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 081 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 4 décembre 2017

Président

M. Bob Zimmer

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

Le lundi 4 décembre 2017

● (1530)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare ouverte la 81e séance du Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique de la 42e législature, première session.

Conformément au sous-alinéa 108(3)h)(vii) du Règlement, nous tenons une séance d'information avec Equifax Canada.

Nous recevons John Russo et...

J'aimerais vraiment que vous prononciez votre nom avant que j'essaie de le faire.

Mme Antonietta Di Napoli (directrice, Opérations mondiales, Equifax Canada Co.): Je m'appelle Antonietta Di Napoli.

Le président: Madame Di Napoli, c'est un très joli nom.

Avant de commencer, je mentionne que l'un des premiers rôles dont je me suis acquitté à titre de président a été d'assister aux audiences sur Equifax, aux États-Unis, pendant lesquelles nous avons entendu que 145,5 millions d'Américains avaient été victimes d'une brèche de sécurité. À l'époque, on entendait que les données de pas moins de 100 000 Canadiens avaient été compromises. Tout récemment, votre entreprise a annoncé que le nombre de Canadiens dont les données avaient été compromises tournait plutôt autour de 19 000.

Il est inquiétant pour les Canadiens, comme ce l'était pour les Américains, que les données de 19 000 Canadiens aient été compromises. D'ici la fin de la séance, nous espérons savoir qu'Equifax a réglé le problème de logiciel qui s'est posé aux États-Unis et que les mesures observées ne se reproduiront jamais plus. Sur ce, je suis impatient de vous entendre.

La parole est à vous, monsieur Russo.

M. John Russo (directeur de la protection de la vie privée et secrétaire général, Equifax Canada Co.): Bonjour, monsieur le président et mesdames et messieurs les députés. Au nom d'Equifax Canada, je vous remercie de cette occasion de nous joindre à votre comité aujourd'hui. Je suis ici afin de vous donner l'information à jour concernant l'incident de cybersécurité et pour répondre à vos questions au meilleur de mes connaissances.

Je me nomme John Russo. Je suis chef de la protection de vie privée et secrétaire général à Equifax Canada. Je travaille avec fierté pour cette entreprise canadienne depuis 10 ans. Je possède un bureau à Toronto, où je vis depuis toujours. Je suis fier des services offerts par Equifax Canada aux Canadiens d'un océan à l'autre de même que de ce que nous avons entrepris avec les gouvernements de partout au pays afin d'aider à renforcer les lois sur la protection de la vie privée pour tous les Canadiens.

Ma collègue Antonietta Di Napoli, directrice de l'exploitation mondiale à Equifax Canada, se joint à moi. Bien que sa participation aux activités liées à la brèche soit limitée, sa vaste expérience des activités et son exposition aux consommateurs apportera une perspective des pratiques et de la procédure touchant les consommateurs.

Je désire vous entretenir de trois sujets en particulier aujourd'hui. Primo, je vous parlerai de ce qui s'est produit lorsque notre société mère, Equifax US, a fait l'objet d'un piratage et que de l'information sensible sur les consommateurs a été volée de ses serveurs. Secundo, je détaillerai les étapes de redressement prises par Equifax Canada pour aider les Canadiens en cause. Tertio, je discuterai de ce que fait Equifax Canada pour s'assurer que cela ne se produise plus, de même que ce que nous faisons pour conférer aux consommateurs un plus grand contrôle sur leur information de crédit personnelle.

Mais avant d'aborder ces trois sujets, je désire vous présenter mes plus sincères excuses. Au nom d'Equifax Canada et de l'organisation d'Equifax dans son ensemble, je demande pardon à tous les Canadiens dont l'information personnelle a été compromise. Être le gestionnaire de confiance de l'information a longtemps été l'un des principes de base d'Equifax, alors nous sommes dévastés par ce qui s'est produit. Je puis vous assurer que dans les mois et les années qui ont mené à cet incident, Equifax US n'a jamais pris à la légère la protection des données. En fait, elle a investi massivement, particulièrement ces cinq dernières années, dans la sécurité et la résilience des réseaux. Néanmoins, la cyberattaque et la brèche se sont produites. De l'information a été volée par des criminels. Mais nous en assumons l'entière responsabilité et pour l'incident et pour l'impact qu'il a eu sur les Canadiens.

D'abord et avant tout, la question que vous vous posez tous est: que s'est-il produit?

Nous savons que des criminels ont perpétré une importante cyberattaque contre notre société mère, Equifax US. En plus d'accéder à l'information de millions d'Américains, ils ont été en mesure d'accéder à l'information d'environ 19 000 Canadiens. L'information ayant fait l'objet d'un accès comprenait de l'information comme: les noms, adresses, dates de naissance, numéros d'assurance sociale et de cartes de crédit. À des fins de références, je vous ferai un bref aperçu chronologique du déroulement des événements.

Le vendredi 29 juillet, la division de la sécurité de notre société mère, Equifax US, a observé un trafic suspect dans le réseau associé au site Web des consommateurs américains. La division de la sécurité est intervenue immédiatement et a bloqué le trafic suspect relevé. La division a continué de surveiller le trafic du réseau et a observé d'autres activités suspectes le 30 juillet. En réponse, elle a retiré complètement l'application Web en ligne ce jour-là.

Le piratage criminel était terminé, mais le travail pour déterminer la nature, l'étendue et, le plus important, l'impact commençait tout juste. À ce moment-là, on ne savait pas que de l'information personnelle avait été volée. Le 2 août, Equifax US a retenu les services d'une firme de cybersécurité indépendante pour faire enquête sur ces activités suspectes et a communiqué avec le Bureau fédéral des enquêtes (« FBI »).

● (1535)

Dans les semaines qui ont suivi, Equifax US et la firme de cybersécurité ont travaillé sans relâche afin de déterminer ce qui s'était produit.

Le 7 septembre, Equifax US a émis un communiqué de presse pour annoncer l'incident de cybersécurité et indiquait qu'elle avait constaté des accès non autorisés à de l'information personnelle limitée de certains consommateurs canadiens. À ce moment, il n'y avait pas d'autres détails sur le nombre de Canadiens en cause ni les données précises qui avaient été compromises.

Concernant notre communication avec les Canadiens, en ma qualité de chef de la protection de la vie privée à Equifax Canada, j'ai d'abord été informé de l'incident de cybersécurité et de son impact potentiel sur des Canadiens avant l'émission du communiqué de presse du 7 septembre. J'ai immédiatement pris des mesures pour aviser les organismes de réglementation fédéraux et provinciaux et, dès le 8 septembre, j'avais communiqué avec les commissaires à la protection de la vie privée appropriés (y compris le commissaire à la protection de la vie privée du Canada) et les organismes de réglementation des consommateurs de partout au pays.

Equifax Canada a également retenu les services de Chantal Bernier, ancienne commissaire de la protection de vie privée au Canada par intérim, maintenant avocate-conseil, membre du groupe Protection de la vie privée et des renseignements personnels de Dentons. Nous voulions satisfaire les niveaux les plus élevés de conformité en matière d'intervention après une brèche et de transparence pour les Canadiens et les organismes de réglementation. Alors que la firme indépendante de cybersécurité travaillait à compléter son enquête et à donner à Equifax Canada les détails sur les Canadiens en cause, nous avons commencé à élaborer et à mettre en place notre plan pour aider ces Canadiens.

Nous avons également mis à jour le site Web des consommateurs canadiens, Equifax.ca, afin d'indiquer à tous les Canadiens où ils pouvaient trouver des réponses. Nous avons aussi engagé du personnel supplémentaire pour notre centre d'appels canadien, prolongé les heures d'ouverture dudit centre d'appels et mis en place une adresse électronique consacrée à la brèche.

Le 19 septembre, Equifax Canada a émis un communiqué de presse pour faire connaître aux Canadiens les détails préliminaires reçus sur la nature de l'impact et ce que l'enquête avait permis d'apprendre à ce moment-là.

Le 2 octobre, Equifax US a émis un communiqué de presse avec des mises à jour, y compris le fait qu'environ 8 000 consommateurs canadiens avaient été touchés par la brèche en plus d'un nombre indéterminé de Canadiens dont les cartes de crédit compromises étaient en cause. Plus tard cette semaine-là, Equifax Canada a reçu le fichier de données renfermant l'information des 8 000 particuliers d'Equifax US, et nous l'avons immédiatement examiné afin de dresser une liste d'envoi. Le 13 octobre, nous avons commencé à poster des lettres de notification, dans les deux langues officielles, aux consommateurs canadiens en cause.

Les lettres de notification avisaient les consommateurs de trois facteurs clés: d'abord que leurs données avaient été compromises, deuxièmement les éléments de données précis compromis et troisièmement, les détails sur la façon d'activer un abonnement à Equifax Canada pour une protection contre le vol d'identité et une surveillance de crédit pour 12 mois.

Le 10 novembre, Equifax US a déterminé que le nombre de Canadiens, en plus de ceux dont l'information de carte de crédit avait été compromise, totalisait environ 11 000 — portant le nombre total de Canadiens en cause à environ 19 000. Ces 11 000 consommateurs supplémentaires ont aussi été avisés par la poste. Tout au long de ce processus, nous avons continué de mettre à jour les organismes de réglementation et notre site Web canadien à la consommation régulièrement afin d'inclure la nouvelle information.

Que faisons-nous pour protéger les Canadiens en cause? À l'instar de sa société mère aux États-Unis, Equifax Canada offre une gamme complète de protection aux Canadiens en cause, sans frais, durant 12 mois. Cette protection comprend premièrement une surveillance de crédit quotidienne avec des alertes pour tout changement important apporté à leur dossier de crédit Equifax; deuxièmement, un accès quotidien à leur score et dossier de crédit Equifax; troisièmement, un balayage Internet avec des alertes si leur numéro d'assurance sociale, leurs numéros de carte de crédit ou de débit sont utilisés dans des sites Web douteux; quatrièmement, une assurance contre le vol d'identité allant jusqu'à 50 000 $ pour couvrir des frais liés au vol d'identité.

● (1540)

Les consommateurs en cause ont reçu un code d'activation dans leur lettre de notification qu'ils peuvent utiliser pour activer les services en ligne. Ou bien, ils peuvent appeler le centre d'appels canadien afin de recevoir de l'aide personnellement.

Voici ce que nous faisons pour veiller à ce que cela ne se reproduise plus. Comme je l'ai mentionné plus tôt, dès que l'intrusion a été découverte, notre société mère Equifax US a commencé une enquête judiciaire concernant les activités de l'agresseur. Cette enquête est maintenant terminée et nous comprenons ce qui s'est passé et l'étendue de l'intrusion. Equifax US a pris des mesures pour corriger les vulnérabilités et a mis en place d'autres initiatives à court et à long terme afin de protéger les données des consommateurs qui lui sont confiées.

Elle a entrepris un réexamen complet des pratiques de sécurité des données et des TI. Elle travaille à renforcer les réseaux et a modifié la procédure pour exiger une confirmation lorsque des rustines de logiciels sont appliquées, de nouveaux outils de détection des vulnérabilités, ainsi que le renforcement du processus de responsabilisation. Elle a également retenu les services d'experts de l'industrie comme PwC et Mandiant pour l'aider à élaborer des programmes de sécurité, y compris des initiatives de correction et de transformation stratégiques qui aideront à déterminer et à mettre en place des solutions afin de renforcer la protection des données et la défense de la cybersécurité à long terme.

Finalement, nous nous sommes engagés à travailler proactivement avec l'industrie dans son ensemble afin d'élaborer des solutions pour relever les défis grandissants liés à la cybersécurité et à la protection des données auxquels nous sommes tous confrontés. Nous voyons cette brèche comme un point charnière — non seulement pour Equifax mais pour toute personne intéressée à protéger l'information personnelle.

Vous avez peut-être entendu dire que le PDG intérimaire d'Equifax US a fait connaître son plan visant à lancer un nouveau service à la consommation qui permettrait aux consommateurs de verrouiller et de déverrouiller leur dossier de crédit à volonté, sans frais, pour la vie, grâce à une interface mobile. Ce produit devrait être lancé en janvier aux États-Unis, et nous travaillons à le présenter au Canada dès que possible l'an prochain afin d'assurer que les consommateurs canadiens aient le même contrôle sur leur information de crédit que leurs homologues américains.

En terminant, je désire encore une fois présenter mes excuses à tous les Canadiens au nom de toute l'équipe d'Equifax Canada. Bien que nous prenions des mesures pour protéger les Canadiens en cause, nous comprenons que ces derniers, partout au pays, ont été contrariés par les nouvelles de la brèche de cybersécurité subie par Equifax US qui en retour a touché l'information personnelle de Canadiens. Plusieurs Canadiens, qu'ils soient personnellement en cause ou non, ont fait part de leurs peurs et de leurs inquiétudes à moi personnellement, aux médias et aux élus. Je partage leurs préoccupations tout comme mon entreprise, et nous nous sommes fermement engagés à faire tout en notre pouvoir pour regagner leur confiance.

Je vous remercie.

Mme Di Napoli et moi sommes prêts à répondre à toutes vos questions.

● (1545)

Le président: Merci, monsieur Russo.

Pour que ce soit bien clair pour tous les membres du Comité, la période de questions pourra durer jusqu'à 17 h 15 environ. Une motion sera ensuite soumise au Comité, après quoi nous devrons aussi discuter un peu des travaux du Comité. Nous pourrons peut-être prendre un peu plus de temps s'il nous reste des questions à poser, mais c'est l'horaire que j'aimerais respecter.

Pour commencer, j'accorde sept minutes à M. Erskine-Smith.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci beaucoup.

D'entrée de jeu, je mentionne qu'Equifax, comme d'autres agences similaires, réalise du profit privé grâce à un service public. Le nombre de Canadiens et d'Américains qui ont vu leurs données compromises est effarant.

J'aimerais d'abord vous demander une précision. Vous avez dit que 19 000 Canadiens étaient touchés. S'agit-il seulement de Canadiens qui vivent aux États-Unis?

M. John Russo: Non, il s'agit de Canadiens qui résident au Canada.

M. Nathaniel Erskine-Smith: Avez-vous un chiffre pour ce qui est des Canadiens vivant aux États-Unis?

M. John Russo: Je n'ai pas ce chiffre avec moi aujourd'hui.

M. Nathaniel Erskine-Smith: Ne devriez-vous pas l'avoir?

M. John Russo: Je me ferai un plaisir de vous le faire parvenir par écrit.

M. Nathaniel Erskine-Smith: C'est intéressant. En préparation de la séance d'aujourd'hui, on se serait attendu à ce que vous nous fournissiez ce chiffre, mais ce serait merveilleux si vous pouviez nous le faire parvenir par écrit.

Vous nous avez présenté un historique de la situation, mais comme vous le savez très bien — et je le sais, parce que j'ai moi aussi assisté à l'audience d'Equifax devant le Congrès —, cet historique est extraordinairement incomplet. Vous n'avez pas mentionné du tout ce qui s'est passé en mars.

Vous pouvez peut-être expliquer au Comité et au public canadien que le département de la Sécurité intérieure des États-Unis, le DHS, vous avait mis en garde en mars dernier. Vous pouvez peut-être nous renseigner un peu sur les mesures prises par Equifax Inc. en réponse à cet avertissement et nous dire si vous estimez que ces mesures étaient suffisantes.

M. John Russo: Bien sûr. Cet historique remonte au 9 mars, aux États-Unis. Equifax a diffusé l'avis US-CERT, comme vous l'avez mentionné, par courriel à l'interne, afin de demander au personnel responsable de l'installation d'Apache Struts de mettre son logiciel à jour. Conformément à notre politique sur les rustines, le département de la sécurité d'Equifax a exigé que la rustine soit déployée dans les 48 heures.

M. Nathaniel Erskine-Smith: Quel genre de suivi a été fait avec le DHS? Le DHS vous a mis en garde le 8 ou le 9 mars. Je crois comprendre qu'il y a eu une demande interne afin que le logiciel soit mis à jour et que la rustine soit déployée. Le département de la sécurité aurait effectué un balayage qui n'aurait pas permis de relever les vulnérabilités observées par le DHS. Quel suivi en a été fait avec le DHS?

M. John Russo: Le 15 mars, notre département de la sécurité a effectué son propre balayage, comme vous l'avez mentionné, et aurait dû repérer les systèmes vulnérables à Apache Struts.

● (1550)

M. Nathaniel Erskine-Smith: Quel suivi avez-vous fait avec le DHS ensuite? Une agence de sécurité, peut-être la plus importante au monde, affirme à Equifax: « Vous avez une vulnérabilité qui pourrait toucher des millions d'Américains. » Vos responsables de la sécurité déploient un programme, mais ne trouvent rien. Je me demande s'il y a eu des communications ensuite entre votre équipe et le DHS pour lui dire: « Nous avons effectué tel balayage et n'avons relevé aucun problème. Qu'avez-vous trouvé que nous n'avons pas trouvé? »

M. John Russo: Je suis ici en ma qualité de directeur de la protection de la vie privée au Canada, et je ne serais pas au courant de ces discussions s'il y en avait eu.

M. Nathaniel Erskine-Smith: Peut-être pouvez-vous demander l'information, puis la faire parvenir ultérieurement au Comité pour le renseigner de toute communication subséquente avec le DHS de la part d'Equifax. Il me semble que si le DHS venait voir mon entreprise et me dire que j'ai une énorme vulnérabilité sur le plan des données, et que je ne trouvais rien à l'issue de mes propres recherches, je voudrais vraiment communiquer avec le DHS pour lui dire que je n'ai rien trouvé et m'assurer de faire un suivi.

De même, vous ne mentionnez pas le 13 mai dans vos notes, mais d'après ce que je comprends, c'est le 13 mai que les pirates ont réussi pour la première fois à accéder aux données. C'est donc entre le 13 mai et la fin juillet que les pirates ont réussi à avoir accès au système d'Equifax, n'est-ce pas?

M. John Russo: C'est juste. L'attaque a eu lieu entre le 13 mai et le 30 juillet.

M. Nathaniel Erskine-Smith: Nous venons à peine de terminer une étude sur la protection des renseignements personnels des Canadiens. Nous sommes en train de préparer nos recommandations. Divers témoins sont venus témoigner devant nous de l'importance du cryptage. Il me semble ahurissant que les données de plus de 145 millions d'Américains et de 19 000 Canadiens aient été compromises, qu'il ait été si facile d'entrer dans le système. Ces renseignements n'étaient pas cryptés. Vous pouvez peut-être nous expliquer pourquoi ces données n'étaient pas suffisamment cryptées.

M. John Russo: Les normes que nous avions en place aux États-Unis étaient exemplaires. Elles étaient reconnues partout dans l'industrie. Ce n'est pas comme si nous ne respections pas les règles d'or de l'industrie. Dans ce cas-ci, la vulnérabilité découlait d'une erreur humaine et d'une erreur des TI, et les pirates ont réussi à déjouer notre défense.

M. Nathaniel Erskine-Smith: Je suppose que vous ne pourrez pas me répondre aujourd'hui, mais vous pourrez peut-être le faire ultérieurement par écrit, là encore. Pour la suite des choses, pour que ce genre d'incident ne se reproduise plus jamais — c'était la troisième partie de votre exposé, et je vous en suis reconnaissant —, pouvez-vous expliquer au Comité quelles mesures vous prenez pour renforcer vos pratiques de cryptage?

M. John Russo: Certainement. Au Canada, nos données sont cryptées et segmentées. Nous sommes conformes à la norme PCI et nous respectons les normes de sécurité.

Pour revenir aux vulnérabilités qui se sont posées, nous avons un système de confirmation en boucle infinie. Grosso modo, nous ne nous contentons pas de déployer une rustine, mais nous devons aussi en recevoir la confirmation, afin de boucler la boucle.

M. Nathaniel Erskine-Smith: C'est très bien de voir que vous avez pris des mesures, notamment l'offre d'une assurance contre le vol d'identité allant jusqu'à 50 000 $ sur une période de 12 mois. Il n'y a toutefois aucune garantie que le vol d'identité surviendra au cours de ces 12 mois, et Equifax est clairement négligente en ce sens à l'égard des renseignements personnels de ces personnes. Vous engagez-vous à garantir l'intégrité de tous les Canadiens en cas d'un vol d'identité qui découlerait de la négligence d'Equifax?

M. John Russo: Nous offrons aux 19 000 Canadiens touchés, environ, notre surveillance de crédit de pointe, un produit qui a été utilisé après les autres grandes brèches survenues au Canada, dont celle de Home Depot. Elle est offerte gratuitement à tous les consommateurs touchés pendant 12 mois. Tous les autres consommateurs qui ont peur peuvent également demander à mettre leur dossier en alerte. Ils n'ont qu'à s'adresser à Equifax. Nous offrons le service gratuitement.

M. Nathaniel Erskine-Smith: Pendant 12 mois?

M. John Russo: Pendant six ans.

M. Nathaniel Erskine-Smith: Donc cette assurance pouvant aller jusqu'à 50 000 $ est-elle disponible pendant six ans?

M. John Russo: Elle s'adresse aux personnes qui choisiront de s'inscrire à la surveillance de crédit, que nous offrons à tous les Canadiens touchés. Tous les autres Canadiens...

M. Nathaniel Erskine-Smith: Non, je parle de l'impact sur les Canadiens, sur ceux qui sont susceptibles de subir les conséquences de la négligence d'Equifax. Je tiens à protéger l'intégrité de ces Canadiens sans qu'ils doivent intenter un recours collectif ou multiplier les poursuites individuelles. C'est ce dont je veux m'assurer, donc j'espère que vous pourrez confirmer au Comité aujourd'hui qu'Equifax garantira l'intégrité de ces Canadiens.

M. John Russo: Oui, des 19 000 Canadiens touchés par cet incident; leur intégrité sera assurée grâce aux produits de pointe que nous leur offrons, qui vient avec une assurance allant jusqu'à 50 000 $ pour couvrir des frais liés au vol d'identité.

M. Nathaniel Erskine-Smith: Pendant 12 mois ou 6 ans?

M. John Russo: Pendant 12 mois.

M. Nathaniel Erskine-Smith: Qu'arrivera-t-il après ces 12 mois? Comment leur intégrité sera-t-elle protégée si le vol d'identité survient après ces 12 mois?

M. John Russo: Ils pourront choisir de renouveler leur inscription à la surveillance de crédit que nous leur offrons ensuite.

M. Nathaniel Erskine-Smith: Ils devront payer pour le service.

M. John Russo: C'est effectivement un service payant au Canada.

M. Nathaniel Erskine-Smith: Cela donne l'impression que vous ne pouvez pas garantir entièrement leur protection s'il y a usurpation d'identité après 12 mois.

M. John Russo: La protection offerte comprend une période de surveillance de crédit de 12 mois assortie de différents indicateurs, notamment lorsque des renseignements personnels sont compromis en cas de vol ou de perte du portefeuille. Il y a aussi des alertes. Le client est avisé toutes les fois qu'une personne a accès à son dossier de crédit pendant ces 12 mois. La période de 12 mois commence au moment de l'activation du produit. Ce n'est pas à la date du piratage ou à celle de la lettre, mais bien lorsque l'abonnement est enregistré.

● (1555)

M. Nathaniel Erskine-Smith: C'est tout le temps que j'avais.

Le président: Merci beaucoup, monsieur Erskine-Smith.

Nous passons à M. Kent pour les sept prochaines minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président, et merci à nos deux témoins présents aujourd'hui.

Lorsque nous avons assisté aux audiences du Congrès à Washington, nous avons entendu de nombreuses observations et déclarations indiquant que votre entreprise et votre secteur sont assujettis à une réglementation vraiment insuffisante. Dans vos remarques préliminaires, vous avez souligné qu'Equifax Canada continue de tenir les organismes de réglementation au fait de la situation. Quels sont les organismes qui vous réglementent? À qui devez-vous rendre des comptes?

M. John Russo: Nos organismes de réglementation au Canada se situent à deux niveaux. Il y a d'abord les agences se consacrant à la protection de la vie privée, comme le commissariat canadien et ses équivalents provinciaux, par exemple en Colombie-Britannique, en Alberta et au Québec. Il y a également les organismes en charge des renseignements concernant le consommateur dans les différentes provinces qui ont adopté une loi en la matière. Nous devons donc rendre des comptes à deux instances distinctes.

L'hon. Peter Kent: Croyez-vous qu'il émane du débat public, surtout aux États-Unis, bien que cela commence également au Canada, une volonté de voir des règlements plus ciblés et plus stricts être adoptés en matière de protection des renseignements personnels?

M. John Russo: Oui. C'est pourquoi j'indiquais dans mes observations préliminaires que nous prenons des mesures proactives de telle sorte que les consommateurs canadiens puissent par exemple, comme c'est le cas aux États-Unis, verrouiller et déverrouiller à volonté leur dossier de crédit, et y avoir eux-mêmes davantage accès en même temps qu'à leurs renseignements personnels, de manière à pouvoir mieux contrôler le tout. C'est un service offert sans frais à tous les Canadiens.

L'hon. Peter Kent: Ai-je bien compris qu'Equifax Canada utilise le même programme Apache Struts et devrait donc appliquer la même rustine?

M. John Russo: Il existe différentes rustines. Ce sont nos systèmes mondiaux de sécurité qui s'en occupent dans les 24 pays où nous sommes présents.

L'hon. Peter Kent: Nous avons appris à Washington que la faille initiale a été découverte par les agences nationales de sécurité qui en ont informé Equifax U.S. Est-ce que la même alerte a été lancée au Canada au mois de mars?

M. John Russo: Parlez-vous d'Equifax Canada?

L'hon. Peter Kent: Oui. Est-ce que l'avertissement servi à Equifax aux États-Unis par les agences nationales de sécurité a été immédiatement transmis à Equifax Canada?

M. John Russo: Je vais devoir vous répondre ultérieurement, car je n'ai pas ces renseignements avec moi.

L'hon. Peter Kent: C'est un peu la source de toutes les interrogations actuelles. Il s'est écoulé une période inexplicablement longue avant que l'entreprise ne soit mise au courant de l'atteinte à la sécurité; des mesures correctives inadéquates semblent avoir été prises; et on a ensuite téléchargé les renseignements personnels de ces millions de gens.

M. John Russo: Pour que les choses soient bien claires, c'est seulement le 29 juillet que nous avons noté des activités suspectes. En mars, en avril et en mai, rien n'indiquait qu'Equifax avait été victime d'une intrusion. Il y a eu des activités suspectes le 29 et le 30 juillet, après quoi nous avons fermé notre portail aux États-Unis.

L'hon. Peter Kent: On était cependant au courant à la suite de l'avertissement servi par les agences nationales de sécurité, bien que je ne me rappelle pas exactement lesquelles, quant à l'intrusion dont le système avait été victime.

Les questions que nous posons aujourd'hui sont un peu les mêmes que celles qui ont été posées à Washington. Pourquoi avoir mis autant de temps à réagir après avoir appris qu'il y avait eu intrusion et que le système était vulnérable à une atteinte qui est forcément survenue par la suite?

M. John Russo: L'alerte a été lancée pour que l'on installe les rustines nécessaires, ce qui n'a pas été fait. Nous pouvons maintenant en ressentir les répercussions à l'échelle planétaire.

L'hon. Peter Kent: A-t-il été question d'installer un pare-feu entre la portion canadienne de l'entreprise et la société mère aux États-Unis, compte tenu des problèmes qui ont touché cette dernière?

M. John Russo: Étant donné que nous avons des filiales dans 24 pays, nous essayons d'assurer la coordination de nos mesures de sécurité à l'échelle mondiale. Nous ne voulons pas de systèmes décentralisés. Nous désirons centraliser ces activités de telle sorte que nos politiques s'appliquent de la même manière partout dans le monde. On ne voudrait surtout pas qu'un pays ait une ceinture pendant qu'un autre a une ceinture et des bretelles.

Afin d'optimiser ces efforts, nous avons haussé le niveau de vulnérabilité associé aux différentes activités. Certaines sont ainsi passées d'un faible niveau de risque à un niveau moyen. Celles qui étaient jugées modérément risquées sont désormais considérées comme présentant un risque élevé. Nous voulons aller encore plus loin que ce que prévoient les normes de l'industrie. Cet incident a vraiment marqué un point tournant pour nous comme pour l'industrie. Nous tenons à nous assurer que cela ne se reproduise jamais.

● (1600)

L'hon. Peter Kent: Aux États-Unis, l'entreprise a perdu confiance dans l'ancien PDG. Peut-on dire la même chose de la société au Canada et des autres filiales nationales d'Equifax? Y a-t-il encore des questionnements au sujet de la direction intérimaire de l'entreprise?

M. John Russo: Je peux vous parler de la situation au Canada. Lorsque j'ai été mis au courant en même temps que le reste de l'équipe de gestion le soir du 7 septembre, nous avons pris sur-le-champ des mesures afin de nous assurer que tous les consommateurs canadiens... Je dois dire que notre priorité était de les protéger et de les aviser. Pour ce faire, il nous a fallu obtenir des données de la société mère aux États-Unis, ce qui a exigé un certain temps. Nos spécialistes judiciaires ont dû passer au peigne-fin plus de 11 000 dossiers pour en arriver à la conclusion en cours d'enquête qu'il y en avait 28 renfermant des données concernant des consommateurs canadiens.

Ce n'est que vers la fin du processus d'enquête que nous avons appris que des Canadiens pouvaient être touchés. C'est environ deux jours avant que les États-Unis en fassent l'annonce, soit le 4 ou le 5 septembre, que les atteintes à l'encontre de citoyens du Royaume-Uni et du Canada ont été mises au jour. On savait seulement que certains éléments étaient touchés. Nous ne connaissions pas la portée de l'intrusion. Nous ne savions pas quels types de données étaient en péril, mais dès que nous l'avons appris, notre équipe de gestion a pris la situation en main en apportant les correctifs nécessaires au Canada.

L'hon. Peter Kent: D'accord.

Certaines sources américaines nous ont amené à croire que les Canadiens touchés avaient déjà fait affaire avec les mécanismes d'évaluation du crédit des États-Unis. Comment des Canadiens peuvent-ils être assujettis à un régime américain? Vous avez dit tout à l'heure qu'il y en avait 8 000, ou plutôt 19 000, parmi les 100 000 recensés au départ, en parlant des Canadiens qui ont été exposés au Canada. Est-il possible qu'il y en ait bien davantage si l'on tient compte des Canadiens qui vivent aux États-Unis ou qui y ont vécu au cours des dernières décennies?

M. John Russo: Les personnes qui résident aux États-Unis et détiennent un numéro de sécurité sociale américain font partie des 145 millions dont le dossier est traité là-bas. Il y en a un nombre relativement minime. Je n'ai pas les chiffres en main, mais ce n'est pas très élevé.

Pour ce qui est...

L'hon. Peter Kent: Comme je fais partie des personnes qui pourraient être touchées, j'ai essayé d'accéder au site Web d'Equifax U.S., mais j'ai dû y renoncer après deux heures de vaines tentatives. Les règles d'accès semblent changer sans cesse, ce qui ne manque pas de soulever d'importantes préoccupations, comme vous pouvez sans doute très bien le comprendre.

M. John Russo: Je comprends votre frustration.

Les 18 000 ou 19 000 Canadiens touchés sont ceux qui avaient une relation de consommateur avec l'entreprise Equifax. La majorité des 19 000 personnes dont les données ont été compromises au Canada avaient effectué des achats en ligne via Equifax et fourni leurs coordonnées de paiement par carte de crédit, ce qui comprend certains renseignements personnels.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

Nous passons maintenant à M. Weir pour une période de sept minutes.

M. Erin Weir (Regina—Lewvan, NPD): Merci beaucoup.

M. Kent vous a interrogé au sujet du temps qui s'est écoulé entre le piratage lui-même et le moment où Equifax s'en est rendu compte. J'aimerais pour ma part vous parler du temps écoulé entre la découverte de l'intrusion par Equifax à la fin juillet et l'annonce publique faite en septembre.

M. John Russo: Revoyons le calendrier. Notre équipe de sécurité aux États-Unis a noté des activités suspectes les 29 et 30 juillet. À ce moment-là, on ignorait qu'il y avait eu intrusion et que des renseignements personnels étaient compromis. Le tout a été affiché sur le portail américain de règlement en ligne des différends en matière de consommation. Le 2 août, Equifax Inc. a retenu les services d'une firme externe de consultants, King & Spalding, qui a elle-même fait appel à un expert pour mener l'enquête judiciaire requise. Comme vous pouvez le comprendre, avec 145 millions de citoyens américains touchés, plus un certain nombre de Canadiens et de Britanniques, ce n'était pas une mince affaire. Il a fallu revenir en arrière pour consulter tous les dossiers passés entre les mains des criminels. Il ne faut pas perdre de vue qu'il s'agissait bel et bien d'un acte criminel. Le FBI a également eu un rôle à jouer. Il y avait de nombreux éléments qui entraient en jeu, un grand nombre de personnes touchées et des gens qui travaillaient sans relâche pour obtenir l'information et les réponses que les Américains et les Canadiens attendaient. Étant donné la complexité de l'enjeu, le nombre de dossiers en cause et le manque de structure qui rendait difficile leur examen approfondi, il a fallu un certain temps pour mener à bien cette tâche.

Comme je le disais tout à l'heure à M. Kent, la portion canadienne de l'incident n'a été mise au jour que 48 heures avant l'annonce faite le 7 septembre. Il s'agit de gigantesques ensembles de données, et il a donc fallu y mettre le temps pour nous assurer de mener une enquête exhaustive et approfondie afin d'identifier chaque consommateur touché et de retracer son adresse actuelle, de telle sorte que notre avis n'arrive pas à son ancienne adresse. Vu l'ampleur de l'intrusion, il a fallu un certain temps pour que notre équipe d'intervention en cas de crise soit prête à donner suite aux questions, craintes, préoccupations et frustrations de ces clients.

● (1605)

M. Erin Weir: On peut penser qu'il aurait été possible d'annoncer qu'un incident s'était produit avant de passer au peigne fin toute l'information. Est-ce en raison de l'enquête du FBI que vous n'avez pas pu faire cette annonce plus tôt?

M. John Russo: Ce n'était pas à cause du FBI. C'est seulement l'un des éléments. Lorsque des intrusions se produisent, il y a toujours un risque que d'autres pirates imitent les coupables. Peu importe le moment retenu pour l'annonce, nous savons que nous devions être prêts à contrer de telles attaques en nous assurant que tous nos systèmes à l'échelle planétaire étaient moins vulnérables qu'ils ne l'étaient en mars dernier. Il a fallu que tous (services juridiques, protection de la vie privée, sécurité, informatique, etc.) mettent l'épaule à la roue pour contribuer à cet important effort. Encore une fois, compte tenu du grand nombre de personnes touchées, il nous a fallu environ 40 jours pour y parvenir.

M. Erin Weir: D'accord.

M. Erskine-Smith a indiqué qu'Equifax offrait essentiellement un service public. Convenez-vous avec lui que votre entreprise peut être assimilée à un service public?

M. John Russo: Nous offrons sur les marchés mondiaux des produits qui procurent aux consommateurs une certaine tranquillité d'esprit en les protégeant notamment contre la fraude et le vol d'identité. Nous avons aussi des produits sans frais comme une alerte indiquant de communiquer avec vous à tel numéro lorsqu'une demande de crédit est présentée en votre nom. Vous signifiez ainsi à tous ceux qui ont accès à votre dossier que vous voulez être avisé avant que du crédit ne soit accordé. Nous facilitons les choses aux consommateurs pour tous les achats importants qu'ils ont à faire. Les gens qui contractent une hypothèque pour la maison de leurs rêves ou qui achètent une nouvelle voiture s'adressent à nous pour que tout se passe de façon efficiente et précise. En l'absence d'information sur le crédit, c'est tout notre système économique qui serait ralenti lorsqu'une demande de crédit est formulée. Comme vous pouvez vous l'imaginer, les banques et les autres institutions financières tiennent à ce que le processus puisse se dérouler rapidement en se fondant sur des informations exactes.

M. Erin Weir: À la base, les gens doivent être disposés à utiliser ces services et à fournir leurs renseignements personnels.

M. John Russo: Vous avez raison. Le consentement du consommateur et les fins admissibles sont deux éléments clés de la Loi sur les renseignements concernant le consommateur. Si ces conditions ne sont pas respectées, il devient impossible pour une institution financière d'avoir accès aux dossiers de crédit d'Equifax. Il faut que le consommateur ait donné son consentement et que ce soit pour des fins autorisées en vertu de la loi.

M. Erin Weir: Il est bien certain que le consentement du consommateur est requis mais, comme vous l'avez mentionné, on a besoin de crédit pour toutes sortes d'événements qui sont pour ainsi dire des passages obligés dans la vie d'une personne. Dans les faits, on n'a d'autre choix que de se prévaloir des mécanismes de crédit en place et de fournir les renseignements demandés.

M. John Russo: L'information que les consommateurs nous transmettent nous permet de mieux les servir en leur donnant accès aux meilleurs taux possible et au crédit nécessaire pour défrayer les coûts associés à ces événements de la vie et effectuer des transactions commerciales au Canada.

M. Erin Weir: On peut dire que le nombre de Canadiens touchés nous a semblé, tout au moins pendant une certaine période, plutôt difficile à cerner avec exactitude. On est ainsi allé de 100 000 jusqu'à 19 000 en passant à un certain moment par 8 000. Est-ce que l'on peut considérer que le nombre actuel de 19 000 est assez ferme?

M. John Russo: Oui, l'enquête est terminée et le nombre de dossiers se situe à environ 19 000. Alors que l'enquête judiciaire suivait son cours, nous avons voulu présenter une estimation préliminaire pour que les gens comprennent bien que la portée de l'inclusion était limitée au Canada, par rapport à la situation aux États-Unis. Nos spécialistes judiciaires nous avaient alors indiqué qu'il pourrait y avoir jusqu'à 100 000 Canadiens touchés.

Lorsque les chiffres définitifs ont été connus, il y avait encore cette question des 209 000 détenteurs de cartes de crédit qui étaient concernés. Il y avait parmi eux un certain nombre de Canadiens que nous avons établi par la suite à 11 000. Si l'on ajoute ces 11 000 détenteurs de cartes de crédit aux 8 000 personnes déjà visées par ailleurs, on obtient un total d'environ 19 000 résidants du Canada.

● (1610)

M. Erin Weir: Avez-vous une idée de qui a pu s'en prendre à Equifax?

M. John Russo: Nous l'ignorons pour l'instant.

M. Erin Weir: Lorsque vous indiquez que des criminels ont piraté Equifax, voulez-vous dire que le piratage lui-même est un acte criminel?

M. John Russo: Le FBI mène actuellement une enquête criminelle aux États-Unis, car il s'agit effectivement d'un acte criminel, peu importe qui l'a commis.

Le président: Merci, monsieur Weir.

Les sept prochaines minutes vont à M. Picard.

[*Français*]

M. Michel Picard (Montarville, Lib.): Je vous remercie, monsieur le président.

Si je comprends bien, vous vendez à vos clients des services de protection contre le vol d'identité.

Est-ce bien cela?

[*Traduction*]

M. John Russo: Nous offrons des services de protection contre le vol d'identité aux consommateurs qui ont été touchés.

[*Français*]

M. Michel Picard: Est-ce un produit qu'Equifax offre à ses clients de façon générale, au même titre qu'un service ou un produit comme une assurance, par exemple?

[*Traduction*]

M. John Russo: Equifax offre deux types de services. Il y en a pour les entreprises commerciales et d'autres pour les consommateurs. Nous offrons en ligne aux Canadiens des services de protection contre le vol d'identité et de l'assurance à ce chapitre. C'est ce que nous appelons la surveillance du crédit.

[*Français*]

M. Michel Picard: Vous vendez donc un service de protection contre le vol d'identité.

Par exemple, si quelqu'un, par un hasard quelconque, usurpe mon identité à cause d'une erreur de ma banque ou d'une transaction que j'ai faite en magasin, ma protection proviendra-t-elle de chez vous si je suis un client d'Equifax?

Faudrait-il que la transaction frauduleuse par laquelle on a volé mon identité implique de l'information provenant de la base de donnée d'Equifax?

[*Traduction*]

M. John Russo: Il n'est pas nécessaire que vous soyez une victime pour pouvoir utiliser nos services. Vous pourriez adhérer à la surveillance du crédit dès aujourd'hui si vous voulez vous sentir plus tranquille grâce aux mesures de protection qui seraient mises en place. Nous offrons des services de surveillance du crédit ainsi que des relevés de crédit sans frais.

[*Français*]

M. Michel Picard: Ce n'est pas la question que je vous pose.

Si je suis un client d'Equifax, que je paie une assurance de protection contre le vol d'identité et qu'on vole mon identité à la suite d'une transaction dans un magasin ou dans un restaurant, est-ce que le service de protection contre le vol d'identité d'Equifax couvrira les pertes encourues en raison de la fraude?

[*Traduction*]

M. John Russo: Non. L'assurance contre le vol d'identité couvre seulement les dépenses que vous engagez en pareilles circonstances. Si vous devez avoir recours à un notaire ou à un avocat, ou vous absenter du travail pour remplacer vos pièces d'identité perdues, l'assurance de 50 000 $ couvrirait les frais qui s'y rattachent. Il appartiendrait par contre au titulaire et à la banque émettrice d'éponger les pertes découlant des dépenses engagées au moyen d'une carte de crédit volée, par exemple pour un repas au restaurant.

[*Français*]

M. Michel Picard: Avez-vous évalué le coût financier du piratage dont Equifax a été victime?

[*Traduction*]

M. John Russo: Comme nous nous sommes attachés en priorité à assurer la protection de nos clients, je n'ai pas de chiffres à vous donner concernant ces coûts. Je peux toutefois vous indiquer que les services que nous offrons sont sans frais pour les consommateurs touchés.

[*Français*]

M. Michel Picard: Je ne cherche pas à savoir ce qui arrive après, mais ce qui arrive avant.

Y a-t-il un montant annuel chez Equifax qui couvre, de façon générale, vos prévisions en matière de gestion de risques?

● (1615)

[*Traduction*]

M. John Russo: Oui, toutes les entreprises constituent des réserves qui les mettent à l'abri de certains risques, en plus des assurances qu'elles contractent, notamment en matière de cybersécurité.

[*Français*]

M. Michel Picard: Est-ce un pourcentage ou un montant fixe?

[*Traduction*]

M. John Russo: C'est un pourcentage. Vous avez peut-être entendu des témoins américains indiquer qu'une part d'environ 12 % de notre budget pour les technologies de l'information est consacrée à la cybersécurité et à la protection de nos systèmes informatiques.

[*Français*]

M. Michel Picard: Quelles mesures prenez-vous pour filtrer les candidats que vous recrutez au sein de votre service informatique?

[*Traduction*]

M. John Russo: Je ne suis pas un spécialiste en ressources humaines ni en sécurité, mais je pourrai vous transmettre par écrit une réponse à cette question concernant nos procédures et politiques en la matière. Je peux tout de même vous dire que tous les employés d'Equifax doivent se soumettre à une vérification approfondie de leurs antécédents.

[*Français*]

M. Michel Picard: J'aimerais que votre société fournisse au Comité les procédures de recrutement et les mesures de sécurité utilisées pour l'embauche et le recrutement de personnel en informatique.

[*Traduction*]

Le président: C'est noté.

[*Français*]

M. Michel Picard: Les allégations à l'effet qu'il s'agit d'une activité criminelle viennent de chez vous, et non pas nécessairement du FBI, parce que vous ne savez pas qui a fait la transaction. Y a-t-il des allégations selon lesquelles de l'aide aurait pu être fournie à l'interne?

[*Traduction*]

M. John Russo: Oui, nous poursuivons notre enquête en collaboration avec le FBI et les autorités policières locales.

M. Michel Picard: Ce n'était pas ma question. Je vais essayer de la formuler différemment.

Avez-vous des indications voulant qu'il y aurait pu avoir un complice de ce piratage à l'interne?

M. John Russo: Vous voulez dire quelqu'un de l'entreprise?

M. Michel Picard: Oui.

M. John Russo: Non. Nous n'avons aucune indication de la sorte...

M. Michel Picard: Et du côté du fournisseur de la technologie que vous utilisez pour votre base de données?

M. John Russo: Il n'y a rien qui nous permette de soupçonner quoi que ce soit de ce côté, monsieur Picard.

M. Michel Picard: Qu'est-ce qui manquait à vos propres services de sécurité pour que vous soyez obligés de faire appel à une tierce partie?

M. John Russo: Pourriez-vous répéter...

M. Michel Picard: Vous nous avez dit avoir fait appel à des experts externes pour faire enquête en même temps que le FBI...

M. John Russo: C'était la firme Mandiant.

M. Michel Picard: Quels sont leurs domaines d'expertise qui semblent échapper de toute évidence à vos propres services de sécurité?

M. John Russo: Nos experts de l'industrie, Mandiant et PwC, ont pu recréer les différentes étapes et requêtes des pirates. Ils ont collaboré avec nos services de sécurité à l'interne pour mettre au jour ces renseignements afin de bien comprendre ce qui s'est produit. Par ailleurs, nous collaborons aussi avec Mandiant et PwC pour déterminer les correctifs à apporter afin qu'un incident semblable ne puisse pas se reproduire.

M. Michel Picard: Vos services de sécurité ne pouvaient pas mener eux-mêmes l'enquête.

M. John Russo: Suivant les conseils du cabinet King & Spalding, ils ont pu retenir les services de spécialistes judiciaires indépendants pour mener une enquête plus approfondie.

M. Michel Picard: J'aurais encore une question, mais j'ai bien peur de ne plus avoir de temps.

Le président: Vous avez en fait cinq secondes. Merci, monsieur Picard.

La parole est maintenant à notre invitée d'aujourd'hui, Mme Boucher.

[*Français*]

Mme Sylvie Boucher (Beauport—Côte-de-Beaupré—Île d'Orléans—Charlevoix, PCC): Bonjour. Je suis très heureuse d'être ici.

C'est vraiment très intéressant, et je vais poursuivre dans la même veine que mes collègues.

Je suis vraiment étonnée. Nous savons tous qu'Equifax a quand même une grande incidence sur nos crédits respectifs. Parlons davantage du Canada. Il y a eu une brèche dans le système et on nous dit que les dossiers de 8 000 personnes ont été piratés. Êtes-vous certain de ce nombre? Pour ma part, le nombre de 8 000 personnes m'apparaît très faible si l'on considère le nombre de clients d'Equifax.

Vous êtes-vous assurés que les supposées victimes de ce piratage en ont été informées, soit par lettre ou par téléphone?

[*Traduction*]

M. John Russo: J'aimerais d'abord rectifier une chose. Il y a 19 000 Canadiens qui sont touchés, et non 8 000. Notre principale base de données portant sur le crédit à la consommation est intacte, car elle n'a pas été visée par le piratage. Les quelque 19 000 personnes touchées ont acheté en ligne un produit avec leur carte de paiement dans le cadre d'une transaction qui a été traitée aux États-Unis. Notre base de données principale sur les commerces et les consommateurs n'a pas du tout été atteinte. C'est seulement notre portail transactionnel aux États-Unis qui a été ciblé.

Nous avons travaillé de concert avec le Commissariat à la protection de la vie privée du Canada pour veiller à ce que tous les consommateurs en cause soient avisés par écrit. Nous avons voulu éviter le téléphone et le courriel, car ils sont propices à des tentatives de hameçonnage à l'endroit de personnes vulnérables comme les aînés et les jeunes. Il était préférable d'adresser une lettre à chacun des Canadiens concernés. Antonietta pourrait peut-être vous en dire plus long sur les moyens que nous avons déployés pour rejoindre nos clients à ce sujet.

● (1620)

Mme Antonietta Di Napoli: Merci beaucoup de votre question.

Comme l'a dit M. Russo, nous avons avisé tous les Canadiens par écrit, car c'est la méthode de communication qu'on nous a suggéré d'utiliser. Chaque consommateur touché a reçu une lettre. Cette lettre les informait de l'atteinte à la sécurité et des renseignements touchés.

Il y avait plusieurs combinaisons possibles. Par exemple, le nom et l'adresse de certains consommateurs pouvaient être touchés, alors que dans le cas d'autres consommateurs, il s'agissait des renseignements liés à leur carte de crédit. Les renseignements compromis de chaque consommateur étaient indiqués dans sa lettre. De plus, nous leur avons offert une protection de 12 mois, comme nous l'avons précisé, et nous leur avons expliqué comment activer ce service et comment communiquer avec Equifax s'ils avaient d'autres questions.

[*Français*]

Mme Sylvie Boucher: Vous avez répondu plus tôt à M. Erskine-Smith que vous offriez un dédommagement d'un an.

Cela me paraît peu. En effet, s'il s'agit d'un acte criminel et que ses auteurs attendent qu'une année soit écoulée avant de commettre le même genre de fraude, en se servant des informations qu'ils ont déjà entre les mains, allez-vous dédommager encore une fois les Canadiens qui en ont été victimes?

Des gens ont des informations entre leurs mains. Si, après une année, les informations que les criminels ont volées sont à nouveau utilisées — les criminels ne pensent pas nécessairement comme nous —, avez-vous prévu aider les Canadiens qui seraient victimes de cette fraude?

[*Traduction*]

M. John Russo: C'est la raison pour laquelle nous emboîtons le pas à notre homologue américain en offrant à tous les Canadiens, dès l'an prochain, une fonction de verrouillage et de déverrouillage du dossier de crédit, en plus du système de surveillance du crédit, qui envoie aux gens des alertes et des messages chaque fois qu'une personne touche leur dossier. Je dis toujours aux clients et aux consommateurs que c'est comme une empreinte digitale. En effet, chaque fois qu'une personne touche leur dossier, c'est comme si elle laissait une empreinte digitale. C'est ce qui permet d'exercer la surveillance.

La fonction de verrouillage et de déverrouillage permettra au consommateur de contrôler l'accès à son dossier de crédit. En effet, personne ne peut avoir accès à un dossier si le consommateur active la fonction de verrouillage, et lorsque ce consommateur fait une demande de prêt à une banque, il peut déverrouiller le dossier. Chaque consommateur contrôle ainsi ses renseignements personnels. C'est la raison pour laquelle nous planifions d'offrir cette fonction au Canada, de façon proactive, dès la nouvelle année. Cela permettra aux consommateurs de profiter de mesures de protection, ainsi que des alertes, comme je l'ai mentionné, qui restent dans le dossier pendant six ans et qui avisent les fournisseurs de crédit qui ont accès aux renseignements de crédit que le client en question a été touché, et qu'il faut communiquer avec lui en utilisant un certain numéro de téléphone, peut-être son numéro de téléphone cellulaire, avant d'accorder le crédit demandé. Ce sont toutes des mesures qu'un consommateur peut prendre en vue de se protéger contre les vols d'identité.

Le président: Merci, madame Boucher.

La parole est maintenant à Mme Fortier.

Mme Mona Fortier (Ottawa—Vanier, Lib.): Je vous remercie de prendre le temps de comparaître aujourd'hui et de répondre à nos questions.

Honnêtement, c'est un problème — et je suis sûre que nous pouvons tous nous en rendre compte — qui touche tous les Canadiens. Vous l'avez mentionné dans votre exposé. Comme un grand nombre de personnes autour de cette table le savent bien, les cotes de crédit et les taux de crédit provoquent beaucoup de confusion et de stress chez nos électeurs, et c'est la raison pour laquelle ils comptent en grande partie sur des services comme le vôtre pour obtenir les renseignements dont ils ont besoin. Pour un grand nombre d'électeurs de ma circonscription, et surtout pour ceux qui n'avaient pas d'épargnes, cette atteinte à la sécurité était une expérience très personnelle et très troublante.

Ce qui m'inquiète, c'est la suite. Je sais que vous avez mentionné dans votre mémoire, et ensuite dans votre exposé, que ces renseignements ont été volés par des criminels. J'aimerais savoir comment vous planifiez découvrir où ces renseignements se retrouveront au bout du compte. Avez-vous embauché des entreprises de sécurité pour tenter de récupérer ces renseignements ou au moins découvrir qui pourrait les avoir volés?

● (1625)

M. John Russo: Je vous remercie de votre question, madame Fortier.

Nous surveillons le Web profond pour découvrir toute transaction suspecte, afin de veiller à ce que les renseignements ne soient pas échangés en ligne. Les Canadiens peuvent être certains que nous suivons ces 19 000 cas pour veiller à ce que leurs renseignements de carte de crédit, leur date de naissance et leur NAS ne soient pas échangés en ligne, et que nous puissions les avertir le cas échéant.

En ce qui concerne la deuxième partie de la question, c'est-à-dire la façon dont Equifax informe les consommateurs, nous avons hâte de travailler avec vous et les électeurs de votre circonscription, que ce soit par l'entremise de séminaires ou d'Equifax 101. Nous serons heureux de faire cela dans toutes les circonscriptions et avec l'aide de tous les députés. Il y a des conseils simples, par exemple, chaque personne peut vérifier son dossier de crédit. Les Canadiens peuvent le faire gratuitement. Ils peuvent vérifier leur dossier de crédit chaque jour s'ils le souhaitent. Ils peuvent aussi s'adresser au département de Toni, qui s'occupe des relations avec les consommateurs, et poser des questions sur leur dossier de crédit et leurs renseignements de crédit, et ils peuvent visiter notre site Web, à l'adresse Equifax.ca pour obtenir des renseignements généraux. Nous aimons offrir ces tournées Equifax 101, comme nous les appelons, aux organismes de réglementation, aux consommateurs et aux groupes de défense des droits des consommateurs de partout au pays, afin que tous soient informés et que les consommateurs aient accès à ces informations pour prendre des décisions éclairées lorsqu'ils font des demandes de crédit.

Toni travaille avec les consommateurs et elle fait le triage des appels avant et après les atteintes à la sécurité. Elle peut donc vous donner une idée des questions posées par les consommateurs.

Mme Antonietta Di Napoli: Merci, John.

Un grand nombre de nos consommateurs, comme l'a dit M. Russo, s'adressent à nous parce qu'on leur a refusé du crédit, car ils ont été victimes de fraude. La plupart de nos conversations avec nos consommateurs concernent surtout l'éducation en matière de crédit. Nous leur expliquons comment le crédit fonctionne au Canada, comment fonctionnent les cotes de crédit, et comment améliorer le crédit et les éléments qui ont des répercussions sur la cote de crédit. Notre rôle consiste principalement à informer les consommateurs. Comme John l'a mentionné, les Canadiens peuvent avoir accès à leur dossier de crédit gratuitement, aussi souvent qu'ils le souhaitent chaque année. Ils peuvent le faire de nombreuses façons, par exemple en visitant l'un des bureaux d'Equifax au pays. Nous leur offrons également un service téléphonique automatisé 24 heures par jour, 7 jours par semaine. Ils peuvent aussi envoyer leur demande par écrit, et nous pourrons leur fournir un exemplaire de leur dossier de crédit.

Comme John l'a mentionné, nous pouvons ajouter une alerte à leur dossier de crédit. Nous encourageons les Canadiens non touchés qui ont des craintes ou des préoccupations au sujet de leur crédit à prendre ces mesures pour se protéger.

Mme Mona Fortier: Merci.

Encore une fois, lorsqu'il s'agit de traiter de façon productive avec les Canadiens et avec vos anciens clients, comment planifiez-vous regagner leur confiance? L'un des points qu'on m'a souvent fait valoir, c'est le temps qui s'est écoulé — et nous en avons parlé — entre le moment où vous avez découvert l'atteinte à la sécurité et le moment où vous avez informé vos clients. De plus, j'aimerais savoir ce que vous faites lorsqu'il n'y a pas d'adresse ou de numéro de téléphone valide au dossier, ou lorsqu'une personne ne vérifie pas son courrier. Comment informez-vous ces gens?

M. John Russo: Toni, voulez-vous d'abord répondre à la deuxième partie de la question?

Mme Antonietta Di Napoli: Absolument.

Manifestement, nous nous sommes rendu compte qu'envoyer des lettres aux consommateurs pouvait présenter quelques défis. Nous avons nettoyé les données, et c'est l'un des facteurs qui a causé quelques retards dans les envois par courrier. Nous nous sommes assurés d'avoir les adresses appropriées et les plus récentes. Nous avons vérifié les données. Comme vous pouvez l'imaginer, nous avons accès à certains de ces renseignements et nous avons donc été en mesure de faire des vérifications croisées et de nettoyer certaines des données initiales. Quelques lettres nous ont été retournées et nous nous occupons de chaque cas individuellement, nous vérifions si les adresses étaient exactes et nous vérifions s'il y a une autre adresse dans une source différente ou nous pouvons communiquer avec les créanciers de ces consommateurs pour vérifier s'ils ont une adresse à jour.

● (1630)

M. John Russo: En ce qui concerne la première partie de votre question, madame Fortier, pour regagner la confiance de nos clients, nous avons rencontré la plupart de nos membres, sinon tous, pour répondre à leurs questions. Nous avons rencontré les membres de l'ABC, l'Association des banquiers canadiens, pour veiller à ce que leurs membres soient parfaitement informés. Nous avons organisé des rencontres en personne. J'ai visité un grand nombre de nos clients pour collaborer avec eux, afin de les aider à minimiser les pertes ou les dommages qui pourraient être causés aux consommateurs à la suite de cet incident. Une atteinte à la sécurité est une atteinte de trop, et Equifax veut donc veiller à mettre en oeuvre des procédures et des processus adéquats, car la sécurité commence avec moi, en tant qu'employé. Elle commence avec Toni. Tout le monde est en sécurité, et nous sommes fiers de cela ici, au Canada. De plus, nos membres peuvent prendre des mesures auprès des banques ou auprès des sociétés de cartes de crédit en vue d'installer des systèmes d'alerte dans les dossiers des consommateurs pour les informer qu'ils ont été touchés par cette atteinte à la sécurité.

Le président: Merci, madame Fortier.

La parole est maintenant à M. Kent. Il a cinq minutes.

L'hon. Peter Kent: Merci, monsieur le président.

Dans l'intérêt des membres du Comité, pourriez-vous décrire le milieu des données relatives au crédit au Canada? Outre Equifax Canada, quelles sont les autres sociétés de services et quelles sont leurs tailles et quels sont leurs revenus annuels, en comparaison?

M. John Russo: Bien sûr. Je ne peux pas parler des revenus de notre concurrent, TransUnion Canada. Il y a quelques agences d'évaluation du crédit plus petites, mais au Canada, les deux principales agences sont Equifax Canada et TransUnion. Aux États-Unis, monsieur Kent, comme vous le savez probablement déjà, il y en a trois, à savoir Experian, TransUnion et Equifax. En ce qui concerne les revenus, je ne connais pas ceux de mes concurrents... Ils sont publiés sur leur...

L'hon. Peter Kent: C'est une entreprise assez profitable, selon moi, étant donné que les organismes d'évaluation de crédit et les fournisseurs de crédit ont accès aux meilleures sources de renseignements complets sur toutes les personnes avec qui ils font affaire.

M. John Russo: Equifax existe depuis 118 ans. Nous fournissons un service à la communauté, car nous permettons aux gens d'ouvrir de petites entreprises ou de faire une première demande de prêt pour fréquenter un collège ou une université. Nous facilitons ces activités, et nous représentons seulement une petite partie de cet écosystème.

L'hon. Peter Kent: Depuis que l'atteinte à la sécurité a été rendue publique, le commissaire à la protection de la vie privée a-t-il communiqué avec vous pour obtenir des explications ou des détails, ou avez-vous communiqué avec le commissaire de façon proactive?

M. John Russo: Comme je l'ai mentionné dans mon exposé, dans les 24 heures suivant l'incident, Mme Bernier, notre avocate-conseil, ou moi-même avions communiqué avec chacun des commissaires à la protection de la vie privée du Canada. Les intervenants du CPVP ont lancé une enquête, et nous collaborons énergiquement avec eux pour répondre à toutes leurs questions. Nous avons été très coopératifs. Nous gérons notre département de la protection de la vie privée au Canada en nous fondant sur la communication, la coopération et le bon sens, et nous en sommes fiers. Nous faisons cela avec tous nos partenaires et tous nos organismes de réglementation.

L'hon. Peter Kent: Pouvez-vous nous fournir des renseignements sur la situation actuelle des deux recours collectifs? L'un d'entre eux, je crois, est de 550 millions de dollars. Je ne suis pas certain de la somme réclamée par l'autre. Je présume que vous contesterez énergiquement ces recours devant les tribunaux.

M. John Russo: Oui, et nous avons retenu les services d'un avocat pour défendre Equifax Canada contre les réclamations des recours collectifs ici et aux États-Unis.

L'hon. Peter Kent: À votre avis, combien faudra-t-il de temps pour régler les deux recours collectifs?

M. John Russo: Je ne peux même pas formuler une opinion sur... Je ne sais pas à quoi ressemblent les arriérés ou les tribunaux ces jours-ci. Je n'ai pas évolué dans la pratique privée depuis 10 ans. Cela dépend du nombre de cas devant les tribunaux, et je ne pourrais même pas estimer le temps nécessaire pour traiter ces affaires devant les tribunaux.

L'hon. Peter Kent: Merci, monsieur le président.

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Baylis. Il a cinq minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): J'aimerais revenir un peu en arrière pour mieux comprendre ce qui s'est produit aux États-Unis. En mars, le département de la Sécurité intérieure des États-Unis a avisé Equifax qu'il existait une faiblesse potentielle dans le système, et qu'Equifax devrait installer un correctif. Est-ce exact?

● (1635)

M. John Russo: Oui, un avis a été envoyé relativement à une mise à jour du logiciel. Le personnel responsable de cela à Equifax, c'est-à-dire l'équipe responsable, n'a pas installé le correctif. Le système de TI qui était censé vérifier que le correctif était en place n'a pas signalé son absence, et il s'agit donc d'une combinaison d'une erreur humaine et d'une erreur liée aux TI.

M. Frank Baylis: On vous a envoyé un avis, mais pour une raison quelconque, une décision a été prise ou cela n'a pas été fait.

Si le correctif avait été en place, ces données auraient-elles été protégées?

M. John Russo: Au mieux de ma connaissance, je ne serais pas devant vous aujourd'hui... oui.

M. Frank Baylis: Ce qui me préoccupe, et cette question a été soulevée par quelques députés, c'est ce qui se produit le 13e mois suivant le vol des données d'une personne. Lorsqu'une personne se fait voler sa carte de crédit, ce n'est pas très grave. Nous pouvons remplacer une carte de crédit. Toutefois, je ne peux pas changer mon NAS ou ma date de naissance, et je ne veux probablement pas déménager à cause de cela. Certaines choses sont fondamentales et sont donc susceptibles d'être exploitées, par exemple, le 13e ou le 14e mois après l'incident.

Si une personne est victime de fraude pendant le 13e mois et qu'elle doit débourser 20 000 $ pour récupérer son identité ou intenter des poursuites contre l'individu qui l'a volée, quelle somme la société Equifax remboursera-t-elle à cette personne?

M. John Russo: Comme je l'ai mentionné, les services que nous offrons, relativement aux normes de notre industrie, ont été utilisés lors d'autres atteintes à la sécurité. En ce qui concerne les organismes de réglementation, la période de 12 mois représente une norme acceptable que nous avons déjà observée lorsque nous avons offert notre soutien à de nombreux clients victimes d'une atteinte à la sécurité. Encore une fois, il existe des services gratuits, par exemple, la surveillance du dossier de crédit; le consommateur peut vérifier son dossier de crédit pour s'assurer que personne n'a volé son identité ou modifié son adresse.

M. Frank Baylis: Est-ce la norme? Lorsque cela se produit dans d'autres endroits, la norme consiste-t-elle à offrir une protection pendant 12 mois et à laisser ensuite ces gens se débrouiller seuls?

M. John Russo: En ce qui concerne les normes pour les cas qui se sont produits au Canada, oui, cette période de 12 mois représente la norme établie.

M. Frank Baylis: Qui établit cette norme?

M. John Russo: Elle a été utilisée dans d'autres organismes. Les tribunaux se sont prononcés à son égard. On a pu la voir dans le recours collectif concernant Home Depot. C'est une norme acceptable dans l'industrie et les pratiques de l'industrie depuis de nombreuses années.

M. Frank Baylis: Est-ce une norme acceptée s'il n'y a aucun tort? Imaginons que Home Depot a tout fait correctement et que, sans que l'entreprise soit fautive, une personne réussit à voler ses données. Toutefois, dans ce cas-ci, il me semble qu'on peut blâmer Equifax. En effet, on a informé Equifax qu'il fallait faire une certaine chose, et l'organisme a choisi de ne pas la faire; il y a donc un fautif dans ce cas-ci.

Est-ce la norme, qu'il y ait des torts ou non?

M. John Russo: En ce qui concerne les recours... Je ne peux pas me prononcer sur la norme. Chaque atteinte à la sécurité et chaque situation est différente pour chaque organisme. Nous sommes prêts à collaborer avec les consommateurs canadiens qui ont été touchés. Étant donné que 19 000 personnes ont été touchées au Canada, par l'entremise de notre département des relations avec les consommateurs et des membres de notre équipe d'intervention en cas d'incident, nous abordons chaque cas canadien individuellement et nous collaborons avec ces personnes pour veiller à ce qu'elles soient sûres que leurs renseignements n'aient pas été compromis et n'aient pas été échangés sur le Web profond.

M. Frank Baylis: J'aimerais poser un autre type de question. A-t-on établi une norme liée à la sécurité qui devrait être utilisée? Nous avons des normes pour plusieurs choses, par exemple les prises électriques. Existe-t-il une norme que doivent suivre les entreprises qui recueillent des données personnelles?

M. John Russo: Par exemple, dans le milieu des cartes de crédit, il existe des mesures de protection supplémentaires liées à la conformité à la norme PCI. Equifax Canada a suivi ce processus en 2015. Ce processus d'enrichissement et de mesures correctives relatives à la norme PCI a été utile au Canada. Cela nous a permis de chiffrer nos données. Nous avons transformé nos données de cartes de crédit en jetons.

M. Frank Baylis: Qui établit cette norme?

M. John Russo: L'organisme responsable de la politique et des procédures relatives à la norme PCI.

M. Frank Baylis: La société Equifax a-t-elle adhéré à cette norme pour les cartes de crédit?

M. John Russo: Pour les renseignements de cartes de crédit. Ensuite, il y a d'autres normes que nous devons suivre, par exemple les lois sur les renseignements concernant le consommateur, qui déterminent où nos renseignements sont conservés, comment on y a accès et comment les mettre à jour. Il y a également des lois sur les renseignements concernant le consommateur qui indiquent comment nous devons mener nos affaires à titre d'agence d'évaluation du crédit au Canada.

● (1640)

M. Frank Baylis: Ces normes étaient-elles respectées lorsque cette atteinte à la sécurité s'est produite?

M. John Russo: Au Canada, oui, ces normes étaient respectées.

M. Frank Baylis: Mais l'atteinte à la sécurité s'est produite aux États-Unis, n'est-ce pas? Les Américains ont-ils des normes équivalentes et étaient-elles respectées à ce moment-là?

M. John Russo: Equifax a des normes régissant le transfert de données: les normes que nous avons ici doivent être équivalentes ou supérieures à celles du pays où se trouve l'information. Dans ce cas-ci, des politiques et des procédures étaient en place, mais à la suite d'une erreur humaine et d'une erreur liée aux TI, une cyberattaque a été perpétrée contre notre société, et les responsables ont été en mesure d'accéder à l'information de 19 000 Canadiens.

M. Frank Baylis: Merci.

Le président: Je cède maintenant la parole à M. Weir pour cinq minutes.

M. Erin Weir: Je suis étonné de constater à quel point l'industrie de la surveillance du crédit ne semble pas être très compétitive. Vous avez mentionné qu'il y avait seulement trois grandes entreprises aux États-Unis et deux au Canada. Je suppose que cela va de soi. La mise en place d'un tel réseau exige des coûts importants au départ, et une fois que l'infrastructure est en place, cela ne coûte pas beaucoup plus cher pour couvrir d'autres personnes ou entreprises. C'est peut-être en quelque sorte un monopole naturel.

Pensez-vous que ce manque de concurrence pourrait justifier une réglementation plus rigoureuse de l'industrie de la surveillance du crédit?

M. John Russo: Pour ce qui est de l'industrie, qui serait mieux placé qu'Equifax pour servir les Canadiens en surveillant leur information? Toutes les compagnies de cartes de crédit, les banques et tous ceux avec qui ils font affaire nous font rapport. Cette information, et le fait de pouvoir signaler aux gens le fait que quelqu'un a laissé son empreinte sur leur dossier... Nous pouvons accéder à cette information pour mieux servir nos consommateurs.

Votre question est pertinente. Il n'y a pas beaucoup d'autres secteurs qui disposeraient d'autant de données et qui pourraient mieux aider les consommateurs à lutter contre la fraude et à les alerter lorsque quelqu'un a accédé à leurs renseignements personnels.

Cela dit, pour ce qui est de la prévention de la fraude et de la sensibilisation, nous sommes bien positionnés dans l'industrie.

M. Erin Weir: Je suppose que le risque, lorsqu'on a toutes ces données réunies au même endroit, c'est d'être potentiellement vulnérable au vol, et c'est ce qui s'est produit dans ce cas-ci. Je me demandais si vous ou votre société mère aviez une idée du coût de cette brèche pour Equifax et les consommateurs.

M. John Russo: Certainement dans les millions de dollars. Je n'ai toutefois pas de chiffres à vous donner. Encore une fois, l'enquête est terminée, mais pour ce qui est des coûts qui s'y rattachent, comme M. Kent l'a mentionné, en raison des poursuites et des mesures de sécurité que nous mettons en place, nous voulons aller au-delà des meilleures pratiques de l'industrie. Nous travaillons maintenant avec notre nouveau PDG intérimaire, Paulino Barros, pour nous assurer que la sécurité passe avant tout.

M. Erin Weir: Equifax a-t-elle mis un certain montant de côté pour indemniser les gens dont la sécurité a été compromise?

M. John Russo: Il y a des réserves prévues pour tous les pays où nous sommes présents, en fonction des poursuites dans chacune de nos 24 filiales.

M. Erin Weir: D'accord, mais à ce stade-ci, il semble très difficile de chiffrer le coût de cet épisode, pour l'entreprise ou pour ses clients.

M. John Russo: C'est exact, monsieur Weir. Nous n'avons pas ces chiffres pour l'instant.

M. Erin Weir: D'accord.

Avez-vous l'impression que d'autres bureaux de crédit sont vulnérables à ce type d'atteinte à la sécurité ou qu'ils disposent de mesures de protection adéquates?

M. John Russo: Je ne peux pas parler de nos concurrents ni des procédures et des pratiques qu'ils ont en place. Encore une fois, je suis ici en tant que directeur de la protection de la vie privée au nom d'Equifax Canada. Pour avoir travaillé avec notre département de sécurité et notre équipe de la haute direction ici au Canada, je sais ce que nous faisons et ce que nous avons fait pour nous améliorer, mais je ne peux pas me prononcer sur TransUnion ou d'autres bureaux de crédit ici au Canada.

M. Erin Weir: Avez-vous pris connaissance de certaines failles dans la sécurité, peut-être pas de cet ordre, mais des failles assez importantes au sein de ces bureaux de crédit?

M. John Russo: Encore une fois, je ne peux pas me prononcer sur ce qui s'est passé ailleurs, mis à part ce que j'ai lu dans les médias.

M. Erin Weir: D'accord. Par rapport à ce que vous avez lu dans les médias, savez-vous s'il y a eu des cas semblables au sein d'autres entreprises?

● (1645)

M. John Russo: Aux États-Unis, je sais qu'il y a eu des cas semblables chez certains de nos concurrents ces dernières années. Il y a eu des atteintes à la protection des renseignements personnels qui ont eu une incidence sur les consommateurs.

M. Erin Weir: Merci.

M. John Russo: Je vous en prie. Je vous remercie pour vos questions.

Le président: Merci, monsieur Weir.

Nous allons poursuivre la période de questions.

Je cède maintenant la parole à Mme Shanahan pour sept minutes.

Mme Brenda Shanahan (Châteauguay—Lacolle, Lib.): Merci beaucoup, monsieur le président.

Merci beaucoup à nos témoins d'être ici aujourd'hui, dans le cadre de cette étude. Je viens de prendre connaissance du dossier et je suis profondément troublée par ce que j'ai appris.

Dans mon ancienne carrière, lorsque j'étais banquière — et cela remonte aux années 1980 et 1990 —, nous nous en remettions à Equifax pour obtenir des renseignements. En fait, je me souviens qu'à l'époque, les données sur les consommateurs provenant d'Equifax n'étaient pas toujours exactes. Nous devions régulièrement faire nos propres vérifications. Lorsque nous recevions un rapport sur un consommateur, que ce soit une entreprise ou un particulier, nous devions assurer un suivi et faire nos propres vérifications. Après un certain temps, les consommateurs eux-mêmes se sont rendu compte que leurs dossiers étaient erronés. En effet — et corrigez-moi si je me trompe —, il y a eu un jugement rendu par un tribunal selon lequel les consommateurs avaient le droit de consulter leurs renseignements.

En tant que banquière, je savais que je n'étais pas autorisée à fournir cette information aux clients, car c'est un service qu'Equifax vend aux entreprises, y compris les banques. À ce moment-là, on ne tenait pas du tout compte du consommateur dans l'achat et la vente de cette information.

Aujourd'hui, je vois sur votre site Web que vous vendez aux consommateurs leurs propres renseignements. Vous recueillez de l'information pour laquelle vous êtes payé par vos clients commerciaux et vous la revendez ensuite aux consommateurs à des fins de vérification pour 20 $ par mois. Pouvez-vous m'expliquer le modèle d'affaires qui sous-tend tout cela?

M. John Russo: Bien sûr.

Tout d'abord, en ce qui concerne les inexactitudes ou les renseignements manquants dans les dossiers, sachez que nous sommes prêts à répondre aux questions des consommateurs de partout au Canada. Toni peut vous parler des centres d'appels à l'intention des consommateurs. Nous voulons nous assurer que l'information est juste et exacte. C'est ce que la loi stipule et c'est ainsi que nous gérons notre entreprise. Il faut que...

Mme Brenda Shanahan: En fait, c'est parce que vous vendez cette information. Il faut que ce soit exact. C'est votre modèle d'affaires. Il vous incombe de vous assurer que l'information est exacte; ce n'est pas au consommateur de le faire. S'il y a des activités douteuses sur le compte d'un client, c'est vous qui devriez payer pour mener cette enquête. Si le consommateur veut connaître sa cote de crédit, il devrait y avoir accès à volonté et sans frais, conformément au jugement rendu par le tribunal au Canada.

Je me souviens qu'une fois par année, les consommateurs devaient remplir des documents papier et fournir tous leurs renseignements. Je le sais, car je donnais cette information aux consommateurs. C'était très onéreux et difficile de s'y retrouver sur le site Web. Je dois d'ailleurs vous féliciter, car je vois qu'il est beaucoup plus accessible aujourd'hui. Il suffit d'aller au bas de la page du site Web d'Equifax pour y avoir accès.

Il n'en demeure pas moins que lorsque les consommateurs doivent faire appel à un spécialiste après avoir été victimes d'un vol d'identité, c'est vous qui devriez payer pour cela.

Cela coûte 19,95 $ par mois. J'aimerais savoir comment vous avez déterminé le coût de ce service aux consommateurs. Vous dites qu'ils peuvent annuler en tout temps, mais je peux lire qu'il n'y a aucun remboursement partiel de frais mensuels.

M. John Russo: Si vous faites partie des 19 000 Canadiens qui ont été touchés, nous payons pour ce service. Jusqu'à maintenant, 2 000 Canadiens se sont abonnés à ce service que nous leur offrons gratuitement.

Mme Brenda Shanahan: C'est pour 12 mois, n'est-ce pas?

M. John Russo: Oui, c'est exact.

Mme Brenda Shanahan: Cela devrait être pour toute leur vie, monsieur Russo — pour la vie. Si ces consommateurs se sont fait voler leur numéro d'assurance sociale et leur date de naissance, ils seront potentiellement à risque pendant toute leur vie. Il faudrait y réfléchir.

Est-ce qu'il me reste du temps?

Le président: Il vous reste trois minutes.

Mme Brenda Shanahan: D'accord, allez-y, continuez.

M. John Russo: Je vais demander à Mme Di Napoli de nous donner un aperçu de l'accès à l'information que les consommateurs peuvent généralement obtenir en ce qui concerne la surveillance de leur crédit et la lutte contre la fraude, soit quelque chose d'aussi simple qu'un rapport de crédit gratuit.

● (1650)

Mme Antonietta Di Napoli: Comme je l'ai mentionné, nous offrons des services gratuitement. Les Canadiens ont un accès illimité à leur dossier de crédit tout au long de l'année. M. Russo a mentionné que nous voulons lancer une fonctionnalité permettant aux consommateurs de verrouiller et de déverrouiller leur dossier de crédit à volonté et sans frais. Après les 12 mois, les consommateurs touchés par cette faille auront la possibilité d'utiliser ce service, atténuant ainsi tout risque d'activité frauduleuse dans leur dossier.

Mme Brenda Shanahan: Je suis désolée, mais je ne comprends pas. Qu'est-ce que cela a à voir avec le verrouillage et le déverrouillage?

J'aimerais en savoir davantage sur ce service que vous souhaitez offrir aux consommateurs gratuitement. Qu'est-ce que cela signifie exactement, et en quoi cela va-t-il aider les gens à se protéger?

M. John Russo: À l'instar de ce que nous offrons à nos consommateurs aux États-Unis, comme l'a dit Paulino Barros, notre PDG intérimaire, d'ici la fin de janvier, grâce à ce service, les consommateurs auront un meilleur contrôle de leurs renseignements.

Par exemple, si j'ai un appareil mobile et que je veux verrouiller mon dossier de crédit, grâce à cette fonctionnalité, tant que je ne déverrouille pas mon dossier, aucune banque ni aucun concessionnaire automobile ou propriétaire peut accéder à cette information. Si je veux faire une demande de crédit, je peux facilement réactiver mon dossier, en quelques secondes, afin qu'une banque puisse avoir accès à mon crédit et prendre une décision éclairée à mon sujet.

Mme Brenda Shanahan: Par exemple, cela pourrait se produire si vous perdez votre portefeuille. Ce n'est pas tellement que vous voulez empêcher votre propriétaire d'y accéder, en supposant que vous voulez vraiment obtenir ce bail, mais vous voulez plutôt empêcher les personnes qui ne sont pas censées y avoir accès. Par conséquent, en quoi cela vous protège-t-il?

M. John Russo: Cette fonctionnalité vous permettrait à l'avenir, d'être à la banque, et du bout des doigts, de déverrouiller cette fonctionnalité. Dans ce cas, vous savez très bien que vous allez le déverrouiller pour permettre à votre banquier de prendre une décision concernant votre location ou votre prêt.

En même temps, comme vous l'avez entendu, il peut y avoir un gel du crédit. Ce n'est pas très pratique pour le consommateur, dans bien des cas, car cela peut prendre du temps et une nouvelle authentification pour pouvoir le débloquer.

Nous essayons donc de mettre au point un service convivial que les consommateurs pourront utiliser facilement et instantanément, au moyen d'un iPhone ou d'un autre appareil, pour se protéger. Ensuite, lorsqu'ils seront dans une institution financière pour obtenir du crédit, ils pourront déverrouiller leur dossier pour effectuer cette transaction puis le verrouiller à nouveau par la suite. Ils auront donc cette possibilité à portée de main.

Mme Brenda Shanahan: Il semble qu'il y ait un potentiel de protéger les gens, mais encore une fois, je reviens à l'intégrité des données. Vous achetez et vendez ces données; c'est donc à vous de les protéger. Cela devrait être fait à vos frais. Si vous devez faire payer quelqu'un, facturez plutôt les entreprises, les institutions financières qui utilisent ces données pour ensuite facturer des intérêts de 24 % sur une carte de crédit.

Le président: Merci, madame Shanahan.

Je cède maintenant la parole à M. Kent.

L'hon. Peter Kent: Il est difficile d'intervenir après ma collègue.

Étant donné que la vulnérabilité d'Equifax aux États-Unis n'a pas été décelée par l'entreprise, par l'équipe responsable du correctif d'Apache Struts — c'est plutôt un organisme de sécurité nationale, c'est-à-dire l'équipe d'intervention en cas d'urgence informatique des États-Unis qui en a fait la découverte —, je me demandais simplement, compte tenu des menaces croissantes à la cybersécurité dans le monde, si Equifax Canada serait plus rassurée s'il y avait un organisme national de sécurité semblable qui surveillait ses réseaux, tous les réseaux d'entreprises au Canada, pour empêcher le genre de problèmes qui ont évolué pendant le long délai entre le moment où on a pris connaissance de la vulnérabilité, le piratage et la fermeture du système.

M. John Russo: C'est une excellente idée, monsieur Kent. Nous examinons toutes les solutions possibles pour améliorer nos activités. La sécurité commence par nous, en tant qu'employés, et je peux vous assurer, comme notre PDG intérimaire l'a dit devant le comité sénatorial, que nous réglerons cela et que, quelles que soient les options que proposent le Comité ou d'autres comités parlementaires en vue de mieux servir les Canadiens, nous y sommes favorables.

L'hon. Peter Kent: Ma dernière question concerne le PDG intérimaire. Peut-on savoir quelle sera la durée de son mandat? Est-ce qu'on est à la recherche d'un autre candidat pour le remplacer ou si vous croyez qu'il sera en fonction tout au long des procédures judiciaires qui, comme vous l'avez indiqué, pourraient s'éterniser?

● (1655)

M. John Russo: Cela relève du conseil d'administration, et je ne suis pas au courant de cette décision. Je peux vous assurer que j'ai travaillé avec M. Barros pendant 10 ans. Il a occupé diverses fonctions, que ce soit comme président international ou comme président des activités aux États-Unis, et c'est une personne intègre. Il est ingénieur, alors lorsqu'il dit qu'il va y remédier, il fera tout son possible pour s'assurer que cela se réalise.

L'hon. Peter Kent: Merci.

Puis-je céder mon temps à Sylvie?

Le président: Allez-y. Elle dispose déjà de sept minutes après vous.

[*Français*]

Mme Sylvie Boucher: Maintenant?

[*Traduction*]

Le président: Madame Boucher, vous avez donc neuf minutes.

[*Français*]

Mme Sylvie Boucher: Aujourd'hui, je remplace un de mes collègues.

À la suite de ce que j'ai entendu, j'aimerais poser quelques questions.

Je suis étonnée de voir à quel point la réputation d'Equifax est en train de s'effriter à cause de cette brèche. Malgré tout le respect que je vous dois, je dois dire que vos réponses ne m'éclairent pas suffisamment.

Je vais vous poser plusieurs questions, mais il y en a une en particulier qui me trotte dans la tête depuis tantôt.

À la suite de la brèche qui a eu lieu chez Equifax aux États-Unis, est-ce qu'Equifax Canada, qui protège les Canadiens de ce côté-ci de la frontière, a mis en place une forme de protection beaucoup plus importante relativement à ce genre de fraude?

Par ailleurs, comme chacun le sait, lorsqu'il y a un problème comme une fraude, par exemple, ou lorsque quelqu'un vole son identité, c'est aussi la réputation du consommateur qui est ternie. Vous êtes-vous arrêtés à cette question et avez-vous prévu un dédommagement? Il vous a fallu beaucoup de temps pour découvrir la brèche. Ici, au Canada, on eu un communiqué de presse en septembre.

Enfin, avez-vous prévu rectifier ce genre de situation, qui aurait pu survenir si un de vos consommateurs canadiens s'était fait voler son identité quelque part entre le moment de la fraude et votre réaction?

[*Traduction*]

M. John Russo: Merci beaucoup pour ces deux questions.

En ce qui concerne ce que nous faisons ici, au Canada, comme je l'ai indiqué, nous avons fait appel à PwC et à Mandiant pour collaborer avec toutes les filiales d'Equifax. Nous avons 24 sociétés partout dans le monde, et nous travaillons avec elles.

Pour ce qui est de la confirmation dont j'ai parlé tout à l'heure, non seulement nous avons exigé la mise en place de correctifs, mais nous avons aussi reçu la confirmation que c'était corrigé, que tout était en place. J'ai mentionné dans ma déclaration qu'il fallait 48 heures pour apporter de tels correctifs. Ce délai a été réduit à 24 heures ou moins de façon générale.

Nous peaufinons également les pratiques, les procédures et les normes de l'industrie. Nous voulons être au-dessus des meilleures pratiques de l'industrie. J'ai omis de mentionner que le directeur de la protection de la vie privée relève désormais du PDG intérimaire. La structure de gouvernance chez Equifax a été modifiée en qui a trait à la reddition de comptes. Nous centralisons la sécurité, plutôt que d'avoir un système décentralisé pays par pays. Nous travaillons avec toutes ces personnes. Nous avons également nommé un agent principal de la transformation pour obtenir une meilleure transparence du point de vue de la sécurité et des TI, non seulement au Canada, mais aussi à l'échelle mondiale, afin que cet incident ne se reproduise pas aux États-Unis, au Canada, en Argentine, ni nulle part ailleurs où nous sommes présents.

Pour répondre à votre deuxième question, au sujet de la réputation des consommateurs concernés, sachez que l'équipe de Toni traite chaque cas individuellement. Nous avons des représentants aux centres d'appels qui sont en mesure de répondre aux préoccupations ou aux frustrations des consommateurs en leur expliquant ce qu'il est advenu de leur information. Nous avons mis en place des mesures de protection qui ont été utilisées dans des incidents beaucoup plus graves que le nôtre en vue d'assurer la protection des Canadiens. Encore une fois, notre priorité numéro 1 est le consommateur canadien. J'ai des voisins, des amis et de la famille qui ont été touchés. Cela a des répercussions sur la réputation de tout le monde. Nous avons 10 000 employés partout dans le monde. Cela les touche autant que les Canadiens qui ont été visés.

En même temps, nous voulons nous assurer que les Canadiens jouissent de la meilleure protection qui soit sur le marché en fonction de la réglementation qui s'applique dans chaque pays. La situation réglementaire aux États-Unis diffère de celle du Canada. Nous devons en tenir compte si nous voulons bien représenter ces personnes.

● (1700)

[*Français*]

Mme Sylvie Boucher: Me reste-t-il du temps, monsieur le président?

[*Traduction*]

Le président: Il vous reste quatre minutes.

Mme Sylvie Boucher: D'accord.

[*Français*]

C'est ce que je me demande. Les criminels ou les gens qui ont obtenu ces informations ne s'en serviront pas nécessairement aujourd'hui ou demain, mais ils pourraient s'en servir en 2018, par exemple. Comment Equifax s'y prendra-t-elle pour s'assurer que les données des consommateurs seront protégées à 100 %?

C'est bien beau tout cela, mais partout où passent les consommateurs, on leur demande d'avoir le dossier Equifax. On consulte Equifax et tout est censé être bien beau.

Voici ce qui m'inquiète dans vos réponses. J'ai l'impression que vous avez attendu de voir ce qu'allaient faire les États-Unis avant de saisir la balle au bond ici, au Canada. Vous avez mis des choses en place, mais comment allez-vous procéder maintenant et à l'avenir pour protéger de plus en plus les consommateurs? Comment allez-vous vous assurer que les données personnelles des consommateurs ne seront jamais rendues publiques?

[*Traduction*]

M. John Russo: Concernant les données visées, notre base de données principale sur les consommateurs et le crédit, nos transactions quotidiennes avec les banques, l'information que nous vendons aux banques n'ont pas du tout été touchées ici au Canada. Encore une fois, les 18 000 cas concernaient des paiements, le traitement et des données aux États-Unis, une transaction entre un consommateur et notre marchand américain.

Quant à l'historique, je veux seulement préciser que c'est le 4 ou le 5 septembre que la portion canadienne de l'incident a été mise au jour; tous les spécialistes tous les gens ont travaillé sans relâche. Les cas canadiens ont été mis au jour plus tard, vers la fin du processus d'enquête. Lorsque nous avons été mis au courant le 7 septembre, nous avons avisé tous les commissaires qu'il fallait aviser. Nous avons communiqué avec nos clients. Nous avons fait ce que nous pouvions pour servir ces citoyens canadiens le mieux possible, et à ce moment-là, nous ne savions même pas combien de gens étaient touchés. Nous avons travaillé avec nos équipes d'intervention et de gestion au Canada pour veiller à ce que nous ayons l'information exacte et que nous collaborions avec nos équipes au sud de la frontière pour avoir tous les outils à notre portée. Après avoir obtenu cette information, nous avons fourni aux consommateurs les mesures de protection en place, les services de surveillance de crédit auxquels ils pouvaient s'inscrire pour que leur identité soit protégée, et on vous a parlé des caractéristiques de ce produit.

Pour veiller à ce qu'une telle chose ne se reproduise pas, simplement pour résumer, nous avons renforcé notre analyse de vulnérabilité, nos processus de gestion des rustines et nos procédures. Nous avons réduit la portée des données sensibles contenues dans nos bases de données dorsales. Nous avons également augmenté les restrictions et les contrôles concernant l'accès aux données contenues dans des bases de données essentielles. Nous avons déployé des pare-feu d'applications Web supplémentaires. La liste ne s'arrête pas là pour ce qui est de notre collaboration avec des spécialistes internes et externes. Ce n'est pas que nos systèmes n'étaient pas bons, mais nous voulons faire mieux.

● (1705)

Le président: Merci, madame Boucher.

C'est maintenant au tour de M. Weir, qui sera suivi de M. Erskine-Smith.

M. Erin Weir: Le commissaire à la protection de la vie privée a lancé une enquête sur le piratage d'Equifax. Je me demande si vous pouvez parler de cette enquête et de votre collaboration avec le commissaire.

M. John Russo: Notre équipe travaille avec le Commissariat, ainsi qu'avec son avocate-conseil externe, Mme Bernier. Nous tenons des rencontres régulières avec eux depuis l'appel téléphonique initial dans les 24 premières heures lorsqu'on nous a informés le 7 septembre. Nous travaillons avec eux. Nous collaborons avec tous les commissaires à la protection de la vie privée au Canada. L'enquête est en cours. Encore une fois, nous recueillons les réponses à leurs questions et travaillons à y répondre correctement de sorte qu'ils puissent terminer leur enquête en temps opportun. Nous faisons preuve d'une grande transparence. Encore une fois, la reddition de comptes et la transparence guident notre entreprise, et nous voulons nous assurer que nous faisons de notre mieux pour les consommateurs et tous nos clients.

M. Erin Weir: C'est bien.

Le président: Merci, monsieur Weir.

C'est maintenant au tour de M. Erskine-Smith.

M. Nathaniel Erskine-Smith: J'ai quelques petites questions.

Un rapport préliminaire concernant l'enquête interne a été publié. Y a-t-il un rapport final qui a été rendu public?

M. John Russo: Concernant le rapport de Mandiant?

M. Nathaniel Erskine-Smith: Oui.

M. John Russo: Il s'agit d'un rapport confidentiel.

M. Nathaniel Erskine-Smith: Je vois. Donc même si les données de 145 millions d'Américains et de 19 000 Canadiens sont davantage publiques, l'enquête interne à cet égard ne sera pas rendue publique.

Parmi les 19 000 Canadiens, combien ont choisi de s'abonner gratuitement pour 12 mois?

M. John Russo: Jusqu'à maintenant, environ 1 700 Canadiens l'ont fait. Toni a des données qui datent de ce matin.

M. Nathaniel Erskine-Smith: S'agit-il du nombre de Canadiens touchés qui ont choisi d'adhérer au programme jusqu'à maintenant?

M. John Russo: Pour le premier envoi, c'était 8 000 personnes. Parmi elles, plus de 1 600 y ont adhéré. Pour le deuxième envoi concernant les 11 000 personnes, cela a été fait au cours des derniers jours, et nous constatons donc une augmentation de la proportion de gens qui y adhèrent. C'était 22 %.

M. Nathaniel Erskine-Smith: Vous avez promis de fournir au Comité le nombre de Canadiens qui sont touchés aux États-Unis également. Allez-vous nous fournir de l'information sur le nombre de Canadiens touchés aux États-Unis qui ont adhéré au programme de protection additionnel également?

M. John Russo: Nous déploierons nos plus grands efforts pour le faire.

M. Nathaniel Erskine-Smith: Merci.

Est-ce que des vols d'identité ont été signalés, que ce soit aux États-Unis ou au Canada?

M. John Russo: À ma connaissance, non. Toni peut parler des relations avec les consommateurs.

Mme Antonietta Di Napoli: L'information que j'ai ne concerne que des consommateurs canadiens, et nous n'avons reçu aucune plainte sur des vols d'identité ou des activités frauduleuses de la part de Canadiens que nous avons identifiés.

M. Nathaniel Erskine-Smith: Pour revenir à une question que j'ai posée précédemment, le 8 ou le 9 mars, le DHS a informé Equifax aux États-Unis d'une vulnérabilité sur le plan des données, et des responsables de la sécurité interne ont mené un audit. À votre connaissance, ils n'ont rien trouvé, et vous nous fournirez de l'information le cas échéant. Aucun suivi n'a été fait auprès du DHS.

Est-ce que des hauts dirigeants d'Equifax ont fait un suivi auprès de leur propre équipe de sécurité et lui ont dit « vous n'avez fait qu'un balayage, et n'avez rien trouvé, mais le DHS vient de nous dire que c'était un problème », ou était-ce le silence radio entre le 15 mars et la fin juillet?

M. John Russo: Notre ancien PDG, Rick Smith, a été informé des activités suspectes le 31 juillet.

M. Nathaniel Erskine-Smith: Oui, mais si le DHS a dit à un haut dirigeant qu'il y avait eu un problème... Vous nous direz si un suivi a été fait auprès du DHS, mais est-ce qu'un suivi a été fait à l'interne après le balayage du 15 mars, ou est-ce que cela a suffi à rassurer la haute direction?

M. John Russo: Je comparais à titre de directeur de la protection de la vie privée canadien.

M. Nathaniel Erskine-Smith: D'accord.

M. John Russo: Je n'ai pas cette information. Je ne sais rien à ce sujet. J'en suis désolé.

● (1710)

M. Nathaniel Erskine-Smith: Il me semble que le DHS avise Equifax d'une vulnérabilité en matière de sécurité, un balayage est effectué, et alors... Je devrais également ajouter que selon l'information que j'ai ici, « Equifax n'a pas utilisé le programme du DHS qui permet la mise en commun automatique d'indicateurs de cybermenaces entre le secteur privé et le gouvernement », et on n'a pas bien installé une rustine comme on aurait dû le faire.

Si l'on fait la somme de tous ces facteurs, diriez-vous que votre société mère a fait preuve de négligence?

M. John Russo: Je ne parlerais pas de négligence.

M. Nathaniel Erskine-Smith: Eh bien, permettez-moi de le faire. Dans les cas où des consommateurs canadiens risquent de subir des conséquences, Equifax ne devrait-il pas garantir leur intégrité et s'assurer qu'aucun Canadien ne subit de conséquence ou de perte à cause de la négligence d'Equifax?

M. John Russo: Nous prenons des mesures en surveillant le Web profond pour que les renseignements ne soient pas échangés, qu'ils ne soient pas compromis. Encore une fois, nous offrons les produits de pointe pour nous assurer que les Canadiens sont protégés. Nous avons un centre d'appel qui peut répondre à toutes leurs questions. Nous prenons les mesures exemplaires, nous adoptons toutes les pratiques exemplaires qu'il faut et nous collaborons avec le Commissariat à la protection de la vie privée et suivons leurs conseils afin de faire la meilleure chose pour chaque consommateur canadien.

M. Nathaniel Erskine-Smith: Pouvez-vous fournir au Comité — par écrit, car j'imagine que vous n'avez pas l'information maintenant — de l'information détaillée sur les mesures qu'Equifax prend pour surveiller le Web profond? Je ne comprends pas complètement ce que cela signifie.

Vous avez donné l'exemple de Home Depot, et en réponse à la question de M. Baylis, vous avez dit que pour les services supplémentaires offerts, la période de 12 mois est en quelque sorte une norme concernant ces atteintes à la sécurité, et vous avez parlé de Home Depot.

Toutefois, vous savez peut-être également, bien sûr, que Home Depot a réglé à l'amiable un recours collectif qui a été intenté contre lui concernant cette atteinte à la sécurité des renseignements personnels, et j'imagine que vous pourriez pleinement vous attendre à mettre des fonds de côté pour un recours collectif et à vous assurer que l'intégrité des Canadiens est garantie dans le processus.

M. John Russo: Nous gérons la procédure judiciaire avec notre avocat.

M. Nathaniel Erskine-Smith: Si je vous pose la question, c'est seulement parce que vous avez dit que Home Depot était un bon exemple. Home Depot a versé des centaines de milliers de dollars à des consommateurs canadiens en raison de cette atteinte à la protection des données, et aucun vol d'identité n'a été commis dans ce cas non plus.

Le Comité envisage de recommander que de nouveaux pouvoirs soient conférés au commissaire à la protection de la vie privée, dont celui d'imposer des amendes à une entreprise si elle n'a pas bien su protéger les renseignements personnels

Que pensez-vous de cette recommandation possible?

M. John Russo: En fait, nous avons collaboré avec l'ancien ministère de l'Industrie, l'Association canadienne du marketing et d'autres associations en ce qui a trait à la réglementation et à l'orientation. Nous collaborons avec le Commissariat à la protection de la vie privée pour mieux protéger les consommateurs et leur donner le contrôle de cette information.

M. Nathaniel Erskine-Smith: Pour ce qui est de la capacité d'imposer des amendes, nous étudions la possibilité que de nouveaux pouvoirs soient accordés au commissaire à la protection de la vie privée. Par exemple, au Royaume-Uni, la commissaire à l'information a le pouvoir d'imposer des amendes et elle l'a fait dans le cas de Sony.

Dans ce cas-ci, étant donné qu'Equifax n'a pas agi correctement, à mon avis, sur le plan de la protection des renseignements personnels des Canadiens, des amendes pourraient vraisemblablement être imposées si le commissaire avait de tels pouvoirs.

Seriez-vous pour que le commissaire à la protection de la vie privée puisse imposer des amendes?

M. John Russo: Nous sommes prêts à collaborer avec le gouvernement pour toute nouvelle orientation et tout nouveau règlement.

M. Nathaniel Erskine-Smith: D'accord.

Merci beaucoup.

M. John Russo: De rien.

Le président: Merci, monsieur Erskine-Smith.

J'ai quelques questions.

Puisque je fais partie des députés qui sont allés à Washington, j'ai une question. Nous savons que le commissaire à la protection de la vie privée surveille les données une fois qu'on y a porté atteinte; il intervient.

Quel organisme canadien équivalent surveille le trafic de données? Le département de la Sécurité intérieure des États-Unis le fait, et M. Erskine-Smith en a parlé maintes fois. Quel est l'équivalent canadien? Qui surveille les données et les atteintes possibles pour Equifax Canada?

M. John Russo: Sur le plan de la sécurité?

Le président: Oui.

M. John Russo: Parlez-vous des organismes d'application de la loi?

Le président: Oui.

● (1715)

M. John Russo: Nous collaborons avec la GRC et le FBI de façon générale en ce qui a trait à cet incident; nous répondons à toutes leurs questions. La majorité des gens touchés étaient des Américains. Pour ce qui est des 19 000 Canadiens, nous répondons à l'ensemble des questions de la GRC et d'autres organismes d'application de la loi.

Le président: Cela correspond à ce que différents membres ont dit, soit que pour 145,5 millions d'Américains et 19 000 Canadiens, les données n'ont pas encore été utilisées, mais le problème, c'est cette grosse bombe qui est sur le point d'exploser et l'utilisation qu'en feront d'autres personnes. On nous a dit que les Canadiens n'ont pas été touchés. Avez-vous entendu parler de problèmes aux États-Unis qui auraient été engendrés par l'utilisation des données de ces 145,5 millions de personnes? Ont-elles été utilisées et si c'est le cas, à quoi ont-elles servi?

M. John Russo: À ma connaissance, il n'y a pas eu de tels cas. Peut-être que Mme Di Napoli a entendu quelque chose dans le cadre de ses discussions avec le département des relations avec les consommateurs des États-Unis. De mon côté, toutefois, en tant que directeur de la protection de la vie privée pour Equifax Canada, je n'ai pas vu de cas où à la suite de cet incident, après avoir été touchée et avisée en ce qui a trait aux 19 000 personnes, une personne a déclaré avoir subi des répercussions négatives et s'être fait voler son identité.

Mme Antonietta Di Napoli: À l'instar de M. Russo, je n'ai pas entendu parler de cas où les Américains ou les Canadiens touchés avaient été victimes d'activités frauduleuses ou de vol d'identité.

Le président: J'ai une dernière question.

À combien se sont élevés les résultats d'Equifax Canada en 2016?

M. John Russo: Je pense que c'était environ 250 millions de dollars.

Le président: Cela rejoint en quelque sorte la question qui a été posée ici.

Le vol d'identité peut changer une vie. Nous le savons. Je crois que si je vous demandais une estimation de ce qu'il en coûterait à une personne si la sécurité de ses données était atteinte, je le répète, cela pourrait changer sa vie. Elle risquerait de ne pas pouvoir s'acheter une maison et une voiture pendant de nombreuses années. Par conséquent, elle pourrait vivre beaucoup de situations traumatisantes.

Je dirais que 50 000 $, ce n'est pas beaucoup pour assurer aux Canadiens que vous réglerez toute brèche. Encore une fois, comme l'a dit Mme Shanahan, vous êtes responsables de ces données. Vous avez la responsabilité de vous en occuper. Je pense que vous devriez, à tout le moins, couvrir tous les coûts, voire les extras, du fait de cette atteinte à la protection des données qui, comme nous le savons tous et comme M. Erskine-Smith l'a mentionné, s'est produite par votre faute. Vous l'avez admis. Vous avez présenté des excuses à cet égard.

Notre comité a terminé ses travaux. Je vous mets au défi de prendre les bonnes mesures et de vous assurer que l'intégrité des Canadiens est garantie. Le problème, c'est que nous ne savons pas à quel moment les Canadiens en vivront les répercussions, mais espérons qu'Equifax prendra les choses en main.

Madame Di Napoli, monsieur Russo, je vous remercie d'être venus comparaître et d'avoir répondu à des questions difficiles.

M. John Russo: Monsieur le président, mesdames et messieurs, je vous remercie.

Mme Antonietta Di Napoli: Merci.

Le président: Nous allons suspendre la séance pendant cinq minutes, et nous passerons à certains travaux par la suite.

● (1715)

(Pause)

● (1720)

Le président: Nous reprenons.

Nous sommes saisis d'une motion de M. Erskine-Smith, que la plupart d'entre vous ont vu.

M. Nathaniel Erskine-Smith: Je crois que vous avez tous la motion. Elle est assez simple.

La personne proposée pour le poste de commissaire au lobbying du Canada a été présentée jeudi dernier à la Chambre, je crois. L'idée, c'est de faire comparaître Mme Bélanger devant notre comité pour une heure.

L'hon. Peter Kent: Nous avons communiqué avec elle dans ses fonctions actuelles il y a quelques semaines. Je crois que c'est fort louable et qu'il est fort probable qu'elle puisse comparaître.

M. Nathaniel Erskine-Smith: C'est ce que je présume.

Le président: Pour les fins du compte rendu, peut-elle? Je crois que oui.

Le greffier du comité (M. Hugues La Rue): Oui. J'ai communiqué avec elle et elle peut comparaître devant nous mercredi.

Le président: D'accord. Y a-t-il d'autres interventions?

Nous passons au vote.

(La motion est adoptée. [Voir le *Procès-verbal*])

Le président: Nous poursuivons la séance à huis clos.

[*La séance se poursuit à huis clos.*]