut mieux faire partie du système, de toute évidence, que l'inverse...

M. Murray Rowe: Exactement.

Bien honnêtement, je pense que la réforme foncière — comme je l'ai indiqué plus tôt au président — est l'un des projets les plus enthousiasmants à venir. Le concept de propriété individuelle, ou ne serait-ce que la possibilité de louer des terres... Cela serait conforme au paragraphe 89(1.1); on parle donc de quelque chose de possible, et c'est dans le cadre de la Loi sur les Indiens. Je pense que le fait de ne pas être en mesure de verser des milliards de dollars afin de permettre aux collectivités des Premières Nations d'investir dans leur logement et d'ensuite le léguer à leurs enfants et à leurs petits-enfants est tout à fait incroyable. À l'heure actuelle, dans la plupart des cas, ils sont dans l'impossibilité d'y participer.

Nous avons effectué une enquête informelle auprès de cinq bandes et, dans certains cas, les taux d'intérêt sont plus élevés de 300 % pour les collectivités autochtones. D'ailleurs, cela tient même compte des garanties de prêt du ministère, c'est-à-dire une garantie à 100 % de la Couronne. Il y a un certain nombre de problèmes que je ne comprends pas. Je crois qu'il y a un problème systémique au sein du milieu bancaire et dans la façon dont les bureaux de crédit recueillent et distribuent des renseignements. C'est, selon moi, quelque chose que l'on doit examiner avec les collectivités autochtones.

L'un de nos objectifs est de mieux comprendre le problème et d'obtenir de la rétroaction directe des chefs et de leurs conseils, et c'est ce que nous faisons activement.

Mais il ne s'agit pas là d'une solution à court terme. Ce que l'on veut, c'est changer les choses, et cela ne peut être fait à la hâte.

● (1145)

L'hon. Laurie Hawn: Rien n'est en place, mais c'est quelque chose que je comprends. C'était une observation très pertinente et j'espère que cela sera inclus dans le rapport.

Mme Carol Gray: Monsieur le président, j'aimerais faire une suggestion afin de nous assurer que nous nous en tenons aux faits.

Nous pourrions entreprendre une étude, et si nous connaissons les codes postaux des réserves, nous pourrions déterminer le nombre de rapports de consommateurs particuliers qui résident dans ces réserves. Nous pourrions nous en tenir au minimum — tout en nous assurant d'avoir au moins 15 foyers, cependant — sans qu'il soit permis d'utiliser ces données. On pourrait entreprendre cette étude et cela nous éclairerait peut-être. Si vous connaissez le nombre de gens qui résident dans une réserve à l'heure actuelle, on pourrait vous dire combien font l'objet d'un rapport et vous fournir des chiffres à ce sujet.

L'hon. Laurie Hawn: Est-ce là quelque chose que vous proposez comme recommandation pour le comité?

Mme Carol Gray: En effet.

L'hon. Laurie Hawn: Oui, d'accord.

M. Murray Rowe: J'aurais quelque chose à dire à ce sujet.

Je pense que cela est bien plus complexe que ce qui se passe. L'un des problèmes, c'est que les bureaux de crédit fondent leurs renseignements sur les normes d'adresse de Postes Canada. Postes Canada ne livre pas le courrier par adresse dans les réserves. Nous connaissons un certain nombre de problèmes fondamentaux.

J'aime votre méthode. Je vous en félicite, mais je pense que le dialogue sur ce qui a lieu... Je pense qu'il nous faut travailler main dans la main avec un grand nombre des employés dévoués du ministère des Affaires autochtones et du Développement du Nord, car nous sommes aux prises avec des problèmes fondamentaux. Dans les réserves, il n'y a pas de numéros de voirie. Il n'existe pas de rues enregistrées.

Je pense qu'il nous faut prendre du recul. Nous devons examiner les choses comme les boîtes postales utilisées par les Autochtones, et les Premières Nations en particulier, et c'est là une chose sur laquelle nous travaillons. Je pense que c'est un moment très intéressant, mais si nous pouvions obtenir l'aide du comité, ce serait très utile.

L'hon. Laurie Hawn: Je vous remercie. C'est utile.

Le président: Voilà qui met tout juste fin au temps qui vous est imparti.

Scott Andrews, pour le Parti libéral, allez-y.

M. Scott Andrews (Avalon, Lib.): Je vous remercie, monsieur le président.

Je vous souhaite à tous la bienvenue. Nous avons avec nous, ce matin, un groupe de témoins intéressants.

J'aimerais revenir à la question de Laurie sur les cartes de crédit et la surveillance du crédit, et aborder les deux sujets en même temps.

J'aimerais que TransUnion donne une réponse aussi, parce que je crois que vous avez dit également que vous aviez un système d'alerte en cas de fraude, alors je présume que c'est semblable.

Ai-je raison de dire que TransUnion et Equifax sont aux premières lignes lorsqu'une personne est sur le point de devenir victime de fraude? Diriez-vous que ce sont les premiers à pouvoir donner le signal d'alarme lorsque le crédit d'une personne est utilisé de façon frauduleuse? Ai-je raison?

Mme Carol Gray: Je vous dirais qu'en matière de crédit, oui, mais il y a des cas d'atteinte aux données qui ne relèvent pas du crédit et où nous ne sommes pas présents à titre de première ligne de défense. Mais s'il est question d'information contenue au dossier d'un consommateur, nous sommes souvent perçus comme la première ligne de défense.

M. Todd Skinner: Avant d'arriver à TransUnion — je n'y suis que depuis 75 jours — j'ai passé une bonne partie de ma carrière dans les services financiers. Je crois que le secteur des services financiers a un rôle de première ligne en matière de prévention de la fraude, de même que le secteur du détail, lorsqu'il obtient les données. Comment conservent-ils les données, comment protègent-ils les données afin qu'il n'y ait pas d'atteinte et que les données ne se retrouvent pas entre les mains de fraudeurs?

Je crois qu'en matière de protection de deuxième ligne, soit lorsque les bureaux de crédit Equifax ou TransUnion sont consultés, c'est à ce moment-là que les produits relatifs au vol d'identité d'Equifax, qui visent à sensibiliser à la fraude, entrent en jeu pour tenter de régler le problème. Je dirais donc qu'en matière de services de première ligne, les services financiers et du détail constituent un aspect, tandis que nous constituons probablement un aspect qui représente une fois et demie cette responsabilité, parce que d'une certaine façon, nous pouvons communiquer avec les consommateurs. Mais la fraude typique prend d'abord naissance au sein de ces institutions.

M. Scott Andrews: Je crois que ce que vous venez de nous dire, c'est que dans la plupart de ces institutions, des cas de fraude se produisent s'il y a atteinte aux données, et si certaines activités d'origine criminelle y sont menées.

M. Todd Skinner: Oui.

M. Scott Andrews: D'accord.

Mme Tara Zecevic (vice-présidente, Decision Solutions, Equifax Canada Co.): J'allais ajouter qu'il n'y a pas toujours atteinte aux données. Parfois il s'agit d'un employé indiscipliné, ou il peut s'agir de fouille de poubelles. Les atteintes peuvent être plus ou moins sophistiquées. Les données peuvent être compromises de diverses façons.

● (1150)

M. Scott Andrews: D'accord; pour ce qui est des coûts de ces alertes, de la surveillance du crédit, le consommateur doit payer ces frais. Pouvons-nous changer cette situation au moyen des mesures législatives? Vous avez dit que selon la loi, il fallait fournir une copie par la poste. Pourrions-nous changer la loi pour accorder aux consommateurs davantage de surveillance du crédit de façon gratuite, par exemple, si nous pouvions lever les restrictions en matière de transmission par la poste, etc.?

Avez-vous pensé aux changements qui pourraient être apportés à la loi pour offrir davantage de services gratuitement sans que cela vous coûte aussi cher?

Me Chantal Banfield: Je peux vous dire que chaque fois qu'il y a une réforme des lois sur les renseignements concernant les consommateurs dans les diverses provinces, il s'agit du genre de choses que nous demandons. De nos jours, avons-nous vraiment besoin d'un bureau à l'extérieur de notre siège social, parce que si ce n'était pas le cas, nous pourrions investir ailleurs — pour offrir de l'information de façon électronique, par exemple. Nous avons donc essayé, mais nous n'avons pas eu de succès. Je crois que mon collègue, M. Russo, vous dira la même chose, à savoir que nous avons tenté notre chance dans les diverses provinces.

Mme Tara Zecevic: J'aimerais ajouter que nous aimerions qu'il y ait des réformes. Ce serait des peines imposées au crime organisé... et aux crimes. Je sais que ces vols d'identité sont souvent perçus comme des crimes économiques et nous aimerions qu'il y ait des peines plus sévères pour ces crimes.

M. John Russo: Je suis d'accord avec les déclarations de Mme Banfield, à savoir que ce ne sont pas simplement des réformes provinciales, mais également des réformes de la Loi sur la protection des renseignements personnels. Nous en avons déjà fait la demande, mais sans trop de succès.

M. Scott Andrews: Vous avez parlé de fantassins, monsieur Russo, c'est-à-dire des gens... là où ils travaillent. Est-ce un grave problème? La GRC est venue témoigner et n'y a pas du tout fait allusion.

J'aimerais savoir si vous pouviez nous donner plus de détails sur cet aspect en particulier. Je crois que c'est la première fois qu'on en entend parler et c'est très préoccupant.

M. John Russo: Oui, et j'ai entendu ces mêmes choses lorsque nous travaillions à l'enquête de la CBC; un service de police de Toronto voyait là un grand problème, mais pour une raison quelconque, ce n'était pas le cas pour la GRC. Je ne suis pas en train de dire qu'un service soit meilleur que l'autre.

Ce qui m'a vraiment intéressé lorsque j'ai commencé à Equifax, il y a sept ans, c'était le stratagème de vols d'identité synthétique, car nous savions que ce crime commençait à émerger. J'examinais les différents rapports, je travaillais avec les services d'application de la loi locale dans les différentes provinces. Il y avait certains noms fictifs qu'ils s'inventaient, comme « Robert Consommateur ». À l'époque, il y avait 100 ou 200 rapports qui portaient sur une identité fictive et nous travaillions de concert avec la police. C'était il y a sept ans. Le nombre de cas a augmenté de façon draconienne chaque année, et nous en sommes à 1 300 ou 1 400 dossiers par mois, en moyenne, qui utilisent des identités fictives de gens qui n'existent pas. Nous le voyons au dossier. Ces personnes font un détournement avec fuite et elles croient pouvoir quitter le pays et ne pas payer les factures. En réalité, ces personnes ne font que créer une nouvelle identité.

Nous l'avons même constaté dans nos centres sans rendez-vous. Nous avons un tel centre dans l'édifice où je travaille à Toronto. Par exemple, une personne peut venir avec son permis de conduire; nous voyons que c'est un homme de 35 ans sur la carte, mais lorsque la carte passe dans le lecteur, nous constatons que les renseignements appartiennent à une femme. Nous avisons bien sûr les forces de l'ordre.

C'est un vrai problème pour nous et c'en est un qui coûte 1 milliard de dollars.

Mme Tara Zecevic: J'ajouterais simplement que c'est souvent difficile de quantifier car, comme John l'a mentionné, les personnes ayant des identités fictives établissent un dossier de crédit au fil du temps. Nous utilisons une expression dans l'industrie, « détournement avec fuite », lorsque l'endettement atteint un sommet sans précédent. Il est souvent très difficile de mesurer ces situations, car elles seront parfois classées dans la catégorie de recouvrement. Dans ces cas-là, c'est très difficile à mesurer puisqu'en réalité, il ne s'agit pas d'un dossier de recouvrement, mais d'une fraude.

M. Scott Andrews: La GRC a-t-elle suffisamment de ressources? Se concentre-t-elle sur de tels dossiers? Ou êtes-vous plutôt frustrés avec les services de police qui ne portent pas assez d'attention à cet enjeu? Avez-vous des commentaires relativement au problème d'application de la loi?

Le président: Pourriez-vous donner une réponse très brève, s'il vous plaît? En fait, monsieur Andrews, votre temps est écoulé.

M. John Russo: Nous pourrions toujours faire plus en travaillant ensemble.

● (1155)

Le président: C'est le genre de concision que nous aimons bien ici, merci.

Cela met fin au premier tour de questions.

Non, en fait, M. Calandra et Mme Davidson vont partager un tour.

Monsieur Calandra.

M. Paul Calandra (Oak Ridges—Markham, PCC): Merci, monsieur le président. Merci aux témoins.

J'aimerais d'abord dire que je sais que vous faites du bon travail, alors pardonnez-moi pour certaines de mes questions.

J'aimerais simplement confirmer un point: la loi vous oblige à envoyer un dossier de crédit gratuit par la poste.

Mme Chantal Banfield: Non, ce que je disais, c'est que la loi nous oblige à avoir des bureaux dans certaines provinces, alors il faut avoir un centre sans rendez-vous.

M. Paul Calandra: Je vois, oui. Mais quel rapport cela a-t-il avec un consommateur qui veut avoir un rapport de solvabilité, sans vouloir nécessairement qu'on le lui envoie par la poste? En quoi est-ce le problème du consommateur que vous deviez avoir un bureau quand nous voulons avoir accès à notre rapport de solvabilité, gratuitement, et par voie électronique? Pourquoi m'importerait-il que la loi vous oblige à avoir un bureau? Ce n'est que le prix de faire des affaires, pour vous.

En quoi est-ce que cela me regarderait, en tant que consommateur?

Mme Chantal Banfield: Le problème, pour nous, c'est qu'avec le temps, nous avons constitué une infrastructure qui est déjà en place, alors pour la changer et investir dans d'autres technologies, il nous faut encore assumer les coûts. Par exemple, nous avons investi dans la technologie de RVI — et je sais qu'Equifax l'a fait aussi; il vous est donc possible, pour obtenir une copie de votre rapport, de téléphoner au centre, de confirmer votre identité en ligne, et vous recevez la copie par courrier. La demande est traitée dans les 24 heures, et le courrier envoyé.

M. Paul Calandra: Oui. Mais c'est toujours par courrier. Je peux payer pour le recevoir immédiatement, en tant que consommateur, mais cela me coûte 26 $. Pour une raison quelconque, je dois attendre le courrier parce que vous devez avoir des bureaux dans les provinces. Eh bien, tant pis pour vous. Vous pouvez toujours fermer boutique si ça ne vous plaît pas. C'est ça, la réalité.

Le problème, c'est que ce sont les consommateurs qui pâtissent. Quand vous faites une erreur, que ce soit ou non de votre faute, ou quand une erreur est commise, cela se répercute sur les consommateurs, et il n'est pas facile pour le consommateur de corriger une erreur qui est survenue — parfois sans que ce soit sa faute, à cause de la négligence criminelle de quelqu'un d'autre, ou peu importe — et la seule façon pour nous de le faire gratuitement, c'est d'attendre que vous nous envoyiez quelque chose par la poste, sinon on doit payer. C'est évidemment un gros dilemme, parce que les choses ont évolué depuis 10 ans, alors votre modèle d'affaires, on pourrait le supposer, devrait lui aussi évoluer.

Mme Carol Gray: Je pourrais peut-être ajouter que ce que nous souhaiterions, c'est qu'il y ait un moyen universellement acceptable et accessible, celui du courrier. Ce n'est pas tout le monde qui a accès à un ordinateur, et quand on découvre qu'il peut y avoir eu atteinte à nos renseignements personnels, on a probablement accès à un téléphone. Alors, une bonne solution serait de nous avertir immédiatement par téléphone pour obtenir le rapport dans les 48 heures, parce que si on faisait tout par Internet, qu'arriverait-il des gens — surtout dans les réserves — qui n'ont pas forcément accès à Internet? Alors, en réalité, le courrier — donc le service gratuit — offre un accès universel. Je comprends toutefois ce que vous voulez dire, et il s'agit de faire évoluer notre modèle d'affaires en ajoutant d'autres moyens d'accès économiques.

M. Paul Calandra: Je comprends ce que vous me dites, mais cela me fait penser à une entreprise qui essaie de trouver toutes les excuses du monde pour ne pas fournir aux gens les renseignements dont ils ont besoin. Vous êtes probablement une des seules entreprises qui ait comparu devant le comité pour nous dire que vous avez besoin de vous fier au courrier parce qu'il y a plus de gens qui y ont accès.

Pour être franc, ici même, j'y ai accès. Je suis peut-être différent des autres, mais la plupart des gens ont accès à un téléphone cellulaire. J'imagine même que la plupart des gens qui habitent sur une réserve ont accès à un téléphone cellulaire qui leur fournit également un accès à Internet. Ils pourraient donc télécharger le rapport gratuitement si vous le leur permettiez.

Tout ce que je vous suggère, c'est que les choses changent. Le vol d'identité est devenu un problème qui a pris de l'ampleur, et il n'y a personne qui soit véritablement là pour protéger les consommateurs. De toute évidence, vous travaillez pour les entreprises, mais pas forcément pour les consommateurs. Lorsqu'un consommateur a un problème par rapport à ce que vous avez fait, ou par rapport aux renseignements que vous avez recueillis, et même si ce n'est pas votre faute, il est difficile de changer les choses et il faut payer si l'on veut des changements immédiats.

Je vous dirais qu'il s'agit là d'un des problèmes.

Mais un autre problème ne réside-t-il pas dans le fait que de plus en plus d'entreprises demandent des rapports de crédit? Une partie de votre système pour évaluer les consommateurs est fondée sur le nombre de rapports générés. Si je veux obtenir un téléphone cellulaire, par l'entremise de Rogers, de Bell ou d'un autre fournisseur, je serai assujetti à un rapport de crédit. Nous ferons une enquête de type « mise à jour » à mon endroit.

De plus en plus d'entreprises, et ce, pour des raisons de moins en moins importantes, vous demandent des renseignements, et cela a une incidence sur les cotes de crédit des consommateurs. C'est vous qui générez ces pointages de crédit.

Ne vaudrait-il pas mieux, afin d'éviter de donner plus d'accès aux gens, de limiter le nombre de transactions qu'une entreprise peut utiliser pour vous demander de leur fournir un rapport?

● (1200)

Mme Carol Gray: J'aimerais clarifier quelques points.

Tout d'abord, une entreprise doit être admissible pour devenir membre d'un bureau pour pouvoir avoir accès au rapport. L'entreprise doit avoir une raison légitime ainsi que des protocoles de sécurité en place afin de pouvoir avoir accès aux rapports des consommateurs. C'est mon premier point.

Deuxièmement, chaque fois qu'une enquête est effectuée au sujet d'un rapport de consommateur, cela ne touche pas nécessairement sa cote de crédit. Les pointages sont calculés de diverses façons et pour différentes raisons. Chaque agence d'évaluation de crédit utilisera les pointages différemment. Ainsi, par exemple, les sociétés de télécommunications ne font pas toutes rapport aux bureaux de crédit des renseignements qu'elles ont recueillis.

Bon nombre des prêteurs n'utilisent même pas ces renseignements lorsqu'ils décident d'octroyer un prêt. Alors il ne s'agit pas...

M. Paul Calandra: Mais s'ils examinent un rapport, est-ce que cela ne va pas avoir une incidence sur le pointage que vous octroyez aux consommateurs?

Mme Carol Gray: Pas forcément.

M. John Russo: Pas forcément. Il y a des enquêtes de type « mise à jour », comme vous l'avez mentionné, ou aussi des enquêtes inscrites à la suite d'une demande de crédit. Lorsqu'il s'agit du processus d'approbation du crédit, cela aura une incidence sur votre pointage. Si une enquête est effectuée tout simplement pour gérer votre compte ou pour une autre raison, alors il s'agit d'une enquête de type « mise à jour ».

Mme Tara Zecevic: John, j'aimerais ajouter que les enquêtes similaires sont regroupées. Ainsi, par exemple, si je veux acheter une maison et que je fais une demande d'hypothèque et qu'au cours d'un certain temps, je me rends à plusieurs institutions financières pour faire des demandes afin d'obtenir le meilleur taux possible pour mon hypothèque, ce serait regroupé dans le cadre d'une seule enquête. De plus, les enquêtes ne sont qu'une des variables qu'on utilise dans le calcul du pointage.

M. Paul Calandra: Très bien, mais le nombre de personnes qui ont accès aux enquêtes de type « mise à jour » ou aux enquêtes inscrites à la suite d'une demande de crédit, peu importe comment vous voulez les appeler... Cela donne à plus de personnes un accès aux renseignements que vous avez recueillis, n'est-ce pas? Et cela ouvre la porte à un plus grand nombre de vols d'identité.

Ainsi, si j'appelle Rogers pour obtenir un téléphone cellulaire et que l'agent me dit qu'il doit vérifier auprès de mon bureau, cela donne à une autre personne au téléphone l'occasion d'avoir accès à mes renseignements, et ce, simplement pour obtenir un téléphone cellulaire, alors que je peux peut-être déjà avoir trois ou quatre autres comptes avec Rogers pour ma télévision et avoir une excellente cote de crédit.

En résumé, qui défend les consommateurs? Je ne pense pas que ce soit vous, car vous travaillez pour les entreprises, et c'est correct. Mais qui nous défend lorsque vous faites une erreur? Pourquoi est-ce qu'il devient tellement difficile pour nous de corriger une erreur que vous faites ou que les entreprises font et que vous mettez en oeuvre en leur nom?

Mme Chantal Banfield: Je souhaite répondre à l'une de vos questions au sujet de la communication d'information lorsqu'il y a plusieurs demandes de rapports de crédit.

Vous avez parlé des entreprises de télécommunications. Normalement, l'agent au téléphone qui présente une demande de vérification de crédit ne voit pas votre dossier, qui se trouve dans une banque centrale sécurisée, une espèce de bunker. Il faut une carte magnétique et ses empreintes digitales pour y avoir accès. L'agent au téléphone ne reçoit qu'un oui ou un non.

M. Paul Calandra: Oui, mais quelqu'un...

Mme Chantal Banfield: Il n'obtient que la décision. L'accès à l'information est extrêmement contrôlé. Je ne voulais pas que vous croyiez que n'importe qui peut voir un dossier de crédit.

M. Paul Calandra: J'imagine que si j'avais déjà trois ou quatre comptes auprès de Rogers et que mon crédit était déjà bon, pourquoi ferait-il une énième demande? Est-ce que vous l'autoriseriez à le faire?

Le président: Ces questions sont très intéressantes, mais je dois maintenant vous interrompre. Vous avez largement dépassé votre temps, Paul. Je pense que vous avez en fait établi un nouveau record.

Voilà qui conclut notre première série de questions. Je vais me prévaloir de mon privilège en tant que président pour poser une question. Je ne poursuivrai pas tout à fait sur la même lancée, mais lorsqu'une entreprise vous demande une vérification de crédit, je remarque que vous ne lui envoyez pas la réponse par écrit. Vous ne lui demandez pas d'attendre 48 heures, le temps que ça arrive par la poste.

Deux d'entre vous ont dit que vous appuyez, avec réserve, l'exigence en matière de notification que la loi prévoit mettre en vigueur. Dans quelles circonstances pensez-vous qu'un consommateur n'aurait pas le droit de savoir que son identité a été compromise? Pourquoi avez-vous des réserves quant à cette disposition?

L'un d'entre vous pourrait-il répondre très brièvement?

● (1205)

Mme Carol Gray: Mes réserves n'ont rien à voir avec l'accès à cette information par le consommateur. Cela fait partie d'un modèle d'affaires en évolution. Il faut investir afin de modifier les canaux d'accès.

Le président: D'accord. Peut-être qu'on y reviendra plus tard.

Monsieur Ravignat, vous avez cinq minutes.

M. Mathieu Ravignat (Pontiac, NPD): Merci, monsieur le président.

Cela vous surprendra, mais je partage un grand nombre de préoccupations soulevées par mon collègue d'en face. Je partage aussi son cynisme. Je trouve qu'il est vraiment étrange que l'on doive se battre pour obtenir de l'information de base sur soi-même, information qui est détenue par des entreprises qui semblent vouloir la rendre inaccessible ou difficile d'accès. Cela dit, je sais qu'il y a eu certaines améliorations.

Quoi qu'il en soit, là n'est pas ma question. Je préfère plutôt parler de la situation des Autochtones.

Il y a deux Premières Nations dans ma circonscription. Je serai bref, mais je souhaite néanmoins illustrer mon argument par une anecdote qu'un ami algonquin de la réserve de Kitigan Zibi m'a racontée. Il avait décidé d'acheter un bateau pour sa mère, car elle allait pêcher chaque saison à un endroit qui était assez loin de chez lui. Il gagnait un bon salaire, et un jour, il a acheté un bateau. Il l'a présenté à sa mère comme une surprise. Elle l'a regardé, ébahie, alors il a expliqué que c'était une façon pour elle de se rendre plus rapidement à son lieu de pêche. Elle a répondu, « Mais pourquoi voudrais-je aller plus rapidement? »

Cette histoire illustre qu'il y a une certaine façon de penser en salle de comité, vous y compris, et que l'on parle d'une façon de voir le monde très différente. Afin d'intégrer ces personnes dans un système auquel elles ne souhaitent peut-être pas participer... Et je ne pense pas que ce soit une simple question d'éducation. Je pense que c'est également une question de choix. Je pense qu'il y a des personnes qui connaissent très bien le système et savent ce qu'il représente. Et certaines personnes et communautés font le choix de ne pas y participer.

C'est peut-être parce que les gens s'interrogent de ce qu'il advient de leurs données. Certains d'entre vous travaillent dans le secteur de la vente de données personnelles. La vente de données personnelles sur les membres des Premières Nations est un problème historique car leurs données, qu'elles soient culturelles, linguistiques, artistiques ou autres, sont volées et ensuite vendues afin que des entreprises non autochtones puissent en profiter financièrement.

Je comprends que l'on pense que c'est une bonne chose qu'il faut absolument faire. C'est pourquoi j'applaudis M. Rowe d'avoir évoqué l'importance de tenir des consultations et des discussions approfondies avec les Autochtones sur l'échange de données et sur la façon dont ils peuvent s'en servir afin de créer des communautés dont ils seront fiers.

Cela dit, monsieur Rowe, il est clair que vous avez mené des consultations. Je voudrais savoir quels sujets et quelles préoccupations les collectivités autochtones ont soulevés au cours de ces consultations au sujet de leur intégration au système de crédit.

M. Murray Rowe: C'est une excellente question.

Nous étions récemment à une conférence à Toronto à laquelle plusieurs chefs de bande ont participé, dont la chef Roxane, de Temagami. Nous avons eu une conversation assez longue. Dans nos échanges, ils se sont tout d'abord montrés très hésitants à travailler avec nous. C'était en fait intéressant, car pour des raisons de différence culturelle, on m'avait demandé de ne pas porter de costume et de cravate. Mais j'ai trouvé cette requête intéressante car dans ma culture, je dois porter un costume et une cravate. Je ne leur demande pas de changer de culture, et je ne m'attends pas à ce qu'on me demande de changer la mienne. Si je porte toujours une cravate, je ne vais pas faire semblant d'être ce que je ne suis pas. Je pense qu'il faut justement ce genre d'honnêteté et ce genre de comportements et d'échanges francs.

Nous avons donc eu des échanges très directs et sincères avec eux. Nous avons parlé entre autres de Pic River, où la demande de logements dans la réserve est très forte. Une dame a dû contracter un prêt personnel à un taux d'intérêt de 24 %. Or, tous les représentants de banques présents à la conférence courtisaient les membres des Premières Nations, affirmant qu'ils voulaient faire affaire avec eux. L'un des Autochtones présents, Moses, gestionnaire de logements, leur a répondu ceci: « Mais de quoi parlez-vous? Comment pouvez-vous vous attendre à ce que quelqu'un vous paie 24 % d'intérêt? »

Cela dit, je reconnais que ces institutions affrontent toutes sortes de problèmes, tels que les garanties de prêt ministérielles, qui sont assorties de toutes sortes de formalités administratives pour que les banques puissent approuver un prêt. Or, les Autochtones répètent encore et encore qu'ils veulent avant tout pouvoir acquérir un certain capital afin de le transmettre à leurs enfants et petits-enfants.

Diane Francis vient de publier un livre. Il parle d'un partenariat entre le Canada et les États-Unis. Je ne suis pas pour cette idée, mais elle mentionne qu'en 1776, le Congrès américain a retiré des terres à la Couronne pour les vendre à des particuliers, ce qui a lancé le plus puissant moteur de création de richesse de l'histoire du monde.

C'est fascinant. Le concept de la propriété foncière remonte à plusieurs centenaires. Nous voyons la richesse que cela a créée aux États-Unis pour les collectivités non autochtones. Et maintenant, un grand nombre d'Autochtones se demandent pourquoi ils ne peuvent pas aussi être propriétaires de leur propre terrain et atteindre cette autonomie financière. Mais je pense que l'on commence à comprendre que les banques sont désormais internationales et qu'elles souhaitent avant tout pouvoir consentir des prêts de façon efficiente tout en s'assurant que les risques sont raisonnables.

Je pense que si l'on peut créer des dossiers personnels, on peut réduire la fraude, ce qui tombe sous le mandat de ce comité, mais en plus, nous pouvons débloquer des milliards de dollars en prêts hypothécaires. Mais il faut le faire de façon concurrentielle. Il faut que les taux d'intérêt soient raisonnables. Ce qui motive les collectivités autochtones, c'est l'idée de transmettre leur richesse à leurs petits-enfants, d'avoir une certaine autonomie financière plutôt que de recevoir la charité.

Les réserves reçoivent 14,1 milliards de dollars. C'est bien, mais je pense qu'elles préféreraient être autonomes financièrement et changer leur situation.

● (1210)

Le président: Vous n'avez plus de temps, monsieur Ravignat.

Monsieur Rowe, nous vous remercions.

C'est maintenant au tour des conservateurs. Monsieur Zimmer, vous avez cinq minutes.

M. Bob Zimmer (Prince George—Peace River, PCC): Merci de comparaître devant notre comité. J'ai deux questions.

Je pense qu'un grand nombre de Canadiens ont l'impression que les pirates sont des petits jeunes de 17 ans qui sont forts en informatique et qu'ils leur volent leur identité pour s'amuser.

Mais qui sont réellement les nouveaux pirates? Qui sont ces groupes du crime organisé? Sont-ils au Canada? S'agit-il des Hells Angels? Pourriez-vous, s'il vous plaît, nous décrire un pirate typique?

M. John Russo: Si vous parlez du hacktivisme, il y a diverses organisations. Il y a des nations qui attaquent d'autres nations. Mais il y a aussi le crime organisé. Vous avez des gangs qui attaquent des particuliers pour obtenir leur information personnelle et créer de nouvelles identités. Enfin, il y a également les voleurs d'occasion: les gens qui trouvent un portefeuille ou une carte d'identité dans la rue et qui commettent un crime isolé. Il ne s'agit pas d'un groupe en tant que tel qui se livre au piratage ou au vol d'information personnelle. Il y a toutes sortes d'acteurs.

● (1215)

Mme Tara Zecevic: J'ajouterais que l'on constate également une certaine collaboration entre différents groupes du crime organisé. Certains groupes sont spécialisés dans le vol d'identité et d'autres, dans la création de cartes bancaires. Un troisième groupe se chargera de se rendre aux guichets automatiques pour retirer de l'argent. Il y a eu de nombreux exemples d'une telle collaboration, et ces groupes fonctionnent comme s'il s'agissait tout simplement d'un commerce. Pourtant, s'ils mettaient leurs talents au profit de causes légitimes, ils pourraient accomplir de grandes choses. On constate cette collaboration à l'échelle internationale.

M. Bob Zimmer: Est-ce que ce sont des gangs qui se livrent à ce genre d'activité? Les talibans? De qui parlons-nous? J'imagine qu'il y a deux sortes de pirates, les Canadiens et les étrangers? Vous avez parlé de pirates qui sont en fait des États.

Qui sont ceux qui nous attaquent et nous volent notre identité le plus souvent?

M. John Russo: La majorité d'entre eux sont des groupes du crime organisé canadiens.

M. Bob Zimmer: D'accord.

S'agit-il de groupes du crime organisé à Vancouver, qui volent des cartes ou de l'information?

Oui, d'accord. Je voulais tout simplement savoir qui sont les principaux pirates.

Vous avez également parlé d'organisations terroristes. Pourriez-vous nous dire quels groupes terroristes ont commis des vols d'identité afin de financer leur régime?

M. John Russo: Je ne pourrais pas vous dire quelles organisations terroristes sont en cause exactement. Lorsque nous collaborons avec les organismes d'application de la loi, nos services de sécurité...

M. Bob Zimmer: Vous savez que ces crimes sont commis, mais vous ne savez pas qui est responsable.

M. John Russo: C'est exact. Nous savons tout simplement que ces crimes sont commis.

M. Bob Zimmer: Je vois.

D'autres témoins nous ont parlé de l'attribution d'un numéro d'assurance sociale aux enfants à la naissance. Monsieur Russo, je pense que c'est vous qui avez dit que ce sont ces numéros qui font l'objet de piratage. On nous a aussi dit qu'étant donné que ce crime peut rester impuni pendant de nombreuses années, quand on se rend compte de ce qui s'est passé, il est trop tard.

Pouvez-vous nous en expliquer la chronologie? Quand le numéro est volé, à quoi peut-il servir? Est-ce qu'il pourrait être... Je n'essaie pas de dire aux criminels comment faire, et je ne voudrais pas non plus que vous le leur disiez. Est-ce qu'on devrait vérifier le rapport de solvabilité de nos enfants quand ils ont 10, 15, puis 20 ans? Est-ce quelque chose qu'on devrait...

M. John Russo: Malheureusement, les mineurs n'ont pas de rapport de solvabilité, ce qui permettrait de protéger ces numéros.

Par exemple, à Equifax, nous avons une base de données de numéros d'assurance sociale où l'on pourrait saisir les données de mineurs, notamment un numéro d'assurance sociale, qui ont été volées. Quand un fraudeur essaie d'utiliser les renseignements de votre fille ou de votre fils mineur, l'institution reçoit un avertissement que le numéro a été volé ou perdu. Comme les enfants n'ont pas de rapport de solvabilité, c'est beaucoup plus difficile.

En quelques mots, l'établissement d'identité — et Tara, qui travaille dans le domaine de la fraude avec les associations qui luttent contre la fraude, pourra vous expliquer plus longuement — commence avec un numéro d'assurance sociale, qui établit l'identité ou l'identité fictive. Avec ce numéro, on peut, disons, faire une demande de téléphone cellulaire et recevoir le matériel. Ensuite, le matériel est annoncé sur Kijiji, par exemple, et quelqu'un vous rencontre près d'une station de métro pour vous le vendre. C'est monnaie courante. Ces identités sont des crimes sans visage et n'existent pas. Les fraudeurs commencent simplement, établissent ce crédit, peut-être pour ouvrir un compte de banque et obtenir un petit prêt, ou recevoir des cartes de crédit. Il ne leur faut qu'une ou deux pièces d'identité. Quand votre enfant, plusieurs années après, fait une demande de crédit, il se rend alors compte que son numéro d'assurance sociale a été compromis et utilisé à maintes reprises.

M. Bob Zimmer: Je vous remercie.

La vice-présidente (Mme Patricia Davidson (Sarnia—Lambton, PCC)): Je vous remercie, monsieur Zimmer.

Nous cédons la parole à Mme Borg. Vous avez cinq minutes.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

J'aimerais revenir sur les questions de M. Calandra. C'est un peu difficile à comprendre. Cependant, je comprends qu'il y ait des restrictions financières.

Je ne sais pas si vous pouvez répondre maintenant à ma question ou si vous aurez besoin de nous faire parvenir la réponse plus tard, mais voici ce que j'aimerais savoir. Si je fais une demande d'obtention de dossier de crédit, combien cela coûte-t-il en ressources à vos deux organismes respectifs pour répondre à cette demande?

[*Traduction*]

M. John Russo: Nous pourrons vous faire parvenir ces chiffres.

Une voix: Ce serait le même prix pour les deux.

[*Français*]

Mme Charmaine Borg: Je ne sais pas si nous avons un processus par lequel vous pourriez communiquer cette information au greffier, mais si c'était possible, ce serait intéressant. Merci beaucoup.

Une autre préoccupation a été soulevée par certains témoins du domaine universitaire. Ils ont dit qu'ils avaient de la misère à obtenir des données ou des renseignements sur certaines choses. Je sais que ce n'est pas nécessairement votre mandat de documenter tout cela, mais avez-vous déjà collaboré à des recherches? Pouvez-vous partager des données avec des universitaires? Je parle ici de données démographiques ou de données sur des problèmes récurrents, par exemple.

● (1220)

[*Traduction*]

M. Todd Skinner: Du point de vue de TransUnion — je soupçonne qu'Equifax pense de même —, nous serions prêts à partager les renseignements avec un organisme. La question revient à savoir comment prévenir autant que possible la fraude. Nous essayons de communiquer avec les organismes gouvernementaux qui délivrent des pièces d'identité et les amener à partager ces renseignements par notre intermédiaire, comme canal de communication, pour vraiment tenter de prévenir la fraude autant que possible. Je ne sais pas si ce canal devrait servir à transmettre ces renseignements, que ce soit votre comité ou à titre ponctuel, mais comment pourrait-on procéder à l'avenir? L'échange d'information pour mieux comprendre l'ampleur du problème, c'est... Nous y sommes très favorables.

[*Français*]

Mme Charmaine Borg: Merci. On nous a présenté cela comme étant une solution possible. Évidemment, si tous ceux et celles qui jouent un rôle là-dedans travaillent ensemble, les résultats seront meilleurs.

Par ailleurs, vous avez dit qu'entre 25 et 30 % des Canadiens demandaient à avoir accès à leur dossier de crédit. Pour ma part, je pense qu'un accès en ligne serait plus facile, mais pensez-vous à d'autres moyens par lesquels on pourrait encourager les consommateurs à demander à accéder à leur dossier de crédit?

[*Traduction*]

M. John Russo: Par exemple, nous allons dans les écoles, dans le cadre des programmes de réussite des jeunes, pour enseigner aux jeunes Canadiens de façon à ce que lorsqu'ils peuvent accéder au crédit, ils savent ce qu'est un rapport de solvabilité, comment le lire et ce qui influe sur leur cote de solvabilité. Nous avons déjà fait pas mal de choses dans le cadre de ce programme, pour jeter les bases nécessaires pour les jeunes Canadiens.

[*Français*]

Mme Charmaine Borg: Monsieur Skinner ou madame Banfield, aimeriez-vous ajouter quelque chose?

Me Chantal Banfield: Nous avons beaucoup d'information sur notre site Web. Nous avons travaillé notamment avec les services de police ainsi qu'avec plusieurs agences en vue de publier cela. Nous faisons également des campagnes dans les écoles.

Je pense que la commissaire à la protection de la vie privée du Canada pourrait inclure plus d'information à l'intention des consommateurs dans sa trousse d'outils. À mon avis, beaucoup de consommateurs consultent plus particulièrement le site Web de la commissaire pour obtenir de l'information quand ils sont victimes de fraude ou d'un autre problème de ce genre.

Mme Charmaine Borg: Merci.

Madame Zecevic, vous souhaitez ajouter quelque chose?

[*Traduction*]

Mme Tara Zecevic: Je voulais seulement ajouter que je siège également au conseil d'administration de Credit Canada Debt Solutions, qui travaille avec les consommateurs qui sont endettés. Comment peut-on les aider à consolider leurs dettes? L'éducation et la littératie financière sont d'importants éléments de la solution.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Est-ce qu'il me reste du temps?

[*Traduction*]

La vice-présidente (Mme Patricia Davidson): Il ne vous reste que deux secondes, alors je crois que nous nous en tiendrons là.

Mme Charmaine Borg: Merci.

La vice-présidente (Mme Patricia Davidson): C'est maintenant au tour de Mme O'Neill Gordon.

Mme Tilly O'Neill Gordon (Miramichi, PCC): Je vous remercie, madame la présidente.

Je tiens à remercier les témoins d'être ici aujourd'hui. Vous nous avez donné de quoi réfléchir.

Ma première question s'adresse à M. Russo. Vous dites, dans vos notes, que « Le fait est que les criminels n'arrêteront pas d'évoluer et que nos lois, notre sécurité et nos tactiques de prévention doivent changer en même temps que lesdits criminels se raffinent ». Pourriez-vous nous expliquer la nature des changements que nous devons apporter? De quelle façon pouvons-nous aider les gens à mieux comprendre ce qui se passe autour d'eux?

Je ne m'adresse pas seulement à M. Russo. Vous pouvez tous répondre, parce que vous avez tous de bonnes idées. Cependant, il faut absolument changer les choses, puisque la situation évolue.

M. John Russo: Pour commencer, le projet de loi S-4 est une bonne initiative puisqu'il donne aux consommateurs un peu plus de pouvoir pour agir de façon proactive afin de savoir quand leurs renseignements personnels ont été compromis. Donc, le signalement obligatoire des violations de la protection des renseignements, une mesure en vigueur dans de nombreux États américains... On peut espérer que ce projet de loi sera adopté au troisième tour, pour instaurer ce signalement obligatoire de façon à ce que les personnes dont les renseignements ont été compromis, perdus ou volés, en soient informés. La plupart du temps, les institutions sont portées à se cacher la tête dans le sable et à ne rien faire, ou si elles ne sont frappées d'aucune amende ou pénalité, elles sont moins susceptibles de faire quoi que ce soit. C'est un élément clé des modifications législatives.

Carol.

● (1225)

Mme Carol Gray: Pour poursuivre dans la même veine que ce que disait John, il est important d'imposer des peines plus sévères, car on a l'impression que c'est un crime sans visage, un crime inoffensif. Il n'y a pas de véritable victime au bout du compte. Mais en fait, il y en a, et comme on le disait tout à l'heure, les coûts sont énormes. Les amendes devraient évidemment concorder avec les coûts pour la société.

M. Todd Skinner: Je voudrais dire une dernière chose. Nous avons beaucoup parlé des infractions qui sont perpétrées dans les petites et moyennes entreprises, qui comptent pour un fort pourcentage de l'ensemble des infractions. Il faudrait vraiment offrir un soutien pour les sensibiliser à la situation et les aider à comprendre, sous l'angle d'un protocole de sécurité, ce qu'il faut savoir pour prévenir ce genre d'infraction. Je suis d'accord avec John et Carol qu'il faut modifier les lois et les conséquences qu'elles prévoient.

M. Murray Rowe: Je travaille beaucoup avec les services de police et je les trouve très déterminés à régler ces problèmes. Mais s'il y a une chose qui pourrait être utile... Quand on investit peu pour régler un problème, on n'aura que de piètres résultats. Donc, ne serait-il pas intéressant de pouvoir faire un suivi du nombre d'agents et du financement que reçoivent des organisations comme la GRC? On peut bien avoir des gens déterminés à trouver une solution, mais si on coupe l'herbe sous le pied des services, on n'obtiendra que de piètres résultats.

Alors au lieu d'être prescriptifs, d'exiger des détails... et de dire à des enquêteurs qui sont déjà très professionnels, « Pourquoi ne pas chercher la source des problèmes? », je pense que le financement est véritablement un facteur déterminant. S'il y a plus de crimes qui font l'objet d'enquêtes, il faudra permettre la tenue de ces enquêtes. À New York, quand on parle de la théorie des fenêtres brisées qu'ont appliquée Giuliani et d'autres, même pour les plus petits crimes, il est étonnant de voir à quel point la criminalité a baissé. Peut-être qu'on pourrait commencer à appliquer cette théorie pour régler les problèmes moins complexes. Il faut toutefois des données empiriques et déterminer combien d'argent est véritablement dépensé plutôt que de demander simplement, « Êtes-vous déterminés à trouver une solution? ».

M. Todd Skinner: Est-ce que je pourrais ajouter une chose? Je pense qu'on peut s'attaquer à ce problème par divers moyens. Il vaut toutefois mieux prévenir que guérir. Quand on pense au nombre d'infractions qui diminuent, mais au nombre de victimes potentielles qui augmente... La technologie progresse plus rapidement que nous. Tout est dans la façon dont on entrepose les données. Il devient moins coûteux d'y accéder. Cette technologie permet d'entreposer beaucoup de données. Alors au lieu d'avoir 100 000 dossiers, c'est un million, et bientôt, ce sera 100 millions.

Je veux seulement insister sur le fait qu'en essayant de résoudre ce problème de vol d'identité en amont, on peut économiser beaucoup de temps et d'efforts. Cela permettrait aussi d'investir les fonds et les ressources que nous avons pour résoudre les crimes en col blanc dans autre chose qui pourrait vraiment faire une différence dans nos collectivités. Alors il faudrait investir le plus possible de ressources dans la prévention pour résoudre ce problème.

Mme Tilly O'Neill Gordon: J'avais une autre question à poser... mais vous avez parlé de l'éducation et de la façon dont on pourrait éduquer plus de gens. Je sais que vous allez dans les écoles, mais actuellement, il y a un segment de la population qui n'a pas reçu cette information à l'école, et ce sont les gens qui sont aussi très vulnérables. Je ne sais pas comment on peut faire passer le message. J'entends parler de deux types de protection. Je me demande combien... Même ma propre famille ne saurait pas que ces protections existent. Ce serait important de les faire connaître. Il y a autre chose, au sujet d'un montant pour obtenir un gel du crédit. C'est le genre de choses qui, je ne sais pas... Je voudrais donc savoir comment on peut aider ces gens-là.

Mme Tara Zecevic: Oui, c'est pourquoi j'ai parlé tout à l'heure de Credit Canada Debt Solutions, un organisme sans but lucratif. Vous pouvez voir ses panneaux publicitaires sur les autobus et ses divers messages publicitaires. Il fait de la publicité pour aider les consommateurs à mieux comprendre les données financières. Il a des conseillers qui peuvent aider les Canadiens, s'ils ont pris la mauvaise voie, à se remettre sur pied et à s'assurer qu'ils prennent le contrôle de leurs finances.

● (1230)

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

Vous voulez ajouter quelque chose, très rapidement?

Mme Carol Gray: Je pense que les bureaux auront davantage de possibilités de travailler en partenariat avec les institutions financières pour faire passer ces messages.

La vice-présidente (Mme Patricia Davidson): D'accord, merci.

Monsieur Ravignat, vous avez cinq minutes.

[*Français*]

M. Mathieu Ravignat: Merci, madame la présidente.

Il est tout à fait normal que vos entreprises visent à faire des profits; il n'y a rien de mal à cela. Cependant, il y a un problème lorsqu'il y a une contradiction entre le désir de faire des profits et celui de protéger les consommateurs et les intérêts des Canadiens. Une des solutions est de légiférer, mais les compagnies pourraient aussi prendre des initiatives, créer des codes d'éthique et de valeurs et mettre en place de bonnes pratiques.

J'ai entendu dire que cela se faisait à un certain degré, mais il y a tout de même une contradiction entre facturer certains services de base dans le cas d'un vol d'identité et éliminer le problème du vol d'identité.

Qu'est-ce qui vous incite financièrement à vous pencher sérieusement sur le problème du vol d'identité?

[*Traduction*]

M. John Russo: Je vais y répondre.

Tout d'abord, à titre de précision, pour une véritable victime de fraude, il ne coûte rien d'inscrire une alerte à la fraude à son dossier chez Equifax. Donc, pour une victime de fraude, c'est gratuit. Je pense que c'est aussi le cas chez TransUnion. Donc, on ne fait pas payer les gens qui ont fait l'objet de fraude. Si vous voulez prendre des mesures proactives, il y a des lois, dont j'ai parlé, au Manitoba et en Ontario, qui permettent d'agir de façon proactive et d'indiquer une alerte à la fraude à votre dossier pour demander qu'on communique avec vous à un certain numéro avant d'octroyer du crédit en votre nom.

Il y a toutefois une dichotomie entre le fonctionnement d'une entreprise et la capacité de gagner sa vie, en ce qui concerne les activités que nous menons et les consommateurs qui tentent d'accéder à de l'information. Il y a des coûts associés à tout cela. Je reviens à l'exemple des États-Unis, où ils ont droit à un signalement par année, par personne, à n'importe lequel des trois bureaux qu'ils ont là-bas. Il y en a trois au Canada, avec Experian.

Au Canada, on peut accéder gratuitement à son dossier 365 jours par année, alors il n'est même pas nécessaire de s'inscrire à un produit de surveillance. Je dis toujours aux gens de téléphoner ou d'envoyer une demande par la poste — c'est plus facile de téléphoner — pour pouvoir accéder à son dossier gratuitement 365 jours par année. Donc, pour ce qui est du produit de surveillance, je donne l'information et le moyen d'y accéder.

[*Français*]

M. Mathieu Ravignat: Par contre, il y a aussi une contradiction entre la promotion de cette possibilité et la promotion des outils de surveillance. Autrement dit, si on vend un produit de surveillance, on ne va pas informer le public qu'il aura accès à ses dossiers gratuitement.

[*Traduction*]

M. John Russo: Je pense que les consommateurs canadiens sont conscients du fait qu'ils peuvent accéder à leurs dossiers par l'entremise de l'IMOA, de notre site Web ou un centre sans rendez-vous. L'information existe donc. Elle est affichée sur notre site Web, Equifax.ca, pour informer les consommateurs. S'ils veulent, comme vous dites, cet accès instantané en temps réel, ils peuvent l'avoir à frais modiques.

Mme Carol Gray: Je pense que c'est aussi une question de donner un choix aux consommateurs. La surveillance assure un degré additionnel de protection. Comme bien des consommateurs, je m'abonne à ce service parce que j'aime aussi me tenir au courant de ma cote de crédit. Cela vient avec le service. J'aime aussi savoir que je suis protégée si je perds mon portefeuille. Alors il s'agit seulement de donner le choix aux consommateurs, et nous avons l'obligation d'expliquer ces options aux consommateurs et de nous assurer qu'ils peuvent faire un choix éclairé.

M. John Russo: Ce que je ne pense pas... Peut-être que M. Skinner peut en parler.

M. Todd Skinner: J'ajouterais peut-être que ce n'est pas seulement une question de surveillance, mais de gestion, et qu'il faut comprendre son crédit et ce qui se passe avec le dossier de crédit. Ainsi, quelle incidence peuvent avoir les fluctuations des soldes sur la cote?

La surveillance du crédit, bien qu'il s'agisse de surveiller le crédit, n'est en fait qu'un outil pour aider les gens à gérer leur crédit dans leur quotidien, quand ils font des achats, que ce soit une voiture ou pour une hypothèque. Ils peuvent ainsi mieux gérer leur crédit.

● (1235)

M. Mathieu Ravignat: La vente de ces produits de surveillance, si vous deviez faire une approximation de la part qu'elle joue dans votre marge de profit, est-elle mineure comparativement à d'autres activités?

Mme Carol Gray: Très mineure.

M. Mathieu Ravignat: Est-ce que vous offrez ce service dans l'optique de recouvrer des coûts, ou est-ce qu'il génère des recettes?

Mme Carol Gray: Il génère des recettes, mais très peu.

M. Mathieu Ravignat: C'est donc une très petite partie de vos activités. C'est intéressant.

Je vous remercie. Je crois que c'est tout.

Le président: Votre temps est écoulé, de toute façon, Mathieu.

C'est maintenant au tour du Parti conservateur. Laurie Hawn, vous avez la parole.

L'hon. Laurie Hawn: Merci beaucoup, monsieur le président.

J'ai une question très précise à poser, puis je céderai la parole à M. Calandra.

Pour revenir à ce que nous disions au sujet de l'enregistrement du numéro d'assurance sociale d'un enfant, nous avons tout récemment ouvert un compte de régime d'épargne-études pour notre toute nouvelle petite-fille. Je pourrai vous montrer des photos plus tard. Si son numéro d'assurance sociale devait être compromis à un moment donné, est-ce qu'une alerte apparaîtra dans le système pour signaler qu'un numéro d'assurance sociale reconnu est lié à un compte? Est-ce que ce serait indiqué à quelque part dans le système?

M. John Russo: Vous pourriez appeler Equifax pour faire entrer ces données dans notre base de données si elles ont été compromises. Vous pouvez le faire de façon proactive si vous savez qu'elles ont été compromises ou utilisées.

L'hon. Laurie Hawn: Donc, je pourrais appeler l'un des organismes et demander d'enregistrer ce numéro d'assurance sociale, et même si ce n'était pas à toute épreuve, je suppose ce serait quand même un élément de protection.

M. John Russo: Ça pourrait aider.

M. Todd Skinner: Il y a une chose dont je n'ai pas parlé et dont nous nous sommes entretenus à l'interne, et c'est la création d'un numéro d'assurance sociale pour un enfant, la création d'une base de données où, plutôt que d'enregistrer un numéro quand il a été compromis, on pourrait enregistrer le numéro d'assurance sociale de l'enfant au moment d'ouvrir un compte REEE. Nous aurions ainsi tous deux les renseignements, ce qui nous permettrait vraiment de prévenir la fraude. L'utilisation du numéro d'assurance sociale des enfants a toujours présenté moins de risques quand on pense à toutes les autres possibilités, mais il y aurait moyen de prévenir le problème.

L'hon. Laurie Hawn: Oui. Vous avez un numéro d'assurance sociale qui ne pourra pas servir avant 15 ou 20 ans, alors il me semble que ces numéros seraient très attrayants pour ceux qui veulent en abuser.

M. Todd Skinner: Oui, et il sera certainement très possible de collaborer sur ce plan, en tant qu'industrie.

L'hon. Laurie Hawn: Je vous remercie.

M. Paul Calandra: Je suis désolé, je sais que j'ai été un peu dur avec vous, mais j'apprécie le travail que vous faites. C'est un peu un défi, tant pour nous que pour vous.

Monsieur Skinner, vous avez dit qu'il était important de partager l'information. Vous avez dit que ça coûte beaucoup d'argent, et que le gouvernement et les organismes devraient échanger plus d'information. Mais est-ce que l'inverse ne serait pas aussi vrai? Quand on complique le partage de l'information, il est plus difficile pour le consommateur de s'apercevoir qu'il a fait l'objet de fraude.

M. Todd Skinner: Le but du partage d'information, c'est de nous aider à prévenir autant que possible la fraude. Je crois qu'il en serait de même pour Equifax. Nous avons de multiples degrés de détection de la fraude en ce qui a trait aux services financiers. Que ce soit le dispositif qu'on utilise pour une ouverture de session, les renseignements qu'on fournit dans la demande ou les questions qu'on pose pour l'authentification de votre identité, plus on a de données sur vous dans l'entrepôt de données, mieux on est en mesure de prévenir le problème.

Pour ce qui est du partage de ces données — cela revient à ce que disait Carol tout à l'heure —, nous sommes assujettis à des règles très strictes en ce qui concerne ceux avec qui on peut partager l'information, et les vérifications des références qu'on fait sur ces organisations quand on partage les renseignements. Quand on présente les renseignements à ces institutions, ce n'est pas seulement qu'un dossier non hiérarchique de l'agence d'évaluation du crédit. On peut demander de répondre par un simple oui ou non. Alors je comprends ce que vous dites, quand vous parlez de couteau à deux tranchants.

Nos deux organisations prennent très au sérieux la gestion des données. Donc, la question est de savoir jusqu'où l'on doit partager l'information? On pense, à la lumière de la quantité de données qu'on a et de toutes les fraudes qui sont commises, que nous avons encore beaucoup de pain sur la planche, et l'accès à cette information pour prévenir la fraude revêt une importance d'autant plus grande.

M. John Russo: Par exemple, un élément pertinent, ce sont les modifications à la LPRPDE que propose le projet de loi S-4 et qui consistent à éliminer les organismes d'enquête. Cela aiderait les deux organisations à collaborer avec tous les membres de l'industrie financière pour prévenir la fraude. On ne serait pas limité à celles qui se sont enregistrées et qui ont été accréditées comme organisme d'enquête. Le partage de l'information pourrait se faire entre toutes les agences d'évaluation du crédit et les établissements de crédit.

● (1240)

M. Paul Calandra: Ce qui m'intéresse le plus toutefois, c'est le partage entre les consommateurs et... Vous vous faites payer par les institutions financières parce que vous les aidez à protéger leurs investissements, à s'assurer que les emprunteurs présentent un faible risque. Mais je constate que les choses ont changé... Et bien évidemment, le vol d'identité est devenu un énorme problème depuis quelque temps.

L'un des grands problèmes que l'on constate, c'est que les consommateurs, à tort ou à raison, qu'ils le croient ou non, ont l'impression d'avoir un accès limité aux dossiers que vous tenez sur eux, et que cela contribue à augmenter le vol d'identité. Ce n'est que lorsque la demande d'une personne est rejetée à cause d'un problème avec son dossier qu'elle apprend que son identité a été compromise.

Est-ce qu'un accès simplifié aux dossiers que vous tenez sur les consommateurs...? Je sais que cela changerait votre modèle d'affaires, mais si l'on avait accès plus facilement, plus rapidement et plus fréquemment aux renseignements que vous détenez sur nous, ne serait-il pas plus facile de lutter contre le vol d'identité?

Mme Carol Gray: Je pense que si vous alliez plus à la source, c'est — nous en avons déjà parlé — une question d'éducation et de sensibilisation.

La question de l'accès n'est pas vraiment un problème dans l'esprit des consommateurs s'ils ne pensent même pas à accéder à leurs dossiers.

M. Paul Calandra: Mais n'est-ce pas un problème? C'est un problème.

Mme Carol Gray: Ça revient à l'éducation.

M. Paul Calandra: Et quand ils veulent y accéder, vous les faites payer.

Mme Carol Gray: Non, pas toujours. Cela dépend de...

M. Paul Calandra: De façon générale...

Je viens de consulter le site Web d'Equifax, qui m'offrait l'accès gratuit à mes données de crédit. C'était gratuit pour 30 jours, et ensuite c'était 14,95 $, sans parler... Tout ça, je l'ai su en quelques secondes. C'est peut-être enfoui quelque part sur votre site.

Mais n'est-ce pas aussi une partie du problème? Vous recueillez des renseignements auprès des gens. Les décisions que vous prenez sont fondées sur ce que les gens vous disent. Je sais que ce n'est pas vous qui décidez sans raison que quelqu'un n'est pas solvable. C'est fondé sur ce que font les consommateurs et nous avons une responsabilité à assumer. Je le comprends.

Vous ne prenez pas ces décisions. Ce sont des renseignements que des gens vous ont transmis, que vous versez dans un dossier, mais ensuite, ils n'y ont pas accès. Pour une raison ou une autre, les consommateurs ont l'impression de ne pas y avoir accès, et quand ils veulent y accéder, ils doivent remplir un formulaire, l'envoyer par la poste, aller à l'un de ces bureaux que vous n'aimez pas avoir, ou téléphoner et attendre une réponse par courrier, ou encore payer 23 $ pour vérifier qu'ils ne se sont pas fait avoir par quelqu'un qui a volé leur identité. Même alors, il faut remplir un rapport et l'envoyer, et c'est vous qui prenez la décision finale.

Comment pouvez-vous expliquer que c'est ce que les consommateurs veulent?

Le président: Monsieur Calandra, je crois que nous devrons dire que c'était davantage une observation qu'une question, puisque votre temps est écoulé. Peut-être que s'il reste une minute à la fin, vous pourrez faire une dernière remarque.

Je regrette, mais je dois passer à l'intervenant suivant. La parole est à Scott Andrews, du Parti libéral.

M. Scott Andrews: Ne vous inquiétez pas, monsieur le président, je vais poursuivre dans la même veine, car je ne comprends pas moi non plus.

Monsieur Russo, vous dites que c'est gratuit pour une victime de fraude véritable. Mais on est déjà une victime. Est-ce qu'il ne s'agit pas de prévenir la victimisation? Ce que je ne comprends pas, et je pense que vous l'avez dit plus tôt... Je suppose que nous nous en prenons aussi à vous, à TransUnion, mais je pense que c'est une lame à deux tranchants.

Vous dites que pour les services de surveillance du crédit, c'est 5 $.

M. John Russo: Pour une alerte, c'est 5 $.

M. Scott Andrews: Cinq dollars pour une alerte. Pour combien de temps?

M. John Russo: Pour six ans.

M. Scott Andrews: C'est donc pour six ans.

Donc, c'est 5 $, moins d'un dollar par année. Un timbre coûte moins d'un dollar, bon sens. Pourquoi est-ce qu'on ne pourrait pas...? Je suppose qu'une alerte n'est qu'un algorithme dans le programme informatique qui... Un instant. Expliquez-moi comment serait déclenchée une alerte, et pourquoi vous ne voudriez pas mettre en garde le consommateur dans tous les cas?

M. John Russo: Il y a une différence entre l'alerte pour le consommateur, et c'est la surveillance du crédit, et l'alerte pour le membre qui extrait le dossier.

L'alerte de 5 $ est légiférée au Manitoba et en Ontario, et nous offrons ce service partout au pays. Quand une institution extrait un dossier, elle est autorisée à le recevoir de façon automatisée. Elle recevrait une alerte d'Equifax qui dirait quelque chose du genre, « Veuillez communiquer avec John Russo à tel numéro avant d'octroyer le crédit ».

En vertu de la loi, l'institution doit alors prendre des mesures raisonnables pour s'assurer qu'elle fait bel et bien affaire avec John Russo et non pas avec John Fraudeur, qui prétend être moi. C'est prévu dans la loi.

M. Scott Andrews: C'est une alerte. Il ne s'agit pas là de surveillance.

M. John Russo: Il s'agit d'une alerte, pas d'une surveillance. Il s'agit d'une alerte à 5 $.

La surveillance du crédit, ce qui coûte moins cher qu'une tasse de café par jour, est un service proactif payant. À moins d'être victime d'une atteinte à ses renseignements personnels et à moins que la société ne paie pour ce service, un consommateur peut payer pour ce service sur une base mensuelle pour avoir la certitude que ceux qui ont accès à son dossier sont autorisés à le faire — je me sers toujours de l'analogie de l'empreinte digitale, c'est-à-dire que si je touche à votre dossier ou si j'y accède, j'y laisse une empreinte digitale. Qu'il s'agisse de demandes de type « mise à jour » ou d'interrogations inscrites à la suite d'une demande de crédit, vous savez si quelqu'un a accédé à vos dossiers. Étant donné que vous recevez des alertes en temps réel, vous pouvez dire: « Attendez une minute, je ne fais pas affaire avec cette banque. Pourquoi sont-ils en train d'examiner mon dossier? » Vous pouvez appeler Equifax. Vous pouvez appeler la banque. Vous pouvez en fait appeler tous ceux qui ont eu accès à votre dossier.

● (1245)

M. Scott Andrews: Je sais que vous demandez aux gens de payer des frais mensuels. Je crois qu'un grand nombre des membres du comité pensent que vous devriez le faire gratuitement pour le consommateur. Je crois que c'est de là que vient notre frustration, car lorsque vous dites, « Laissez l'entreprise payer si vous êtes victime d'une infraction aux données », souvent, nous ne savons pas que nous sommes victimes d'une atteinte à nos renseignements personnels avant qu'il ne soit beaucoup trop tard.

Mme Carol Gray: Le service de surveillance nous coûte cher. Nous accédons à des millions de fichiers commerciaux qui nous sont envoyés électroniquement tous les jours. Il faut les télécharger, les parcourir et cibler si quelqu'un veut bénéficier de la surveillance. Les services informatiques coûtent cher. C'est pour cette raison qu'il s'agit d'un service payant.

M. Scott Andrews: Todd, désirez-vous intervenir?

M. Todd Skinner: Quand il s'agit de surveillance du crédit, et je reviens à ce que j'ai dit plus tôt, il n'y a pas que la surveillance. L'outil de surveillance du crédit tel qu'il est vendu s'accompagne également d'un processus d'éducation, d'un processus de gestion. Encore une fois, j'ai mon dossier de crédit. Je reçois un courriel pour m'aviser qu'il n'y a rien de nouveau, mais j'y ai toujours accès pour voir ce qui se passe, si les chiffres changent, les cotes de crédit changent — tous les éléments qui sont importants pour surveiller le crédit.

Je suis d'accord avec Carol pour dire que les gens pensent que quand c'est informatisé, c'est automatisé... mais vous devez traiter des centaines de millions de transactions tous les mois, et cela coûte cher. Ensuite, il y a le centre d'appels pour venir en aide à ces clients. Souvent, lorsqu'il y a des alertes de fraude... et je sais que nous parlons ici d'un accès en ligne. L'autre chose que je tiens à souligner, c'est que lorsque vous avez un client qui appelle pour signaler une fraude, tous ces renseignements se trouvent peut-être sur le site Web, mais la personne a toujours besoin de parler à quelqu'un. Elle veut parler à quelqu'un pour qu'il la rassure sur ce qui s'est passé, car elle ne tient pas à rester dans l'ignorance.

Il y a l'aspect... Nous tournons à perte avec les alertes de fraude. Je sais qu'elles coûtent 5 $, mais lorsque vous parlez à quelqu'un et que vous essayez de lui expliquer ce qui s'est passé et ce qu'il devrait chercher, vous perdez de l'argent dans le processus.

Le président: Scott, j'espère que vous ne vous apprêtiez pas à conclure par une grosse question.

J'ai bien peur que notre temps soit écoulé, et nous avons également terminé nos séries de questions. Je suis heureux que tout le monde ait eu la chance de prendre la parole deux fois.

Nous allons remercier nos témoins d'Equifax, de Forrest Green et de TransUnion, qui ont grandement contribué à notre étude sur le vol d'identité.

Merci à vous tous.

Je tiens à aviser les membres du comité que jeudi, nous recevrons un groupe de témoins très intéressant. Nous recevrons des représentants de la Banque Toronto-Dominion, de la Banque Royale, de la CIBC, de la Banque de Montréal et de la Banque Scotia, sans l'Association des banquiers. Si vous pensez que ces gens-ci ont passé un mauvais quart d'heure, cela vous donne une idée de ce qui nous attend jeudi prochain.

Quoi qu'il en soit, je remercie tout le monde. Voilà qui met fin à notre réunion.

La séance est levée.