CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

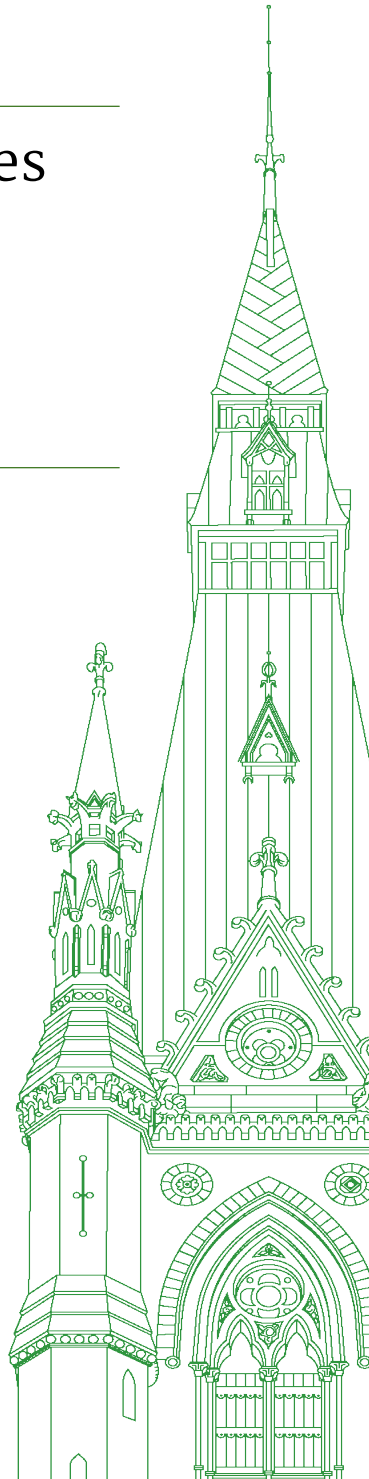
43e LÉGISLATURE, 1re SESSION

Comité permanent de l'industrie, des sciences et de la technologie

TÉMOIGNAGES

NUMÉRO 008

Le jeudi 12 mars 2020



Présidente : Mme Sherry Romanado

Comité permanent de l'industrie, des sciences et de la technologie

Le jeudi 12 mars 2020

● (1105)

[*Traduction*]

La présidente (Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Bonjour à tous.

Conformément au paragraphe 108(2) du Règlement, nous poursuivons notre étude sur les appels frauduleux au Canada.

Nous souhaitons la bienvenue à M. Matthew Gamble de la section canadienne de l'Internet Society, et à M. John Lawford du Centre pour la défense de l'intérêt public.

Messieurs, vous avez droit à 10 minutes chacun pour votre exposé, après quoi nous passerons aux questions des membres du Comité. Si vous me voyez agiter ce petit carton jaune, c'est un avertissement que je vous sers pour que vous sachiez qu'il ne reste que trente secondes au temps imparti et qu'il faudra bientôt passer à l'intervenant suivant.

Je rappelle aux gens présents dans la salle qu'ils ne peuvent pas prendre de photo pendant la séance du Comité.

Je cède donc d'abord la parole à M. Gamble. Vous avez 10 minutes.

M. Matthew Gamble (directeur, Internet Society Canada Chapter): Bonjour à tous.

Je m'appelle Matthew Gamble et je suis directeur de la section canadienne de l'Internet Society. Je suis heureux de comparaître devant vous aujourd'hui pour traiter des appels importuns et frauduleux au Canada.

J'aimerais d'abord vous présenter brièvement notre organisation. Nous sommes une société à but non lucratif qui intervient dans différents dossiers juridiques et politiques pour militer en faveur d'un Internet ouvert, accessible et abordable pour tous les Canadiens. Un Internet ouvert est une tribune permettant les échanges d'idées et de points de vue, mais dans les limites imposées par la loi. Un Internet accessible permet à toutes les personnes et à toutes les entités d'avoir librement accès à des sites Web où s'épanouissent toutes les formes d'expression autorisées par la loi. Un Internet abordable est un mode d'accès aux services en ligne à un prix raisonnable pour tous les Canadiens. Vous trouverez sur notre site Web de plus amples détails sur notre organisation, nos activités et nos publications.

Nous sommes pleinement conscients des répercussions qu'ont sur les Canadiens les appels frauduleux et importuns. Selon les résultats d'une étude menée par Truecaller, chaque Canadien reçoit en moyenne 12 appels non sollicités par mois. Si j'en crois mon expérience personnelle, j'ai l'impression que ce nombre est en fait beaucoup plus élevé.

Le nombre d'appels automatisés frauduleux, comme ceux de l'arnaque téléphonique liée à l'Agence du revenu du Canada (ARC), ne cesse d'augmenter, et ce, pour plusieurs raisons. Ces appels ne coûtent pas cher, n'entraînent que peu de conséquences et permettent parfois, quoique rarement, de soutirer à d'innocents Canadiens leur argent durement gagné. L'effet cumulé des appels frauduleux liés à l'ARC et des innombrables appels nous offrant des services comme le nettoyage des conduits d'air fait en sorte que les gens sont devenus hésitants à répondre lorsqu'ils reçoivent un appel d'un numéro inconnu et qu'ils perdent de plus en plus confiance en leur propre téléphone.

Pour vous donner une idée de mon expérience dans ce domaine, je peux vous dire que j'ai été, il y a 13 ans, le concepteur et l'architecte en chef du service Gardien télémarketing de Primus Canada, une mesure de protection qui a permis de faire un important pas en avant dans la lutte contre les appels non sollicités. Ce service a empêché des millions d'appels de télémarketing de se rendre jusqu'aux Canadiens grâce à une liste d'appelants indésirables connus qui a été établie avec la contribution des citoyens.

La situation a cependant changé du tout au tout depuis l'époque où ce service a été mis en place, si bien que les systèmes qui filtrent les appels en tablant uniquement sur l'identification de la ligne appelante ne sont plus efficaces. Il est désormais monnaie courante que des gens mal intentionnés usurpent des numéros de téléphone valides ou génèrent aléatoirement des numéros semblables à celui de la personne appelée, ce qu'on appelle la mystification de voisinage.

Ces acteurs malveillants de la nouvelle vague exploitent les principes mêmes s'inscrivant dans l'ADN de nos réseaux de télécommunications. Ces réseaux ont été érigés sur la base d'une confiance explicite entre les entreprises de télécommunications et conçus de manière à ce que tous les appels puissent être acheminés quoiqu'il arrive. Ces entreprises n'examinent pas le contenu des appels avant de les acheminer et peuvent être nombreuses à intervenir pour un même appel, tant et si bien qu'il devient difficile, voire impossible, d'en déterminer la source.

À première vue, la solution au problème des appels automatisés peut sembler plutôt évidente. Il suffit d'interdire la falsification de l'identité de l'appelant. Les choses ne sont malheureusement jamais aussi simples qu'elles le paraissent. On peut être justifié de vouloir camoufler l'identité de l'appelant pour plusieurs bonnes raisons liées aux fonctionnalités d'appel, aux considérations commerciales et à la protection de la vie privée.

On peut imaginer, par exemple, une intervenante d'un refuge pour femmes qui essaie de joindre chez elle une victime de violence conjugale sans que son conjoint sache que l'appel vient du refuge. Il est utile en pareil cas de pouvoir falsifier l'identification de l'appelant pour masquer la provenance de l'appel.

D'autres fonctions téléphoniques encore plus simples, comme le renvoi d'appel ou l'utilisation de différents fournisseurs de service de téléphonie par la même entreprise, sont fondées sur la possibilité de modifier au besoin l'identifiant de la ligne appelante. C'est une fonction qui fait partie intégrante de notre réseau téléphonique commuté public et qui ne pourrait pas être facilement désactivée sans causer d'importants dommages collatéraux.

Comme on vous l'a indiqué cette semaine, le CRTC coordonne ses efforts avec ceux des intervenants de l'industrie canadienne des télécommunications pour s'attaquer à ce problème sur différents fronts. On veut notamment exiger un identifiant de ligne appelante valide pour tous les appels, demander au Comité directeur sur l'interconnexion du CRTC de concevoir un mécanisme de traçage des appels, et exiger des entreprises de télécommunications qu'elles mettent en place le cadre de normes STIR/SHAKEN pour l'authentification et l'identification des appels.

Parmi toutes ces initiatives, c'est l'application des normes STIR/SHAKEN qui interpelle le plus notre organisation. Élaborées à partir de technologies inspirées du travail des groupes consultatifs sur les normes applicables à l'Internet, les normes STIR/SHAKEN devraient rétablir la confiance des consommateurs envers l'identification de la ligne appelante grâce au recours à une signature numérique inscrite dans les métadonnées de l'appel. Lorsqu'elles seront pleinement mises en œuvre, ces normes permettront aux entreprises de télécommunications d'établir en temps réel la source des appels et de filtrer aisément ceux qui usurpent des numéros connus comme ceux de l'ARC et de la GRC, par exemple.

Il y a un obstacle important qui empêche la mise en œuvre des normes STIR/SHAKEN au Canada et qui nous a incités à intervenir dans ces différents processus du CRTC. Ce nouvel outil pourrait causer de sérieux problèmes liés aux politiques, à la technologie et à la protection de la vie privée qui n'ont pas encore été réglés.

Parlons d'abord des politiques. Les normes STIR/SHAKEN ont été élaborées par le Groupe d'études sur l'ingénierie Internet (IETF), puis adoptées par bon nombre des grands fournisseurs des États-Unis qui les utilisent au sein de leurs propres réseaux. Comme ce sont de grandes entreprises qui ont pris les mesures d'adaptation nécessaires à cette fin, plusieurs des décisions prises au départ concernant les politiques et la conception profitent à ces grandes entreprises au détriment des plus petites.

La plus importante de ces décisions a été de permettre seulement à l'entreprise téléphonique à laquelle le numéro appartient de confirmer sans réserve l'identité de l'appelant. C'est une mesure qui peut sembler logique, mais il n'est pas aussi simple qu'on le croit d'établir à qui appartiennent les numéros de téléphone. Plus de 1 200 entités sont enregistrées auprès du CRTC comme revendeurs de services de télécommunications. Il s'agit généralement de fournisseurs de services téléphoniques qui exploitent leur entreprise sans détenir en propre aucun numéro de téléphone. Ces entités s'en remettent plutôt à des ententes d'accès de gros conclues avec les grands fournisseurs. Ces entreprises offrent des services de télécommunications très utiles aux Canadiens, comme les plateformes d'autocommutateur privé en entreprise, les services résidentiels en marge du réseau et d'autres produits téléphoniques novateurs.

Comme vous le savez, le CRTC a demandé à tous les fournisseurs de services de télécommunications, y compris les fournisseurs non dotés d'installations, de mettre en œuvre les normes STIR/SHAKEN.

Les entreprises de télécommunications de plus petite taille se retrouveront dans une situation extrêmement désavantageuse si les normes et les politiques élaborées jusqu'à maintenant sont mises en œuvre sans qu'aucun changement y soit apporté. S'il leur est impossible d'apposer elles-mêmes une signature adéquate sur leurs propres appels, on les situera dans une classe inférieure par rapport aux grandes entreprises. Avec le temps, cela pourrait inciter des clients à se tourner plutôt vers les grandes entreprises de télécommunications capables d'attester adéquatement de la provenance de tous les appels. On créera ainsi un système de télécommunications à deux paliers au Canada, suivant qui est capable ou non d'apposer sa signature numérique. Si l'on devait en arriver là, on réduirait à néant tous les efforts déployés par les petites entreprises depuis de nombreuses années pour innover et accroître leur capacité concurrentielle.

Du point de vue technologique, les normes STIR/SHAKEN sont problématiques du fait qu'elles exigent une interconnexion entre les entreprises de télécommunications au moyen de points d'interface de service (PIS) fondés sur un protocole Internet (IP). Alors que les petits fournisseurs dont je parlais sont généralement reliés à une entreprise plus grande en amont via la technologie PIS, les interconnexions entre les grandes entreprises de télécommunications canadiennes se font principalement au moyen de l'ancienne technologie fondée sur le multiplexage par répartition dans le temps (MRT). Il est presque ironique de constater que les petites entreprises de télécommunications utilisant l'interconnexion PIS qui sont les mieux placées pour assurer le déploiement de cette technologie sont mises de côté dans ce processus, mais c'est la réalité dans le contexte actuel du marché canadien.

Enfin, nous nous inquiétons vivement des répercussions de la mise en œuvre des normes STIR/SHAKEN sur la protection de la vie privée des consommateurs. L'apposition d'une signature numérique aux appels permettra à l'entreprise d'arrivée de compter sur une vaste gamme de données vérifiées sur la source et la destination des appels. On espère que les fournisseurs de services de télécommunications pourront ainsi concevoir des solutions comme Gardien télémarketing qui ne se limiteront toutefois pas au numéro de l'appelant, mais pousseront davantage l'analyse pour retracer des éléments comme l'entreprise à la source de l'appel. C'est semblable à ce qui se fait pour le filtrage des pourriels dans l'espace Internet. Les données analytiques sont basées non seulement sur l'adresse de la source, mais aussi sur la réputation des réseaux qui acheminent l'appel.

Tout cela peut sembler fort intéressant, mais il n'en découle pas moins de graves préoccupations quant à la protection de la vie privée des Canadiens du fait que certaines entreprises ont choisi de confier cette fonction analytique en sous-traitance à une autre entité commerciale. Celle-ci pourrait facilement en profiter pour alimenter les bases de données commerciales existantes afin de dégager des profils encore plus détaillés des ménages canadiens. On pourrait par exemple déduire des données collectées qu'un ménage commande des mets à emporter tous les soirs, un renseignement précieux pour une compagnie d'assurance-vie qui pourrait y voir un mode de vie malsain accroissant les facteurs de risque.

En conclusion, bien que nous puissions sembler nous opposer au déploiement des normes STIR/SHAKEN, c'est tout à fait le contraire. Nous sommes persuadés que la mise en place de ces normes au sein des réseaux de télécommunications canadiens est une avancée essentielle si l'on veut regagner la confiance des consommateurs et les protéger contre la fraude. Nous voulons simplement que toutes les parties prenantes comprennent bien qu'il convient de s'assurer que cette mise en œuvre se déroule dans les règles et de façon ouverte et transparente. Comme c'est le cas pour toutes les autres technologies basées sur Internet, nous devons veiller à ce que tous les intervenants, y compris les petits fournisseurs de services de télécommunications, puissent participer à armes égales.

Enfin, et surtout, nous devons nous assurer d'inscrire dans l'ADN de toute nouvelle technologie déployée de solides mesures de protection de la vie privée. Comme nous avons pu l'apprendre avec Internet, essayer d'améliorer la protection de la vie privée au sein d'un système déjà déployé, c'est comme tenter de réparer un aéronef en plein vol. C'est une mission impossible qu'il faut absolument éviter.

Je vous remercie pour le temps que vous m'avez consacré et je serai ravi de répondre à toutes vos questions.

● (1110)

La présidente: Merci beaucoup.

Nous passons maintenant à M. Lawford. Vous avez 10 minutes.

M. John Lawford (directeur exécutif et avocat général, Centre pour la défense de l'intérêt public): Madame la présidente, mesdames et messieurs les députés, je vous remercie.

Je m'appelle John Lawford et je suis directeur exécutif et avocat général au Centre pour la défense de l'intérêt public, ici même à Ottawa.

Notre centre est un organisme de bienfaisance enregistré qui est constitué en vertu d'une loi fédérale. Nous fournissons des services juridiques et effectuons des travaux de recherche pour la défense des intérêts des consommateurs vulnérables à l'égard de services publics importants.

Nous participons fréquemment aux audiences du CRTC et représentons les intérêts des consommateurs relativement aux services bancaires de détail et aux systèmes de paiement auprès de l'Agence de la consommation en matière financière du Canada (ACFC), du ministère des Finances et de l'Ombudsman des services bancaires et d'investissement (OSBI).

La fraude à la consommation est un dossier épineux. Les entreprises l'évitent parce qu'elles ne veulent pas s'exposer au risque d'être tenues responsables à l'égard de la fraude. La police ne dispose pas des ressources nécessaires pour contrer un phénomène d'aussi grande envergure et d'une complexité technique extrême qui varie d'un vecteur à un autre. Les instances réglementaires comme le CRTC délimitent leurs sphères de compétence le plus étroitement possible afin de ne pas être responsables de ce problème qu'elles voient comme un véritable gouffre opérationnel.

Pour chaque victime, la fraude est source d'humiliation et a souvent des effets dévastateurs. C'est un sujet que nous cherchons tout naturellement à éviter comme nous le faisons pour la pauvreté du fait que l'injustice flagrante et la douleur infligée aux victimes nous rebutent. Nous voulons donc féliciter votre comité de tenir des audiences comme celles d'aujourd'hui sur les appels frauduleux, l'un des aspects de cette problématique.

Les statistiques à notre disposition sur l'ampleur du problème de la fraude sont tellement fragmentaires qu'elles constituent en elles-mêmes un obstacle dans notre lutte contre ce problème. Elles ne proviennent d'aucune source officielle ou bien définie. Nous avons des données récentes du Centre antifraude du Canada (CAFC) qui indiquent pour l'année 2019 quelque 46 000 signalements avec 19 000 victimes et des pertes d'environ 100 millions de dollars.

Les signalements reçus par le CAFC portaient principalement sur des fraudes commises par téléphone et via Internet. Pour sa part, l'ACFC rapportait par exemple pour 2007, 15 millions de victimes de fraudes ayant totalisé des pertes de 450 millions de dollars, ce qui incluait sans doute d'autres types de fraudes, comme celles commises en personne. Les sources de données plus fiables ou plus à jour sont cependant plutôt rares. Ainsi, le CRTC a uniquement des chiffres sur les plaintes relatives à la liste de numéros de téléphone exclus, mais pas de statistiques précises sur les fraudes.

D'après ce que nous a appris notre travail sur le terrain, nous estimons plutôt que l'ampleur du phénomène de la fraude téléphonique serait de 10 à 100 fois plus grande que ce qu'indiquent les chiffres du CAFC. Nous parlons ici de la fraude au moyen d'appels et de textos utilisant notamment les numéros de téléphone courants, mais sans tenir compte des arnaques par Internet dont on peut être la cible sur son téléphone mobile.

À la lumière de nos contacts directs avec les consommateurs et les groupes représentant les aînés et les personnes à faible revenu, comme la Fédération nationale des retraités et citoyens âgés et ACORN Canada, nous sommes également d'avis que la fraude téléphonique cible expressément et touche démesurément les aînés et les personnes à faible revenu, y compris certains néo-Canadiens. Plus encore que tous les autres Canadiens, ces gens-là n'ont vraiment pas les moyens d'être victimes d'une fraude.

Je ne traiterai pas de la fraude par transfert non autorisé de numéro ou de carte SIM. Il s'agit toutefois d'une nouvelle problématique à laquelle il faut s'attaquer sans tarder. Vous entendrez d'ailleurs tout à l'heure le témoignage de Randall Baran-Chong, victime de ce genre de fraude qui milite avec éloquence en faveur de la recherche d'une solution à cette arnaque dévastatrice. Je lui laisse le soin de vous expliquer de quoi il s'agit exactement. Je signale toutefois que notre centre a réclamé la tenue d'audiences publiques du CRTC avec la participation de groupes de consommateurs, d'utilisateurs des réseaux sans fil, de l'Association canadienne des télécommunications sans fil (ACTS) et des grands fournisseurs. Je dois cependant vous dire que tant le CRTC que l'ACTS ont refusé jusqu'à maintenant la tenue d'une enquête publique.

J'aimerais donc plutôt vous entretenir aujourd'hui de la fraude téléphonique dans sa forme traditionnelle, à savoir celle qui vise à amener une victime à répondre à son téléphone, résidentiel ou mobile, et à engager la conversation avec un fraudeur dont le but ultime est d'inciter la victime à lui transférer des fonds ou à lui révéler suffisamment de renseignements personnels pour qu'il puisse lui-même transférer des fonds à l'insu de la victime. Pour ce genre de fraude, on peut avoir recours à la falsification des numéros ou des noms affichés de telle sorte que la victime croit à tort qu'elle reçoit un appel d'une organisation légitime comme un ministère du gouvernement ou le bureau de police local.

Pour que cette forme traditionnelle de fraude par téléphone soit vraiment efficace, il faut toutefois pouvoir miser sur l'automatisation pour générer un important volume d'appels. Plus les appels sont nombreux et acheminés efficacement du point de vue du fraudeur, meilleures sont les chances de piéger une victime.

Je peux vous dire que des milliards d'appels sont faits chaque année à des numéros de téléphone canadiens, et qu'au moins des dizaines de millions d'entre eux sont des appels frauduleux automatisés à la première étape de l'escroquerie. Voici comment cela fonctionne. Un programme écrit par le fraudeur appelle des milliers de téléphones en l'espace d'une heure à partir généralement d'un numéro de téléphone falsifié. Aucune intervention humaine n'est nécessaire. Vous n'avez qu'à multiplier le tout par le grand nombre de programmes, d'ordinateurs et d'autres fraudeurs qui se livrent au même manège en ciblant différents indicatifs régionaux pour vous faire une petite idée de l'ampleur du problème.

● (1115)

À l'étape deux, c'est la victime potentielle qui répond et qui, au lieu de raccrocher, écoute le message enregistré, parce que la source de l'appel lui inspire de la confiance ou de la crainte, ou simplement parce qu'elle se sent seule et recherche un contact humain, quel qu'il soit. Si la victime appuie sur le « 1 » pour entendre le message, elle parle directement à un fraudeur qui tentera de la mener jusqu'au transfert de fonds.

Les appels automatisés sont donc autant de lignes lancées à l'eau dans une mer de détenteurs d'un appareil téléphonique. Les appels se rendant jusqu'à la deuxième étape de conversation directe avec le fraudeur sont relativement beaucoup moins nombreux. Leur nombre inférieur demeure toutefois très considérable, bien que nous ne sachions pas à quel point. C'est à cette étape que la fraude intervient.

Quoi de neuf? Qu'est-ce qui a changé récemment dans ce domaine pour nous donner l'impression que la fraude téléphonique a pris des proportions épidémiques? Ce n'est peut-être pas le bon moment pour parler d'épidémie. Pourquoi les Canadiens, et surtout les aînés et les personnes à faible revenu, sont-ils de plus en plus nombreux à être victimes d'appels frauduleux?

La situation s'explique du fait que la technologie a permis de démocratiser le système téléphonique. Auparavant, pour pouvoir composer plusieurs numéros à la fois, il fallait connaître le logiciel administrant le réseau de la compagnie de téléphone. Ce logiciel ne permettait qu'un certain débit de numéros composés. La quasi-totalité du système téléphonique repose désormais sur un protocole Internet. Il est ainsi possible pour un petit nombre de programmeurs informatiques d'effectuer plusieurs millions d'appels à plusieurs millions de numéros.

La téléphonie IP a permis l'entrée de nouveaux joueurs et de nouveaux services sur le marché, mais a aussi entraîné une explosion de la fraude, notamment parce qu'il est possible avec le protocole IP de falsifier des numéros, ce qui est plus difficile avec l'ancien logiciel. Reste quand même que plus on lance de lignes à l'eau, plus on a de chances d'attraper du poisson.

Les intervenants de l'industrie téléphonique, et tout particulièrement les entreprises depuis longtemps en place comme Bell Canada et Telus, ne connaissent que trop bien cette réalité, comme c'est le cas pour le CRTC qui considère à tout le moins que les appels automatisés indésirables relèvent de sa compétence en matière de télémarketing et, dans une moindre mesure, à l'égard de la liste des numéros de téléphone exclus. Tous ces intervenants s'emploient à contrer la falsification des numéros. Le CRTC exige déjà que ces entreprises bloquent les numéros manifestement falsifiés comme 000-000-0000. Tous travaillent à la mise en œuvre des normes STIR/SHAKEN dont on vient de vous parler, lesquelles ne fonctionnent vraiment que pour les appels totalement fondés sur un protocole IP. Il s'agit en fait d'attribuer une cote de confiance à chaque appel. Ainsi, le logiciel de destination peut systématiquement bloquer les appels provenant probablement de composeurs automatiques informatisés. Ces deux mesures vont être utiles, mais elles ne vont pas régler le problème une fois pour toutes.

Il y a aussi de nouvelles technologies de blocage des appels au niveau du réseau, comme celle conçue par Bell Canada qui a adressé une demande au CRTC pour que l'on autorise l'utilisation d'algorithmes fondés sur l'intelligence artificielle en vue de détecter les sources probables d'appels automatisés. Cela comprend également certains dispositifs confidentiels à sécurité intégrée que l'on s'est engagé à mettre en place et le blocage de tout appel suspect acheminé via le réseau de Bell qui est très vaste au Canada.

Bien que ces mesures créent de l'inquiétude chez les autres entreprises qui doivent utiliser le réseau de Bell pour acheminer les appels de même que pour les consommateurs légitimes qui risquent de voir leurs appels être bloqués sans motif valable, elles pourraient permettre de réduire le volume des appels semblables, l'un des aspects du problème qui nous intéresse. On essaie de mettre l'automatisation à contribution pour contrer l'automatisation. Tout bien considéré, nous pensons qu'il s'agira sans doute d'une mesure bénéfique, mais nous sera-t-elle offerte gratuitement ou aurons-nous des frais à payer?

Enfin, pour que l'on puisse vraiment s'attaquer au contenu de ces appels frauduleux, il faudrait que le CRTC jouisse de pouvoirs accrus en la matière. Nous recommandons que l'on s'inspire de la loi américaine de protection des consommateurs de services téléphoniques, et que l'on adopte une loi visant expressément à contrer les appels frauduleux, par exemple sur le modèle de la loi des États-Unis sur le télémarketing, la fraude et les abus à l'égard des consommateurs. Dans ce contexte, nous notons également que le rapport faisant suite à l'examen de la législation en matière de radiodiffusion et de télécommunications aurait pu être l'occasion de recommander des modifications à la Loi sur les télécommunications afin de conférer au CRTC davantage de pouvoirs pour lutter contre les appels frauduleux, ou encore de recommander l'adoption d'une loi visant expressément la lutte contre les fraudes téléphoniques, qu'elle soit administrée par le CRTC ou peut-être par un nouveau commissaire aux données.

Nous avons également besoin d'un bassin plus centralisé, plus complet et plus fiable de statistiques et de rapports sur les fraudes par téléphone et par Internet. Les données à ce sujet doivent pouvoir être collectées et diffusées à intervalles réguliers. En dernier lieu, il faut que le Parlement continue à s'intéresser à la fraude téléphonique en assurant la surveillance nécessaire à l'intérieur d'une démarche démocratique. C'est un enjeu trop important pour qu'on laisse les instances réglementaires, les entreprises concernées et la police continuer à se renvoyer la balle à ce sujet.

Merci beaucoup.

● (1120)

La présidente: Merci beaucoup, monsieur Lawford.

Nous commençons maintenant le premier tour de questions où chacun aura droit à six minutes en débutant par Mme Gray.

Mme Tracy Gray (Kelowna—Lake Country, PCC): Merci, madame la présidente.

Je vais adresser ma première question à M. Lawford.

Vous avez indiqué que les personnes âgées et celles qui ont un faible revenu sont plus vulnérables à la fraude téléphonique. Je sais que vous avez visité ma circonscription de Kelowna—Lake Country, et j'ai moi-même entendu parler de gens qui ont été ciblés, aussi bien en mandarin qu'en pendjabi, par des fraudeurs relativement à des questions touchant l'immigration ou l'impôt, et plus particulièrement Revenu Canada.

D'après vous, quelles méthodes de sensibilisation pourraient être mises de l'avant de telle sorte que les aînés et les autres personnes vulnérables au Canada risquent moins d'être victimes d'escroqueries semblables?

M. John Lawford: Je crois que l'on pourrait en faire bien davantage pour augmenter la résilience des consommateurs canadiens. C'est seulement un volet de la problématique, mais c'est un bon point de départ.

Certains efforts ont été déployés dans d'autres secteurs où les consommateurs sont victimes de fraudes dans des langues autres que le français et l'anglais. Pour l'instant, aucune des instances en place n'est responsable de ce phénomène dans le cadre de son mandat, et je ne vois pas vraiment qui pourrait s'en charger. Le CRTC pourrait probablement s'acquitter de ce genre de tâche en produisant des outils pour la sensibilisation des citoyens et des collectivités, mais c'est vraiment l'une de ces situations où il convient de communiquer directement avec les consommateurs en utilisant un langage qu'ils comprennent.

Je ne sais pas trop comment on devrait s'y prendre pour déléguer dans ces collectivités une personne de confiance qui leur communiquerait directement les mises en garde nécessaires, mais il s'agit néanmoins d'une excellente idée.

Mme Tracy Gray: Merci.

Dans vos observations préliminaires, vous avez dit préconiser la tenue d'une enquête publique sur le phénomène de la fraude en précisant que vous avez fait des démarches auprès du CRTC à cet effet.

Pourriez-vous nous en dire plus long sur la teneur exacte de votre requête et sur la réponse que l'on vous a faite?

M. John Lawford: Certainement. C'est au sujet du problème de transfert non autorisé de carte SIM dont Randall va vous parler dans la deuxième portion de votre séance.

Il y a eu jusqu'à maintenant un échange de lettres entre le CRTC et l'Association des télécommunications sans fil pour savoir ce qui se fait exactement pour éviter ce transfert non autorisé, car d'autres pays, comme l'Australie, ont déjà adopté des règlements pour l'interdire. Il y a donc cet échange de lettres sur le site Web, ce qui m'incite à poser directement la question. Qu'attendez-vous pour agir? Pourquoi n'y a-t-il pas une enquête publique comme c'est habituellement le cas au CRTC?

Jusqu'à maintenant, les entreprises concernées ont répondu qu'elles ne voulaient pas discuter de fraude sur les tribunes publiques pour éviter que les escrocs ne soient au courant de leurs approches. Quant au CRTC... je ne sais pas pourquoi on ne veut pas tenir une enquête publique. Je pense que le CRTC souhaite voir l'industrie régler rapidement la question. Cependant, je ne comprends pas pourquoi on procède de cette façon, car l'obscurité est habituellement propice à la fraude; il est préférable d'en discuter sous les réflecteurs. En général, les meilleures règles sont celles qui sont adoptées dans le cadre d'un processus ouvert et transparent.

● (1125)

Mme Tracy Gray: Merci.

J'ai aussi quelques questions pour M. Gamble.

Vous avez indiqué que ce sont les grandes entreprises qui ont travaillé à l'établissement du cadre nécessaire à l'application des normes STIR/SHAKEN et que vous êtes intervenu pour faire valoir le point de vue de certaines organisations de plus petite taille.

Est-ce que les choses ont changé? Est-ce que l'on consulte maintenant les petits fournisseurs? Leur est-il désormais possible d'avoir leur mot à dire et d'exprimer leurs idées?

M. Matthew Gamble: Bien que seulement quelques petites organisations soient représentées dans le cadre du processus actuel du groupe de travail du Comité directeur sur l'interconnexion du CRTC, leurs préoccupations sont bel et bien prises en compte.

Je vous dirais que bon nombre de ces petites entreprises n'ont tout simplement pas les ressources nécessaires pour participer à ce genre d'exercice. Pour une entreprise qui ne compte que deux ou trois employés, il est difficile d'en libérer un pour contribuer à l'élaboration de ces normes techniques.

Dans les mémoires soumis au CRTC jusqu'à maintenant, les entreprises reconnaissent qu'il s'agit d'un problème, mais indiquent qu'il pourrait être réglé ultérieurement, sans toutefois préciser aucune échéance.

Mme Tracy Gray: J'ai l'impression que l'on écoute les différents points de vue, mais que l'on va de l'avant avec la mise en oeuvre sans vraiment tenir compte des préoccupations et des suites possibles.

M. Matthew Gamble: Tout à fait. On semble maintenant penser qu'il faut aller de l'avant avec la mise en oeuvre au sein des grandes entreprises en attendant que les plus petites reprennent éventuellement le terrain perdu. Comme vous le savez, il est toujours problématique d'essayer de réparer quelque chose une fois le processus en marche.

Mme Tracy Gray: Les petites entreprises ne devraient-elles pas mettre en oeuvre ces normes en même temps que les autres?

D'un point de vue technique, il faudrait que ces normes puissent s'appliquer partout simultanément, mais ces entreprises-là ne disposent pas des capacités nécessaires. Est-ce bien ce que vous êtes en train de nous dire?

M. Matthew Gamble: C'est exact. L'autre conséquence possible, c'est qu'elles seraient obligées d'avoir recours à un seul fournisseur pour leur approvisionnement en gros aux fins de l'acheminement de tous les appels. Elles ne pourraient plus choisir avec quels partenaires elles veulent faire affaire à cette fin.

Mme Tracy Gray: D'accord.

Dans le même contexte, il y a aussi la question des fournisseurs de services téléphoniques IP qui sont informés de ces appels avec falsification du numéro et des sites Web offrant différents services de canular téléphonique.

Savez-vous si les normes STIR/SHAKEN peuvent permettre de détecter les appels déguisés en provenance de ces sites? Pouvez-vous nous dire ce qu'il en est?

M. Matthew Gamble: Lorsque les normes seront entièrement mises en œuvre, chaque appel se verra attribuer un niveau d'attestation. Il y a trois niveaux différents: attestation du point d'accès, attestation partielle et attestation complète. L'attestation du point d'accès indique seulement la provenance de l'appel sur le réseau. On peut savoir ainsi via quel point d'accès l'appel est passé de l'Internet au réseau téléphonique. De cette manière, on peut connaître tout au moins la provenance initiale de l'appel.

Mme Tracy Gray: Il n'y a cependant aucune réglementation ni aucun moyen à notre disposition pour faire quoi que ce soit au sujet de ces sites Web. Il s'agit simplement davantage de savoir d'où proviennent les appels.

M. Matthew Gamble: C'est exact. Il n'y a pas d'obligation de bien connaître son client dans le domaine des télécommunications.

Mme Tracy Gray: D'accord.

Par ailleurs...

La présidente: Il vous reste 10 secondes.

Mme Tracy Gray: Je ne crois pas que cela va être suffisant.

La présidente: Je suis désolée.

C'est maintenant au tour de M. Ehsassi qui a également droit à six minutes.

M. Ali Ehsassi (Willowdale, Lib.): Merci, madame la présidente.

Merci, monsieur Gamble. Merci, monsieur Lawford.

Vous nous avez transmis une foule d'informations qui vont nous être extrêmement utiles.

Monsieur Lawford, vous vous êtes dit préoccupé du fait que les aînés sont particulièrement ciblés et touchés par ce phénomène, ce dont nous sommes tous conscients.

Pouvez-vous me dire s'il est techniquement possible pour les fraudeurs d'effectivement cibler les personnes âgées?

M. John Lawford: Les messages qui sont envoyés visent à susciter la crainte ou l'intérêt. Ceux qui cherchent à semer la crainte peuvent par exemple être efficaces en ciblant les Néo-Canadiens. Pour ce qui est de nos aînés, on essaie plutôt de leur offrir quelque chose qui risque de les intéresser. Il arrive également qu'ils reçoivent des messages visant à leur faire peur.

Les deux groupes peuvent être ciblés par des appels semblables, mais les personnes âgées ont davantage... Il y a deux éléments que l'on se doit de reconnaître à ce sujet. En prenant de l'âge, on a généralement tendance à faire davantage confiance aux gens. Par ailleurs, les aînés vivent une certaine forme d'isolement social. C'est ce que nous disent les gens qui font partie de nos groupes clients. On en vient à être disposé à répondre à n'importe quel appel. Les arnaqueurs ne le savent que trop bien. C'est la raison pour laquelle un grand nombre de ces appels ciblent les personnes âgées. Pour dire les choses comme elles sont, on espère piéger une personne qui se sent seule.

Je n'ai pas vraiment étudié le contenu exact des messages. Je pense toutefois que les menaces fonctionnent mieux auprès des immigrants récents.

● (1130)

M. Ali Ehsassi: Merci.

Monsieur Lawford, je ne sais pas si vous avez eu l'occasion de prendre connaissance du compte rendu des témoignages que nous avons entendus cette semaine. Comme vous le savez, nous avons reçu des représentants du CRTC...

M. John Lawford: Oui.

M. Ali Ehsassi: ... et de la GRC.

Il y avait également des dirigeants de Bell, de Rogers et de Telus.

Ces grandes entreprises ont des approches distinctes et des programmes différents pour le filtrage et le blocage des appels.

M. John Lawford: Oui.

M. Ali Ehsassi: Pouvez-vous nous dire ce que vous pensez des différentes approches adoptées par ces entreprises?

M. John Lawford: Certainement.

À la base, tout le monde s'entend sur le fait qu'il faut bloquer les appels provenant d'un numéro que l'on sait invalide. Cet aspect-là est déjà réglé.

Interviennent ensuite les normes STIR/SHAKEN. Les grandes entreprises n'aiment pas le fait qu'il s'agit d'un protocole pouvant être utilisé directement sur l'application d'un tiers ou sur votre téléphone. Les appels jugés suspects seront ainsi bloqués si c'est ce que vous désirez, car vous pouvez aussi configurer votre appareil différemment.

Les entreprises de téléphonie ne font pas nécessairement beaucoup d'argent avec ce dispositif, mais il fonctionne plutôt bien. Il peut y avoir des problèmes liés à la transparence et à l'équité dans sa mise en oeuvre. Nous n'allons pas nous attarder à cela pour l'instant. Les normes STIR/SHAKEN devraient permettre de régler la question. Il est tout à fait vrai qu'elles ne s'appliqueront pas aux appels n'utilisant pas le protocole IP qui sont acheminés par les réseaux téléphoniques conventionnels, mais ce n'est pas non plus ce qui devrait nous intéresser ici.

Bell et Telus utilisent au niveau de leur réseau des systèmes fondés sur une approche différente. Telus exige de l'appelant qu'il saisisse des chiffres supplémentaires dans le but de ralentir ses efforts. Je pense qu'un bon programmeur peut trouver une solution de contournement. On ne sait pas encore si cela peut fonctionner et si l'on pourra vendre ce dispositif à d'autres fournisseurs ou à d'autres intervenants au sein du système téléphonique. Il est aussi possible qu'on le vende directement aux consommateurs. Je crois que le but visé en définitive, c'est sans doute de le vendre aux consommateurs.

L'approche de Bell est différente. On mise sur le blocage des appels au niveau du réseau, ce qui suscite de nouvelles questions quant à la façon dont les appels sont bloqués, aux raisons pour lesquelles on le fait et à la teneur exacte du système. Ce sont justement ces questions qui font actuellement l'objet de discussions à huis clos au CRTC. Je crois que Bell voudrait également en arriver à vendre cette fonctionnalité aux consommateurs, mais je n'en ai pas la certitude. Comme on l'a déjà indiqué, ils se distinguent de certaines autres entreprises de télécommunications du fait que la plupart des appels sont acheminés via leurs réseaux.

M. Ali Ehsassi: Je vous pose la même question, monsieur Gamble.

Vous avez indiqué que la concurrence allait en souffrir, car les petites entreprises sont défavorisées.

Pouvez-vous nous dire ce que vous pensez des différentes approches exposées par les entreprises?

M. Matthew Gamble: Je crois que ces entreprises font de leur mieux, mais qu'elles doivent composer avec le fait qu'elles ne possèdent pas toutes les données nécessaires. Comme pour le système intégré de télémarketing en place il y a un certain nombre d'années, le numéro de téléphone est en fait le seul élément de données que nous pouvons utiliser. Tant que nous n'aurons pas davantage de renseignements à notre disposition, comme la provenance des appels ou leur source exacte, nos efforts de filtrage se limiteront à faire de notre mieux pour que nos outils technologiques puissent contrer ceux utilisés par les fraudeurs.

M. Ali Ehsassi: Merci.

Monsieur Lawford a indiqué qu'il souhaite voir le CRTC tenir des audiences publiques à ce sujet. Est-ce quelque chose que vous préconisez vous aussi?

M. Matthew Gamble: Pour ce qui est du transfert non autorisé de carte SIM, oui.

M. Ali Ehsassi: Oui, d'accord.

Monsieur Lawford, vous nous avez dit que les Américains ont été plus efficaces à ce chapitre. Vous avez notamment parlé de leur loi sur la protection des consommateurs de services téléphoniques. Pensez-vous que le Canada devrait procéder de la même manière?

M. John Lawford: Oui, j'estime qu'il convient d'accorder des pouvoirs supplémentaires au CRTC afin qu'il puisse s'attaquer plus directement à la fraude. Pour l'instant, la fraude électronique, si je puis m'exprimer ainsi, n'est pas considérée comme une infraction au Canada. Vous vous rendez coupable de fraude à partir du moment où vous parlez à quelqu'un au téléphone dans cette intention. Dans l'état actuel des choses, le CRTC peut s'en prendre à vous uniquement si vous avez recours à des appels automatisés, mais il n'a pas vraiment compétence, comme le soulignait M. Scott, en matière de fraude. Je crois que c'est l'élément qui manque.

M. Ali Ehsassi: D'accord, et...

La présidente: C'est malheureusement tout le temps que vous aviez, monsieur Ehsassi.

[*Français*]

Monsieur Lemire, vous disposez de six minutes.

M. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Merci, madame la présidente.

Je vous remercie de votre présentation. Je tiens à dire que celle-ci survient alors que je viens de croiser une citoyenne âgée de ma circonscription qui m'a confié avoir été victime d'une fraude importante. Je ne pense pas que cela se soit fait par téléphone, mais cette conversation confirme quand même l'importance de nos travaux.

Je vous présente aussi Simon-Pierre Savard-Tremblay, qui est député bloquiste de Saint-Hyacinthe—Bagot et qui s'occupe également des dossiers liés à l'industrie et au commerce international.

Comme première question, je voudrais tout d'abord savoir quelles sont vos attentes en ce qui a trait au CRTC, ainsi qu'à nous, le législateur.

Monsieur Lawford, vous avez notamment parlé d'une loi contre la fraude téléphonique. Quelles mesures concrètes pourrait-on prendre pour vous aider ou pour assurer de bien régulariser la situation?

● (1135)

M. John Lawford: Premièrement, il faudrait encourager le CRTC à ouvrir une enquête sur l'usurpation des cartes SIM. C'est un problème qui est assez léger pour l'instant, mais qui va bientôt s'aggraver.

Deuxièmement, comme je l'ai dit, le CRTC est un peu coincé par la législation, qui ne lui donne pas assez de pouvoirs. Je ne sais pas exactement quoi suggérer au sujet de cet organisme, sinon de lui donner un peu plus d'outils pour étudier les activités frauduleuses. Il y a de petits bémols dans les démarches en cours, mais ils sont trop [*inaudible*] pour vous.

M. Sébastien Lemire: Monsieur Gamble, avez-vous quelque chose à rajouter sur vos attentes relativement au CRTC et à nous comme législateur?

[*Traduction*]

M. Matthew Gamble: Pas pour l'instant, merci.

[*Français*]

M. Sébastien Lemire: Pour ma deuxième question, je m'adresse à vous deux, compte tenu de vos champs d'expertise respectifs. Sentez-vous que le CRTC et la GRC comprennent bien l'importance de la téléphonie IP et des appels automatisés en lien avec la fraude?

[*Traduction*]

M. Matthew Gamble: Je crois qu'ils font de leur mieux, mais qu'ils n'arrivent pas à suivre le rythme des avancées technologiques. Dès qu'ils arrivent à bien comprendre une problématique, une nouvelle fait son apparition.

[*Français*]

M. Sébastien Lemire: Parfait.

Monsieur Gamble, vous avez mentionné tantôt que les petites compagnies étaient désavantagées par rapport aux grosses. J'ai justement demandé aux représentants des trois sociétés de télécommunications qui ont comparu mardi s'ils étaient prêts à fournir de l'aide. Ils nous ont tous répondu qu'ils étaient prêts à poser des gestes.

Sentez-vous que c'est le cas, concrètement? De plus, comment pourrait-on aider davantage les petits acteurs?

[*Traduction*]

M. Matthew Gamble: Je pense que ces entreprises veulent vraiment apporter leur aide, mais que cela leur est très difficile compte tenu de la façon dont les normes en place ont été élaborées. Pour que cela devienne chose possible, il nous faut changer complètement la manière dont nous allons établir les normes STIR/SHAKEN.

[*Français*]

M. Sébastien Lemire: Il y a aussi toute la question du temps dont ont besoin ces compagnies pour respecter les normes, puisque la technologie est difficile à implanter. Croyez-vous qu'elles agissent de bonne foi présentement?

[*Traduction*]

M. Matthew Gamble: Comme je connais la plupart des fournisseurs de services technologiques auxquels ces entreprises font appel, je peux vous confirmer qu'elles font vraiment de leur mieux.

[*Français*]

M. Sébastien Lemire: Monsieur Lawford, sentez-vous que le CRTC a tardé à réagir aux préoccupations des citoyens sur cette question? Croyez-vous que l'organisme aurait pu être plus proactif dès le début?

M. John Lawford: Le CRTC est assez proactif dans le dossier des appels déguisés.

En ce qui a trait à l'usurpation des cartes SIM, par contre, c'est vraiment la pagaille. Le CRTC nous assure qu'il y aura une solution dans ce dossier, mais qu'elle ne sera communiquée qu'aux compagnies, sans faire preuve de transparence. C'est donc un dossier dans lequel je ne fais pas confiance au CRTC, et je demande une enquête publique pour savoir ce qu'il fait.

M. Sébastien Lemire: Ma prochaine question concerne les aînés.

Selon vous deux, est-ce que suffisamment de mesures préventives sont prises, et comment pouvons-nous nous assurer de mieux protéger nos aînés?

M. John Lawford: Mon opinion ne sera peut-être pas agréable à entendre. Selon moi, il est impossible de dépasser un certain niveau d'éducation technologique lorsqu'il est question des aînés, malgré tout ce que nous pouvons leur enseigner ou les exemples que nous pouvons leur donner quand nous les rencontrons. Nous recevons trop d'appels pour qu'il n'y ait pas de victimes. Les échanges par courriel sont plus importants.

● (1140)

M. Sébastien Lemire: C'est ce que je retiens de votre discours: le volume d'appels est trop important, ce qui signifie qu'il y a beaucoup de victimes même si le nombre officiel de cas de fraude est bas.

Monsieur Gamble, avez-vous quelque chose à ajouter relativement aux aînés?

[*Traduction*]

M. Matthew Gamble: Non. Je partage le point de vue de M. Lawford quant aux différents obstacles qu'il vous a exposés.

[*Français*]

M. Sébastien Lemire: Merci beaucoup.

La présidente: Merci beaucoup.

[*Traduction*]

C'est maintenant M. Masse qui va poser ses questions pendant les six prochaines minutes.

M. Brian Masse (Windsor-Ouest, NPD): Merci, madame la présidente.

Convenez-vous avec moi que tout ce que nous avons pu entendre jusqu'à maintenant nous porte à croire que cette forme de fraude touche démesurément les aînés et les personnes à faible revenu?

M. John Lawford: C'est certes la façon dont je vois les choses. Il y a aussi en particulier les nouveaux arrivants au Canada pour lesquels certains appels peuvent susciter davantage de crainte.

M. Brian Masse: J'ai une question que je vous adresse à tous les deux. Les représentants des différentes entreprises nous ont parlé de quelques-unes des mesures qui sont prises, mais il faut également dire que le CRTC leur permet de s'en tirer à bon compte en ne les obligeant pas à offrir le blocage d'appel sans frais. Il m'apparaît pourtant raisonnable que l'on offre à tous les Canadiens ce service de blocage sans qu'ils aient à débourser un traître sou. Il est difficile de savoir avec précision ce que les entreprises incluent ou non dans leurs forfaits.

Nous allons procéder à une étude plus approfondie de ces questions. On peut essentiellement affirmer que les consommateurs doivent maintenant payer davantage pour un meilleur filtrage des appels et une plus grande protection contre la fraude. Êtes-vous, oui ou non, d'accord avec cette affirmation?

M. John Lawford: Je dirais oui et non, et permettez-moi de m'expliquer.

Il n'y a pas de frais pour le blocage des numéros déguisés. C'est ce qu'a décidé le CRTC. Pour ce qui est des normes STIR/SHAKEN, tout dépendra de la façon dont elles seront mises en œuvre. Quant au réseau, je pense vraiment que Bell et les autres entreprises vont vous demander 10 $ par mois.

M. Matthew Gamble: Je voulais juste ajouter que certaines entreprises au Canada imposent des frais alors que d'autres ne le font pas.

M. Brian Masse: Oui. Cela fait partie des éléments au sujet desquels j'aimerais que l'on nous soumette des recommandations. D'ici à ce que les normes STIR/SHAKEN soient mises en oeuvre, il faudrait que les consommateurs aient accès à ces mécanismes sans devoir attendre. Nous sommes vraiment témoins d'une situation où l'on abuse des gens. Si ces entreprises demandent plus de temps pour l'application des normes STIR/SHAKEN, il faut que des mesures soient prises dans l'intervalle pour que les Canadiens ne soient plus aussi nombreux à être victimes de ces actes frauduleux qui représentent par ailleurs un véritable fléau pour notre économie. C'est ce que nous avons pu observer par le passé avec les pourriels, ce qui nous a notamment incités à adopter ces lois.

Serait-il déraisonnable de demander que les consommateurs puissent compter sur une mesure semblable à une cote établie par J.D. Power quant au traitement de la fraude par certaines de ces entreprises? C'est ce qui se fait dans le secteur de l'automobile où je travaillais auparavant. Il faut qu'une entité indépendante évalue la situation de chaque entreprise de telle sorte que le consommateur puisse décider en toute connaissance de cause quels services il souhaite obtenir en fonction de ce que cela lui coûtera.

Je crains que les mieux nantis puissent bénéficier d'une meilleure protection que les Canadiens à faible revenu. Je crois qu'il pourrait être utile de mieux informer les consommateurs en leur permettant de décider pour eux-mêmes.

M. John Lawford: Si l'on en arrive à un système où les consommateurs doivent payer en partie pour cette protection, je pense que l'établissement d'un classement quelconque pourrait être une bonne façon de procéder.

Si des mesures réglementaires sont prises pour s'assurer que le service est offert sans frais, le CRTC devrait tout de même compiler des statistiques pour voir si les entreprises s'y conforment et évaluer l'efficacité de leurs systèmes. Si ceux-ci ne respectent pas les normes, il faudrait trouver des façons de voir à ce que les améliorations nécessaires soient apportées dans chaque cas.

M. Matthew Gamble: Une fois que les normes STIR/SHAKEN seront mises en oeuvre et accessibles, on en arrivera à un système qui se rapprochera de celui que l'on a actuellement avec le filtrage des pourriels. Nous pouvons juger de son efficacité en fonction du nombre d'appels importuns que nous recevons. Ce seront les données à notre disposition.

M. Brian Masse: Cependant, pour ceux qui n'ont pas les moyens de procéder à la mise à jour de leur appareil pour certains de ces systèmes, il sera impossible d'en bénéficier. Il faudra soit acquérir un nouvel appareil à cette fin ou remplacer celui que l'on possède déjà, ce qui entraînera également des retombées économiques pour certains, mais aussi un effet dissuasif pour d'autres. Cela complique aussi les choses pour ceux qui n'ont pas la possibilité de modifier aussi facilement que d'autres leur forfait téléphonique. Ce sera vraiment un enjeu de taille.

Serait-il bon que nous sachions maintenant ce qu'en pense le commissaire à la protection de la vie privée? Il faut malheureusement constater que le CRTC n'a pas fait l'objet d'une réforme en profondeur depuis plus de 20 ans. Il risque fort d'éprouver de grandes difficultés à apporter certains des changements requis si le Parlement ne modifie pas les lois pour lui en donner les moyens.

Devrions-nous chercher à obtenir le point de vue du commissaire à la protection de la vie privée au sujet des normes STIR/SHAKEN et de tous ces enjeux?

M. Matthew Gamble: Je crois que oui. On n'a pas encore trouvé de solutions au titre des graves répercussions découlant du transfert de données à des tiers à des fins d'analyse.

M. John Lawford: J'ajouterais simplement qu'il nous serait très utile de réfléchir à notre politique numérique dans une perspective plus générale. Ce n'est pas ce que nous faisons actuellement. Il serait bon de consulter le commissaire à la protection de la vie privée concernant les normes STIR/SHAKEN, mais également pour déterminer si les autres mécanismes de blocage au niveau du réseau suscitent certaines préoccupations. Il faudrait peut-être aussi intégrer au processus le commissariat responsable du numérique, si une telle entité voit effectivement le jour.

● (1145)

M. Brian Masse: Est-ce que ces considérations devraient être intégrées à nos obligations internationales découlant des accords de libre-échange? Le nouvel ACEUM comprend une charte du numérique, mais est-ce une option que nous devrions envisager également pour nos accords de libre-échange avec d'autres pays?

M. John Lawford: Voulez-vous dire par là que chacun des règlements que nous prendrions devraient comporter une exigence semblable?

M. Brian Masse: Oui, et peut-être aussi pour prévoir une forme quelconque de surveillance ou un accord parallèle touchant les abus et les fraudes au moyen du téléphone et de l'Internet.

M. John Lawford: Nous sommes effectivement d'accord, mais nous croyons qu'il convient surtout d'intégrer cela à une politique globale du numérique qui irait de pair avec notre politique commerciale.

M. Brian Masse: Vous avez indiqué que le Parlement devrait être plus actif dans la lutte contre la fraude. Pouvez-vous nous en dire plus long quant aux mesures que nous devrions prendre dans le contexte actuel et peut-être nous suggérer aussi quelques améliorations à apporter à la réglementation?

M. John Lawford: En disant cela à la fin de mes observations, je voulais faire valoir qu'il y aurait peut-être lieu d'intégrer aux articles du Code criminel qui traitent de la fraude des dispositions ciblant expressément la fraude téléphonique ou l'hameçonnage.

La présidente: Il vous reste 10 secondes.

M. Brian Masse: C'est bon, je vous remercie.

La présidente: Merci beaucoup.

Nous passons maintenant au tour de questions où chacun aura droit à cinq minutes.

La parole est à M. Van Popta.

M. Tako Van Popta (Langley—Aldergrove, PCC): Merci.

Ma question s'adresse à M. Lawford et va un peu dans le sens de celle que M. Masse vient de poser.

Le CRTC est de toute évidence un joueur important dans le contexte de cette lutte contre la fraude par téléphone et par Internet. Vous avez laissé entendre que le moment était peut-être venu d'évaluer l'efficacité du CRTC.

Est-ce qu'il manque quelque chose dans la loi habilitante ou est-ce simplement que l'organisation est inefficace?

M. John Lawford: Je n'irais pas jusqu'à dire que l'organisation est inefficace. Elle a pour l'instant un mandat qui se limite à empêcher les activités illégales de télémarketing et à gérer la liste des numéros de téléphone exclus. C'est cela et rien d'autre. Comme M. Scott l'a indiqué très clairement, le CRTC n'est pas là pour arrêter la fraude.

M. Tako Van Popta: Serait-il bon que le mandat du CRTC soit élargi? Que peuvent faire les parlementaires pour améliorer les choses?

M. John Lawford: Oui, cela aiderait.

M. Tako Van Popta: Que pourrions-nous faire plus précisément?

M. John Lawford: Il s'agit de voir comment on peut concevoir une loi qui va définir précisément ce qu'on entend par fraude téléphonique, ou fraude électronique, comme on l'appelle aux États-Unis, en tant qu'infraction distincte. On peut penser à différentes façons d'y parvenir.

À titre d'exemple, il est actuellement difficile d'intenter des poursuites à l'égard d'une fraude du fait qu'il est impossible de remonter la chaîne pour rendre criminellement responsables tous ceux qui ont eu un rôle à jouer dans l'appel, qu'il s'agisse de la personne qui a parlé à la victime, ou des gens qui possèdent et exploitent le système, qu'ils soient au Canada ou à l'étranger. Il nous faudrait peut-être une loi qui ferait porter une part de la responsabilité criminelle à tous ceux qui ont contribué au cheminement de l'appel frauduleux de telle sorte que cette activité devienne moins attrayante vu l'absence de conséquences, comme l'indiquait M. Gamble.

M. Tako Van Popta: Bien.

L'un des témoins que nous avons entendus cette semaine nous a dit que même si l'on avait dépisté des centaines de milliers de coupables de fraude téléphonique, on ne pouvait rien faire, sans avoir obtenu l'approbation du CRTC, pour les empêcher de joindre leurs éventuelles victimes.

Êtes-vous d'accord avec cette affirmation?

M. Matthew Gamble: L'interprétation actuelle de la Loi sur les télécommunications va dans ce sens-là.

M. John Lawford: Voici ce qui est un peu étrange dans toute cette histoire. Les appels automatisés sont illégaux. Personne n'est autorisé à utiliser des appels automatisés à des fins commerciales, point à la ligne. Il y a seulement des exceptions pour les hôpitaux, les écoles et les établissements semblables. Ces appels sont illégaux, mais à partir du moment où une personne répond en appuyant sur le « 2 » ou sur le « 1 » et parle à quelqu'un, il n'y a pas fraude tant et aussi longtemps qu'une somme d'argent n'est pas transférée. Pendant que l'escroc essaie de vous arnaquer, aucun crime n'est encore commis.

C'est l'astuce. Comment faire en sorte qu'il soit facile d'intervenir à ce niveau pour empêcher cette pratique? Les entreprises ne peuvent pas écouter les appels, car cela exige un mandat. C'est le problème avec lequel nous devons composer.

M. Tako Van Popta: Existe-t-il une solution facile?

M. John Lawford: Il n'y a pas de solution facile, mais je me dis qu'il pourrait y avoir une loi bien rédigée qui permettrait, lorsque des victimes perdent effectivement de l'argent, de remonter jusqu'à la provenance de l'appel. S'il est possible de prouver que tous ces appels ont été envoyés à l'étape initiale de l'hameçonnage et qu'il y a eu suffisamment de gens qui ont mordu à l'appât, il devrait y avoir un moyen nous permettant de poursuivre tous les responsables.

● (1150)

M. Tako Van Popta: Dans cette lutte contre la fraude téléphonique, nous avons parlé du CRTC et de son pouvoir réglementaire, mais dans quelle mesure la technologie peut-elle être un outil efficace? Je pense surtout aux normes STIR/SHAKEN. L'un des témoins que nous avons reçus cette semaine nous disait que l'on est prêt à les mettre en oeuvre, mais que les appareils personnels ne disposent pas encore de la technologie nécessaire.

M. Matthew Gamble: Il y a deux aspects à considérer dans le cas des normes STIR/SHAKEN. Il y a l'aspect réseau, celui qui nous intéresse le plus. Il s'agit de la possibilité de bloquer les appels au niveau du réseau, avant même que le téléphone du consommateur ne sonne. Il y a ensuite l'autre aspect auquel ce témoin faisait référence, à savoir la présentation finale, c'est-à-dire ce crochet ou cette notification sur l'écran du téléphone de l'utilisateur pour lui indiquer qu'un appel a été bloqué.

Nous pouvons en faire beaucoup pour prévenir les cas les plus flagrants au niveau du réseau. Il faudra ensuite de nouveaux appareils et des dispositions de la sorte pour s'attaquer aux problématiques plus pointues.

M. Tako Van Popta: Combien de temps cela devrait-il prendre?

M. Matthew Gamble: On l'ignore pour l'instant, car on travaille encore à l'élaboration des normes pour ce niveau d'affichage. Il y a aussi le problème de tous les Canadiens qui n'ont même pas de téléphone numérique, comme c'est le cas notamment de certains aînés, et qui ont toujours un appareil analogique qui ne peut même pas afficher les données améliorées.

M. Tako Van Popta: Le temps requis va varier en grande partie en fonction de la mesure dans laquelle les consommateurs sont aptes ou disposés à adopter les nouvelles technologies.

M. Matthew Gamble: Exactement, de telle sorte que ce qui se fait au niveau du réseau puisse procurer des avantages dès le départ.

M. Tako Van Popta: J'ai une question pour M. Gamble.

La présidente: Il vous reste 10 secondes.

M. Tako Van Popta: Je vais en rester là pour l'instant. Merci.

La présidente: Merci beaucoup.

Les cinq prochaines minutes appartiennent au député Jowhari.

M. Majid Jowhari (Richmond Hill, Lib.): Merci, madame la présidente.

Je partagerai mon temps avec mon collègue Casey. Je disposerai donc de deux petites minutes et demie pour la question et la réponse.

Monsieur Gamble, vous avez parlé des normes STIR/SHAKEN. Vous avez parlé de la politique, de la technologie et de la protection des renseignements personnels des consommateurs, précisément en ce qui concerne l'impartition à des sources de données pour l'analytique. Vous avez aussi parlé des désavantages subis par le petit fournisseur. Mais j'en ai retenu que, faute d'essayer de prévoir ces conséquences dès la conception comme on l'aurait dû, on a peut-être causé ce déséquilibre.

Pourriez-vous nous éclairer sur ce que devraient être ces modifications de conception pour ramener l'équité?

M. Matthew Gamble: Je n'essaierai pas de vraiment approfondir les décisions des concepteurs de technologie qui le justifieraient, mais la difficulté réelle est qu'il n'existe pas de moyen facile pour faire passer un numéro de téléphone d'un propriétaire à un autre et de déléguer cette responsabilité. On y travaille maintenant, mais, dans les certificats numériques, c'est très difficile.

Ça revient vraiment à notre traitement des compagnies de téléphone de revente. Dans les réseaux téléphoniques canadiens, ils ont toujours été à un niveau inférieur à celui des entreprises mères, mais il n'y a jamais eu de raison pour que ça cause des difficultés. Si nous laissons plus de fournisseurs s'élever au niveau des propriétaires des installations, avec interconnexions SIP et ce genre de choses, nous pourrons résoudre certains de ces problèmes.

Ça revient vraiment à la conception de tout le système de revente, qui ne peut pas être facilement réparé.

M. Majid Jowhari: Me reste-t-il du temps?

La présidente: Trois minutes et demie.

M. Majid Jowhari: Eh bien non. Moins les deux et demie cédées, il m'en reste environ une.

Pouvons-nous parler de la protection de la vie privée des consommateurs et de l'impartition des données pour l'analytique? Est-ce que, encore une fois, ce sera au désavantage des petits joueurs?

M. Matthew Gamble: Difficile à dire. Les joueurs ne disent pas tous à qui ils impartissent le traitement de leurs données, et certains peuvent ne pas le faire. Rien n'exige l'impartition à une entreprise tierce d'analyse. Si vous tenez à offrir le meilleur filtrage des pourriels, vous devrez obtenir les meilleures analytiques possible, ce qui peut vous obliger à communiquer les données à des tiers.

Ce sont généralement des Américains et, même s'ils promettent de ne pas communiquer les données à d'autres tiers, vous devez vous inquiéter d'abord de leur envoi à l'étranger, puis du risque qu'elles soient violées ou compromises.

M. Majid Jowhari: D'accord. Merci.

M. Sean Casey (Charlottetown, Lib.): Revenons au même point, c'est-à-dire une faiblesse dans le système STIR/SHAKEN, qui désavantage injustement les petits joueurs. Vous avez dit que ce n'était pas facile à résoudre. Est-ce un exemple du mieux ennemi du bien?

Est-ce un vice fatal et rédhibitoire, contre lequel ne semblerait efficace que la solution de Bell utilisant le blocage de réseau?

M. Matthew Gamble: Le vice n'est pas fatal. Deux ou trois propositions de solutions existent, plus ou moins inspirées du groupe de travail SITA. Elles n'ont pas encore fait l'objet d'un consensus.

Le consensus des groupes devrait se faire d'ici six à huit mois, peut-être, mais quand le CRTC fixera le délai au 30 septembre prochain et que les solutions à des problèmes si fondamentaux seront encore éloignées de six à huit mois, ça causera des tiraillements.

● (1155)

M. Sean Casey: Ça se rattache également à ce que vous disiez sur la nécessité de toujours avoir quelques coups d'avance sur les fraudeurs. Pour ce système, je suppose que ça s'est bien passé à l'étranger. Les fraudeurs sont-ils en train de nous rattraper, et la technologie doit-elle sauter à la génération suivante?

M. Matthew Gamble: Je ne crois pas. Je pense qu'après STIR/SHAKEN, il faudra des modifications réglementaires.

Actuellement, les fournisseurs ne sont pas responsables des appels sur les réseaux. Dès que STIR/SHAKEN permettra de déterminer le fournisseur à l'origine d'un appel, vous pourriez peut-être donner au CRTC le pouvoir de... Si un fournisseur se révélait la source d'une importante majorité d'appels frauduleux, on pourrait, d'une façon ou d'une autre, l'en trouver responsable.

M. Sean Casey: Monsieur Lawford, vos observations sur une autre technologie prometteuse ont piqué mon intérêt: elle est accessible par Bell. Vous vous demandiez si elle nous serait vendue ou offerte gratuitement.

Quel serait le risque, pour la société, d'une technologie gratuite? Quelle sorte de réaction pouvons-nous prévoir de Bell? En serions-nous privés si on obligeait la compagnie à l'offrir gratuitement?

M. John Lawford: Non, pas nécessairement, parce que Bell veut aussi mettre fin aux appels frauduleux, parce que, notamment, les abonnés délaissent les lignes terrestres, une hémorragie à laquelle elle veut mettre fin.

Elle pourrait donc le faire de toute façon. Elle pourra souhaiter la vendre dans certaines situations où ce serait indiqué, comme hors du marché de la consommation. Ma seule crainte est que certains disposent de la technologie et d'autres pas.

La présidente: Malheureusement, notre temps est écoulé.

Je vous remercie tous les deux de vous être déplacés.

Nous devons mettre fin à cette partie de la séance quelques minutes plus tôt, parce que notre prochain groupe a besoin de certains ajustements techniques. Il nous faudra une dizaine de minutes pour être prêt pour lui.

Merci encore une fois d'être venus. Bonne journée.

● (1155)

(Pause)

● (1206)

La présidente: Mesdames et messieurs, soyez les bienvenus au Comité permanent de l'industrie, des sciences et de la technologie. Nous étudions les appels frauduleux.

Nous accueillons M. Randall Baran-Chong, cofondateur de Canadian SIM-swap Victims United.

Par vidéoconférence, nous sommes en contact avec Mme Kate Schroeder, membre du conseil d'administration du Réseau canadien pour la prévention du mauvais traitement des aînés.

Soyez tous les deux les bienvenus. Chacun de vous disposera de 10 minutes pour son exposé, après quoi des députés, à tour de rôle, vous questionneront.

Quand j'agiterai le carton jaune, vous saurez qu'il vous reste 30 secondes. Ça ne signifie pas de ne pas me regarder pour ne pas le voir. Ça signifie qu'il vous reste 30 secondes pour conclure.

Pour nous assurer de ne pas perdre le contact avec Mme Schroeder, nous commençons par elle.

Madame Schroeder, vous disposez de 10 minutes.

Mme Kate Schroeder (membre du conseil d'administration, Réseau canadien pour la prévention du mauvais traitement des aînés): Bonjour, madame la présidente. Je vous remercie, vous et le Comité, de votre invitation à venir discuter de ce sujet important.

La présidente: Madame Schroeder, je suis désolée. Attendez un moment. Des difficultés techniques nous empêchent de vous entendre.

Très bien, veuillez poursuivre.

Mme Kate Schroeder: Parfait.

Je me nomme Kate Schroeder. Je fais partie du conseil d'administration du Réseau canadien pour la prévention du mauvais traitement des aînés, le RCPMTA, que j'appellerai le Réseau.

Le Réseau, qui s'étend à la grandeur du Canada, bénéficie de l'appui des chefs de file des domaines du vieillissement, de la recherche, des soins de santé et de la prévention du mauvais traitement des personnes âgées, qui comprend également l'intervention, entre autres choses. Le Réseau sert de trait d'union entre les personnes et les organisations, il favorise l'échange de renseignements sûrs et promeut la mise au point de programmes et de politiques sur les questions touchant la prévention du mauvais traitement des personnes âgées. Son action s'exerce localement, dans les régions, dans les provinces et les territoires ainsi qu'à l'échelle nationale grâce à notre centre de partage de connaissances à cnpea.ca.

Nous sommes heureux de saisir cette occasion pour faire connaître les difficultés et les répercussions qu'entraînent les appels frauduleux chez les Canadiens âgés. Notre travail se focalise sur le rassemblement et la diffusion de ressources adaptables, de pratiques exemplaires et des acquis de la recherche en cours et de l'élaboration de politiques par des experts canadiens pour que, collectivement, nous puissions prévenir et combattre le mauvais traitement des personnes âgées. Les observations et les recommandations qui suivront se fondent sur l'immense travail de certains de ces experts.

L'appel frauduleux vise à tromper la victime dans le dessein de contrôler un aspect — financier ou autre — de sa vie ou de son identité. Ce crime a des répercussions chez tous les Canadiens, quels qu'en soient l'âge, la race, les études ou les antécédents. Une santé défaillante, la naïveté financière, un réseau social ténu, entre autres facteurs, peuvent augmenter le risque d'être la victime d'escroqueries, risque qui ne fait qu'augmenter avec l'âge.

Le vieillissement rapide de la population canadienne a des répercussions sur tous les aspects de notre pays et de son économie. D'ici 2031, 23 % des Canadiens auront plus de 65 ans. D'ici 2061, le Canada pourrait compter 33 % de plus de personnes âgées que d'enfants. Cette évolution nous offre déjà sur les fraudes de nouvelles statistiques inquiétantes que nous ne voyons pas se résorber à mesure que la population vieillit, puisque les personnes âgées sont souvent des cibles toutes désignées.

Les statistiques publiées par le Centre antifraude du Canada révèlent que, le 29 février 2020, depuis la dernière année, 7 804 signalements de fraude ou de tentatives de fraude avaient fait 4 119 victimes confirmées au Canada et causé des pertes se chiffrant à plus de 9,2 millions de dollars.

D'après le Centre, les arnaques téléphoniques ont fraudé les Canadiens, entre le 1er janvier et le 31 octobre 2019, d'un montant estimé de 24 millions de dollars. Les statistiques publiées révèlent que les pertes subies par les personnes âgées constituent jusqu'à 25 % des pertes totales attribuées aux fraudes signalées et que ce taux augmente considérablement.

Ce qu'il y a de dérangeant dans ces statistiques, c'est qu'elles ne correspondent qu'aux fraudes signalées. D'après les études accessibles, nous savons que le taux de signalement des fraudes peut être d'à peine 13 %, souvent parce que les victimes âgées ont peur ou honte et craignent d'être jugées incompétentes ou de ne s'être pas montrées à la hauteur en se laissant berner par ces appels.

Les appels frauduleux sont endémiques partout au Canada. Il s'agit notamment de mystifications fondées sur la ressemblance des numéros de téléphone, d'appels faisant croire en l'existence d'un mandat d'arrestation visant la victime, d'offres de croisières ou de voyages gratuits, d'appels annonçant une catastrophe naturelle, d'arnaques simulant des appels de l'Agence du revenu du Canada, d'arnaques où le fraudeur se fait passer pour le petit-fils de la victime et d'arnaques technologiques.

Les trois dernières arnaques sont plus susceptibles de toucher les personnes âgées. Un facteur important de risque est l'isolement social, considéré comme facteur de risque accru du mauvais traitement des personnes âgées en général. Les adultes isolés qui ont besoin de rapports humains, à qui leur famille manque ou sans réseau de soutien sur lequel compter sont plus susceptibles d'être des victimes faciles.

Les causes de la vulnérabilité plus grande des personnes âgées sont souvent complexes et reliées. Les facteurs de risque sont notamment la perte récente d'un être cher, l'absence de réseau de soutien, l'isolement social, l'insécurité économique, la pauvreté, un déficit cognitif, la non-perception ou la non-compréhension de la nature des appels, l'emploi de technologies sophistiquées, en évolution constante.

Les victimes se sentent ensuite souvent stigmatisées. La complexité du signalement et des enquêtes sur ces types de fraude diminue la probabilité, pour les victimes, d'aller jusqu'au bout du processus de signalement.

● (1210)

Parmi certains des obstacles qui, d'après nos observations, nuisent au processus de signalement, on trouve la crainte de paraître incompétent; la crainte de la remise en question de son autonomie ou de sa capacité de décider; la crainte de devoir confesser une erreur à ses enfants ou aux êtres chers, vu que, dans les familles, entre les parents et les enfants, les questions d'argent et de technologie peuvent souvent engendrer des tensions; l'ignorance des services compétents à qui s'adresser; la possibilité de susciter des réactions d'âgisme quand on essaie d'expliquer sa situation.

Chose sûre, ces types d'appels frauduleux vont en augmentant et touchent tous les Canadiens. Les solutions doivent être propres à chaque cas et suivre une démarche intergénérationnelle tout en étant concertées entre les secteurs privé et public, les groupes de consommateurs, les organismes financiers et les services d'application de la loi. Parmi les principaux éléments favorables à la prévention et à l'intervention, signalons la sensibilisation, l'éducation et l'accès facile au processus de signalement ainsi qu'une démarche respectueuse et informée pour la communication avec les victimes âgées et l'appui à leur accorder.

Parmi ces recommandations générales, le Réseau préconise notamment les actions suivantes: mettre sur pied des campagnes de sensibilisation sous toutes les formes — dans les médias sociaux, sur le Web, sur supports imprimés, à la télévision — pour aider tout le monde, sans égard à l'âge, à comprendre les différentes formes d'arnaque ou de fraude en vogue; appuyer et promouvoir des programmes de formation en intervention s'adressant aux tiers, auprès des établissements financiers, des études juridiques et d'autres groupes de consommateurs; appuyer la mise sur pied de programmes non seulement pour aider les Canadiens à s'y retrouver dans les méandres du signalement des fraudes, mais pour améliorer de façon marquée l'accès au soutien après avoir signalé une fraude pour prévenir la « revictimisation »; encourager la mise sur pied de programmes de sensibilisation et de soutien accessibles à partir de chez-soi ou d'autres milieux de vie; améliorer l'accès à des moyens réguliers et abordables de transport dans les régions rurales, pour prévenir l'isolement social et faciliter l'accès aux ressources nécessaires; promouvoir des communications sans cesse proactives de la part de divers joueurs — l'Agence du revenu du Canada, les banques, les entreprises de télécommunication, les fournisseurs de services aux personnes âgées — pour informer les personnes âgées des arnaques à la mode qui les menacent.

Merci.

● (1215)

La présidente: Merci infiniment.

La parole est à M. Baran-Chong.

Vous disposez de 10 minutes.

M. Randall Baran-Chong (co-fondateur, Canadian SIM-swap Victims United, à titre personnel): Bonjour. Je me nomme Randall Baran-Chong. Je suis un entrepreneur de Toronto, ce qui explique pourquoi j'ai tenu à m'exprimer au moyen d'une présentation PowerPoint.

Je suis venu représenter Canadian SIM-swap Victims United, une organisation de défense des victimes regroupant des citoyens ordinaires, de partout au Canada et de tous les horizons, constituée à la suite d'une fraude téléphonique décrite comme l'une de celles que les experts redoutent le plus. À titre de défenseurs des victimes, nous transformons notre pénible expérience en espoir d'une sensibilisation meilleure, avec, pour seul objectif, en le combinant aux avis des experts et à la mobilisation de l'industrie et d'influenceurs comme vous pour encourager l'action, celui de ne pas ajouter d'autres noms à notre liste de victimes.

Même si mon histoire commence à la fin d'octobre 2019, son vrai début se situe en 2007, alors qu'un ancien collègue à vous, Maxime Bernier, alors ministre de l'Industrie, annonçait la transférabilité des numéros sans fil. Essentiellement, il s'agissait de donner aux consommateurs le pouvoir de voter avec leurs dollars, c'est-à-dire de changer de fournisseur sans s'embarrasser de la perte de leurs numéros de téléphone.

Bref, il s'agissait de leur donner du pouvoir et la possibilité de choisir leur fournisseur. Mais, malgré ces bonnes intentions, cette autorisation, comme la route de l'enfer pavée de bonnes intentions, a conduit à l'enfer que beaucoup d'entre nous, les victimes, appelons l'arnaque du transfert de SIM, dit aussi portage non autorisé. C'est essentiellement le transfert non autorisé du numéro de téléphone de la victime, de sa propre carte SIM, ou carte d'identification d'abonné, à une autre carte SIM.

Disséquons schématiquement ce transfert. L'immense majorité des transferts de SIM sont motivés par le lucre. Leurs auteurs commencent par faire leurs recherches, c'est-à-dire bien connaître les victimes, à un niveau personnel, et essayer de trouver certains de leurs identifiants, mais, en réalité, pour le faire par un portage non autorisé, ils veulent obtenir les renseignements clés nécessaires à l'opération. Il s'agit d'abord du numéro même de téléphone, puis de l'un des renseignements suivants, décrit par le Wireless Network Portability Council, qui a défini ces règles: le numéro de compte de l'abonné, l'identifiant ou un numéro d'identification personnel. Quand on y pense, il suffit du numéro de téléphone et de l'un de ces identifiants, et le numéro de téléphone est d'un accès très facile pour la plupart d'entre nous. La moitié du travail est donc déjà faite.

Comment obtenir les renseignements qui manquent? C'est là qu'interviennent les méthodes de ces fraudeurs.

L'une de leurs principales méthodes est la manipulation, ce qui signifie prendre avantage de la faillibilité humaine des représentants de service après-vente. Souvent, les fraudeurs leur feront croire qu'ils ont perdu leur téléphone et qu'ils ont grand besoin d'en obtenir un autre. Ils profiteront du système. Ils pourront même prétendre qu'ils ont oublié leur numéro d'identification personnel et ils fourniront d'autres renseignements qui sont même plus faciles à connaître, comme le code postal ou le nom de jeune fille de la mère, et ainsi de suite, pour contourner les règles du système et accéder aux renseignements utiles au portage.

Ils utiliseront l'hameçonnage, de faux numéros de téléphone ou des courriels faux prétendant émaner de Rogers et demandant à la victime de saisir son numéro de compte, mais c'est en réalité le fraudeur qui obtient l'information. Il peut aussi employer les médias sociaux pour trouver des renseignements personnels sur la victime et, comme dernièrement, recourir à des fuites de données. Telus et sa marque défensive Koodo ont annoncé que leurs clients, de 2017 et avant, ayant vu les renseignements sur leurs comptes compromis par un utilisateur non autorisé, devaient tous faire protéger leurs comptes contre le portage.

Enfin, et c'est ce qui est des plus odieux, ils ont des complices à l'intérieur des entreprises. Nous l'avons vu aux États-Unis, où des employés d'entreprises comme AT&T et T-Mobile ont vendu des renseignements sur les comptes à ces fraudeurs pour 20 $ ou moins.

Voilà comment ils effectuent le portage.

Dès qu'ils possèdent les renseignements nécessaires, ils se procurent souvent un compte de téléphone prépayé. Aucune identification n'est nécessaire pour l'obtenir grâce à la Loi sur la protection des renseignements personnels et les documents électroniques; il est essentiellement impossible de retracer ces individus ou de remonter jusqu'à eux. En possession des renseignements, ils font l'appel et exécutent le portage avec le fournisseur, puis, en vertu de la décision de 2005 du CRTC, le portage doit se faire en l'espace de deux heures et demie ou moins.

Mardi, j'ai vu que l'un de vous a reçu un message, prétendument de l'Agence du revenu du Canada, et j'espère que vous ne lirez jamais sur votre téléphone le message vous annonçant que votre carte SIM est hors service. C'est de cette manière que la victime s'aperçoit de son portage non autorisé. En réalité, elle n'a rien fait. Quand ça m'est arrivé, il était 23 h 40, et je me suis soudainement aperçu que mon téléphone ne fonctionnait plus. J'ai d'abord songé à un ennui technique, mais, en fin de compte, j'étais la victime d'un portage non autorisé.

● (1220)

Dès ce moment, tous les appels, sortants ou entrants — textes, tout ce qui y ressemble — tombent entre les mains du fraudeur. C'est l'étape de l'« abandon et de la réinitialisation », pour laquelle, j'en suis sûr, beaucoup d'entre vous possèdent l'authentification à facteur textuel pour leurs comptes de médias sociaux, leurs comptes bancaires, ce genre de comptes. Si vous oubliez votre mot de passe, vous cliquez sur « mot de passe oublié » et vous recevrez un message texte pour l'utilisation unique d'un mot de passe pour le réinitialiser ensuite. Ensuite, essentiellement, il peut redéfinir le mot de passe.

Maintenant que le fraudeur possède votre numéro de téléphone, il reçoit ces messages texte ou ces appels, en vous tenant à l'écart de votre propre compte. Il passe ensuite au pillage. Souvent, il pille en équipe. Ça se matérialise par l'arrivée massive de courriels dans votre boîte de réception vous prévenant de la modification du mot de passe de votre compte et de l'ajout d'un nouveau contact à votre compte, et vous ne pouvez que regarder, impuissant.

Dans mon cas particulier, c'est arrivé en fin de soirée, comme je l'ai dit. J'ai appelé mon fournisseur qui m'a d'abord remercié pour m'informer que ses heures de service allaient de 8 heures à 20 heures, du lundi au vendredi. Son mur de défense n'est efficace que 12 heures contre un ennemi en campagne 24 heures. Pour obtenir de nouveau le numéro de téléphone, il faut souvent plusieurs heures ou, comme je l'ai parfois vu, quelques jours.

Comment font-ils leurs dégâts? Ils emploient trois grandes méthodes de déprédation. La première est le vol direct, à la saveur cryptologique, qui les rend très difficiles à retrouver ensuite, mais il y a des victimes ordinaires comme la famille Johnson de Peebles, en Saskatchewan, qui a perdu des centaines de milliers de dollars du compte de son exploitation agricole. D'autres profitent des applications auxquelles sont liées des cartes de crédit, comme dans le cas de l'infirmière Sheila O'Reilly d'Oakville.

Contre moi, ils ont essayé l'extorsion et le chantage. Ils ont obtenu l'accès à mon disque nuagique. Essentiellement, cinq années de ma vie de petit entrepreneur, avec compte de petite entreprise et compte personnel, tout ça est désormais entre les mains d'un tiers. J'ai raconté cette mésaventure à un Américain qui avait perdu 1 million de dollars — 90 % de ses économies — qui m'a répondu que le tort que j'avais subi était bien pire que le sien. Il partageait ma peine.

Souvent, ils vendent les données sur le Web invisible pour la somme ridicule de 20 à 120 $, s'il s'agit de justificatifs d'accès, et jusqu'à 3 000 $ pour les données complètes d'identification. Parfois, aussi, ils prennent le contrôle du compte. Par exemple, Jack Dorsey, le fondateur de Twitter... Si un tel personnage peut être victime de ce genre de crime, qui, parmi nous, est en sécurité? Même des célébrités comme Mariah Carey et Adam Sandler ont été des victimes de ce genre de crime. Dans d'autres cas, les fraudeurs ciblent des comptes qui ont des noms d'utilisateur appétissants. Un Torontois, Jack Hathaway, a perdu son pseudonyme Instagram, « cosplay », qui est une cible particulièrement recherchée.

À la différence des arnaques comme la mystification par des numéros de téléphone qui semblent légitimes ou d'autres manoeuvres frauduleuses dont vous avez entendu parler un peu plus tôt, ces dernières fraudes ne sont pas nécessairement le fait de centres d'appels à l'étranger contre lesquels nous nous sentons impuissants. Pas plus tard qu'en novembre, on a arrêté un jeune Montréalais de 18 ans qui avait participé au vol de 300 000 $ appartenant à des Canadiens et de plus de 50 millions appartenant à des Américains.

Ça prouve que ces crimes ne sont pas commis par des programmeurs, des bidouilleurs ou des codeurs de haut niveau. Ici, ce sont des individus au parfum, en général des personnes de moins de 25 ans, d'après les arrestations faites aux États-Unis, par exemple.

Nous nous sommes finalement aperçus que nos numéros de téléphone sont notre nouvelle forme d'identité. Notre carte SIM est comme notre nouvelle carte d'assurance sociale, et la sécurité qui l'entoure est aussi efficace que le maillon le moins efficace de la chaîne, que ce soit pour des causes techniques ou humaines. Enfin, le portage non autorisé peut avoir des conséquences sur le reste de nos existences. Nous devons donc le voir d'un autre oeil.

● (1225)

Que fait-on dans d'autres pays? Aux États-Unis, on considère cela comme un risque pour la sécurité nationale. En Afrique, on compte sur la collaboration entre les banques et les entreprises de télécommunications pour repérer le risque de fraude. En Australie, on a mis en place une mesure réglementaire visant à instaurer un processus préalable au portage qui permet de déterminer si les demandes ont été autorisées ou non. On a même prévu des mesures pour les entreprises de télécommunications qui ne respectent pas le processus destiné à vérifier si le portage est autorisé.

La présidente: Monsieur Baran-Chong, malheureusement, vos 10 minutes pour votre exposé sont écoulées.

M. Randall Baran-Chong: D'accord.

La présidente: Je tiens à vous remercier, toutefois, de nous avoir fait part de votre histoire. Nous avons en main vos documents, et j'espère que, durant la période des questions, vous aurez l'occasion de nous donner davantage d'information.

M. Randall Baran-Chong: Merci.

La présidente: Nous allons maintenant commencer par un tour de six minutes.

La parole est d'abord à M. Patzer.

Vous disposez de six minutes.

M. Jeremy Patzer (Cypress Hills—Grasslands, PCC): Je vous remercie beaucoup.

Ma première question s'adresse à vous, monsieur Baran-Chong.

Durant l'expérience que vous avez vécue, vous avez toujours réfléchi aux différentes mesures qui auraient pu être prises pour empêcher des fraudeurs de détourner votre numéro et à la façon dont Rogers aurait pu vous protéger. Je pense que vous étiez sur le point d'aborder cela avant de devoir mettre fin à votre exposé.

Que pourraient faire les fournisseurs pour empêcher les transferts non autorisés de numéros? Vous pourriez peut-être parler de ce que vous vous apprêtiez à dire.

M. Randall Baran-Chong: Je m'en excuse.

D'un point de vue canadien, nous pensons que, tout d'abord, des modifications à la réglementation s'imposent et qu'une mesure similaire à celle mise en place en Australie relativement à l'autorisation préalable au portage doit être adoptée. C'est aussi simple que d'obtenir un message texte de la part du nouveau fournisseur qui dit: « Avez-vous demandé ce portage? » En Australie, on reçoit essentiellement un appel ou un message texte de la part du nouveau fournisseur. Supposons que votre téléphone a bel et bien été volé. Vous devez alors vous rendre dans un magasin pour prouver votre identité à l'aide d'une pièce d'identité délivrée par le gouvernement et demander un portage. Comme John Lawford, du Centre pour la défense de l'intérêt public, l'a souligné, il faut davantage de transparence également concernant le processus.

L'Association canadienne des télécommunications sans fil, l'ACTS, a demandé à ce qu'un grand nombre de renseignements au sujet du processus ne soient pas communiqués, mais, dans le monde de la cybersécurité, on sait bien qu'on ne peut pas assurer la sécurité sans clarté. À titre d'exemple, l'une des mesures adoptées par Rogers consistait à envoyer un message texte qui disait: « Nous avons reçu une demande de votre part pour le portage de votre numéro de téléphone. Si vous n'avez pas fait cette demande, appelez-nous. » Cette mesure ne fonctionne pas pour trois raisons.

Premièrement, parfois, des gens vont penser qu'il s'agit-là d'un faux message texte, car toutes ces fraudes ont miné leur confiance, alors ils ne tiennent pas compte de ces messages. Par conséquent, le portage s'effectue en l'espace de deux heures et demie. Deuxièmement, certaines personnes ont essayé de joindre l'entreprise par l'entremise de son service d'assistance téléphonique, mais ils n'ont jamais été en mesure de parler à quelqu'un. Un portage a même été effectué 12 minutes après la réception du message texte. Troisièmement, un fraudeur très intelligent va consulter les médias sociaux et savoir quand vous serez en vacances, et il procédera au portage lorsque vous n'avez pas votre téléphone avec vous.

Il existe des moyens évidents que nous pouvons mettre en place afin d'éliminer ce problème, du moins temporairement. Ensuite, nous devons cesser complètement d'avoir recours à l'authentification à deux facteurs par message texte.

M. Jeremy Patzer: D'accord. Quelles seraient d'autres méthodes d'authentification à deux facteurs que... ou souhaiteriez-vous qu'on procède complètement autrement qu'en Australie?

M. Randall Baran-Chong: Il y a ce qu'on appelle des jetons logiciels. Il y a notamment Google Authenticator ou Authy, qu'on peut obtenir sur différents types d'applications que nous utilisons. De nombreux médias sociaux les offrent. Souvent, ils constituent un moyen d'authentification secondaire. Ils ne sont pas très connus. Ils sont malheureusement accessibles uniquement pour les utilisateurs de téléphones intelligents. Un grand nombre des applications que nous utilisons encouragent encore l'authentification à deux facteurs par message texte. Les banques entre autres favorisent encore uniquement ce type d'authentification.

● (1230)

M. Jeremy Patzer: Merci.

Ma prochaine question s'adresse à Mme Schroeder.

Lors de la dernière réunion, j'ai parlé du problème grandissant des fraudeurs qui ciblent de plus en plus les gens par l'entremise des médias sociaux ou de messages textes. Nous savons que les jeunes Canadiens sont présents sur ces plateformes, mais pouvez-vous me dire dans quelle mesure les aînés peuvent être particulièrement touchés par ce problème?

Mme Kate Schroeder: Ce n'est pas une idée fausse; il est tout à fait vrai que la jeune génération est extrêmement présente sur les réseaux sociaux, mais il en va de même pour les aînés au Canada. Facebook est un média social très populaire auprès des Canadiens vieillissants. Il est aussi, malheureusement, un terreau fertile pour les fraudes, les escroqueries romantiques et ce genre de choses. Tout part de ce besoin d'être connecté, d'entretenir des relations. C'est l'isolement social qui pousse les aînés à établir des liens grâce à ce réseau social.

M. Jeremy Patzer: Oui, tout à fait.

Sur le plan de l'éducation et de la sensibilisation, quelles autres mesures doivent être prises? Est-ce que des groupes comme le vôtre prennent déjà des mesures pour éduquer et sensibiliser les aînés? Est-ce que des programmes ont été mis en place pour leur permettre de bien comprendre le problème et les aider à en prendre conscience?

Mme Kate Schroeder: Il existe certes de tels programmes. Je sais que le Bureau de la concurrence Canada a élaboré « Le petit livre noir de la fraude ». C'est un document auquel on peut avoir accès qui porte sur ce genre de problèmes.

Il faut faire connaître ces ressources et les rendre largement accessibles, en les offrant dans les organismes de services sociaux, les banques et d'autres organisations. C'est nécessaire à mon avis.

Étant donné que les aînés constituent un groupe démographique important, il faut s'assurer que ces ressources sont offertes en ligne et en format papier. Je dirais qu'il faut davantage faire la promotion de ces ressources.

En ce qui concerne les nouvelles mesures qui sont mises en place, pour faire suite à ce que M. Baran-Chong vient de dire, je dirais que nous diffusons très bien l'information au sujet des fraudes liées à l'ARC, des escroqueries romantiques et de ce genre de choses, mais les entreprises de télécommunications, notamment, doivent mieux transmettre l'information concernant les nouvelles fraudes et les choses que les gens doivent savoir.

La présidente: Je vous remercie beaucoup.

La parole est maintenant à Mme Jaczek.

Mme Helena Jaczek (Markham—Stouffville, Lib.): Je vous remercie, madame la présidente.

Madame Schroeder, je comprends bien vos propos et je suis tout à fait d'accord avec vous.

Un des témoins précédents, M. Lawford, a parlé du fait que certains aînés abandonnent leur ligne terrestre parce qu'ils en ont assez des fraudes téléphoniques, des appels importuns, etc. Êtes-vous au courant de cela? Est-ce que cela est un problème pour vos clients?

Mme Kate Schroeder: Oui, cela se produit. Je pense qu'à mesure que la population vieillit, elle passe de plus en plus à la téléphonie mobile. Je crois que nous pouvons tous convenir que cela ne règle pas nécessairement le problème.

Je pense qu'il y a deux éléments. Si les aînés se contentent d'éliminer leur ligne terrestre, nous nous inquiétons bien entendu du fait que cela ne fera qu'accroître leur isolement social et nous nous demandons comment nous pourrons joindre ces personnes, si un problème survient, pour nous assurer qu'elles sont en sécurité et qu'elles vont bien.

En ce qui concerne les téléphones mobiles, je peux vous dire qu'il y a autant d'appels frauduleux sur les téléphones cellulaires que sur les téléphones fixes. C'est ce que nous constatons. Je pense que c'est préoccupant, car cela ne fait qu'amplifier nos préoccupations concernant les risques potentiels pour ces personnes.

Mme Helena Jaczek: Tout à fait. Comme M. Baran-Chong nous l'a fait remarquer, s'ils abandonnent leur ligne terrestre, ils vont bien entendu commencer à utiliser un téléphone cellulaire, alors on peut présumer qu'ils seront tout aussi susceptibles d'être victimes de ce transfert de SIM dont nous venons d'entendre parler. Jusqu'à hier, je n'étais pas au courant de cette affaire, alors je suis extrêmement heureuse d'en avoir entendu parler.

Monsieur Baran-Chong, vous n'avez pas été en mesure de terminer votre exposé. Vous avez parlé de l'Australie. Là-bas, si quelqu'un prétend avoir perdu son téléphone, il doit personnellement se rendre au magasin et montrer une pièce d'identité délivrée par le gouvernement. Pouvez-vous nous dire ce que le CRTC devrait faire selon vous, étant donné les faits?

● (1235)

M. Randall Baran-Chong: Bien sûr. Je crois qu'il faudrait premièrement inscrire ces mesures dans la réglementation, car nous avons souvent vu les fournisseurs se contenter d'affirmer qu'ils respectent la réglementation. Cependant, la décision a été prise en 2005, et, bien entendu, les menaces ont changé considérablement.

Comme M. Lawford l'a laissé entendre plus tôt, le CRTC doit demander beaucoup plus clairement à l'ACTS et à l'industrie d'être davantage transparentes en ce qui concerne la prévalence de ce problème. Est-ce qu'elles s'y attaquent efficacement?

Nous sommes heureux que le CRTC ait fait parvenir une lettre le 15 janvier dernier, mais dans la lettre qu'il a reçue de l'ACTS, tout ce qui nous intéressait, comme les mesures qui sont prises et la prévalence, a été largement caviardé. En outre, nous n'avons aucune idée du type de mesures prises par l'industrie que le CRTC considérerait comme efficaces, du type de mesures que le CRTC pourrait prendre si l'industrie n'agissait pas, ni du calendrier de mise en œuvre, car plus ce problème persiste, plus il y aura de victimes.

Mme Helena Jaczek: Recommanderiez-vous notamment que les mesures prises par l'ACTS soient rendues publiques? Comment devrait-on procéder selon vous?

M. Randall Baran-Chong: Je pense qu'il faut à tout le moins reconnaître, particulièrement en ce qui concerne les mesures de protection des clients, que les mesures prises doivent être divulguées et que les clients doivent être partie prenante. J'ai parlé du problème des messages texte qui ont été envoyés. Les gens n'étaient pas au courant qu'une nouvelle mesure de protection avait été mise en place, alors ils ont immédiatement été sceptiques. Il faut davantage rendre publiques ce genre de mesures.

Je peux comprendre, toutefois, qu'il faut mieux former le personnel. Je ne peux pas vous dire le nombre de fois que j'ai communiqué avec mon entreprise de télécommunications et que j'ai dû expliquer à ses représentants du service à la clientèle les politiques de l'entreprise sur le portage — en fait, je l'ai même fait hier soir. J'ai pratiquement fait de la sociologie appliquée pour obtenir mon numéro d'identification personnel de la part d'une personne qui ne... J'ai fourni des renseignements qui sont très faciles à obtenir.

Il faut donc former les employés. Je comprends si cela n'est pas nécessairement divulgué publiquement, mais il faut que les autres informations soient rendues publiques.

Mme Helena Jaczek: Hier, nous avons pris connaissance d'un article sur la fraude liée aux SIM. Il semble que la Police provinciale de l'Ontario ait diffusé des conseils sur la façon dont les gens peuvent se protéger.

Vous avez parlé de la protection des renseignements personnels — ne pas répondre aux courriels d'hameçonnage et aux messages texte — mais je ne connais absolument pas les gestionnaires hors ligne de mots de passe. Pouvez-vous m'expliquer de quoi il s'agit?

M. Randall Baran-Chong: Il s'agit des jetons logiciels que j'ai mentionnés plus tôt. C'est comme Google Authenticator. Ce logiciel génère un code sur votre téléphone et vous demande d'entrer ce code dans votre application. Au lieu de recevoir un message texte, vous recevez un code. On peut aussi utiliser un jeton matériel. Certaines personnes ont peut-être déjà vu ces clés RSA qui génèrent un code également. L'authentification pourrait se faire à l'aide d'un jeton logiciel ou matériel. Essentiellement, il ne faut pas qu'il soit lié à notre téléphone.

Mme Helena Jaczek: Je vous remercie beaucoup.

La présidente: Merci.

[*Français*]

Monsieur Lemire, vous avez la parole.

M. Sébastien Lemire: Merci, madame la présidente.

Je vais poursuivre avec M. Baran-Chong.

[*Traduction*]

Je comprends votre réalité et je vous suis reconnaissant d'utiliser votre expérience pour faire de la prévention auprès des gens.

[*Français*]

Vous avez formulé plusieurs de vos attentes envers le CRTC. Elles figurent à la fin de votre document et je remercie Mme Jaczek de l'avoir souligné.

En avez-vous d'autres relativement au CRTC? De plus, en avez-vous pour ce qui est de la GRC et des compagnies de télécommunications?

● (1240)

[*Traduction*]

M. Randall Baran-Chong: Je vais vous donner un exemple. Les différents organismes d'application de la loi qui s'occupent de ce problème ont reconnu, je crois, qu'il doit y avoir une meilleure coordination. Même si ces criminels travaillent sans doute au sein de groupes rapprochés, il y a des victimes un peu partout au pays. La GRC a mis sur pied le Groupe national de coordination contre la cybercriminalité, qui commencera ses activités à la fin du mois d'avril, je crois. Ce groupe sera en mesure d'assurer une meilleure coordination en ce qui a trait à ce genre de cas. Lorsque nous, les victimes, faisons part de notre histoire, nous pouvons souvent déceler des dénominateurs communs. Nous transmettons cela aux agents d'application de la loi qui travaillent sur nos cas.

Comme nous l'avons dit, ces nouveaux types d'avis et de vérifications préalables au portage doivent être codifiés et il faut davantage de transparence quant à ce qui se passe au sujet du portage. Nous devons veiller à ce que les entreprises de télécommunications mettent en place des politiques uniformes. Enfin, je pense que les gouvernements et l'industrie devraient faire l'objet d'une étude, sur le plan de la gestion des données sensibles, pour voir s'ils ont recours à l'authentification à deux facteurs par message texte et déterminer comment ils peuvent passer à un autre type d'authentification. Autrement, nous nous exposons aux transferts de SIM.

[*Français*]

M. Sébastien Lemire: Dans la situation dont vous avez été victime, avez-vous reçu un soutien ou de l'aide de la part de quelque intervenant que ce soit?

[*Traduction*]

M. Randall Baran-Chong: On m'a offert 100 $.

[*Français*]

M. Sébastien Lemire: C'est tout?

[*Traduction*]

M. Randall Baran-Chong: Oui, je crois que cela en dit long.

[*Français*]

M. Sébastien Lemire: C'est consternant!

Vous avez parlé de la vente illicite de données par des employés. Comment peut-on aider les compagnies à se doter de meilleures mesures de sécurité qui empêcheraient de vendre aussi facilement les informations des clients? Je pense ici au cas de Desjardins, qui retient beaucoup l'attention au Québec. Faut-il augmenter les fouilles des intranets ou les rondes des agents de sécurité, ou prendre d'autres mesures? Que suggérez-vous pour agir à la source?

[*Traduction*]

M. Randall Baran-Chong: Les particuliers sont également responsables en partie de la protection de leurs données, notamment de ce qu'ils mettent dans le nuage. Dans une certaine mesure, on agit un peu en idiot en téléversant presque tout. Je ne savais même pas en fait que tout cela était téléversé dans le nuage, car je ne l'utilisais pas vraiment.

J'ai voulu raconter mon histoire pour que les gens sachent qu'il faut faire attention à ce qui est téléversé. Ironiquement, des spécialistes en cybersécurité nous disent de ne pas utiliser le nuage, d'avoir recours à un disque dur externe. Ils nous disent même de ne pas enregistrer nos mots de passe dans nos navigateurs, de les écrire plutôt sur papier avec un marqueur plutôt qu'avec un stylo qui laisserait une empreinte sur le papier. Nous faisons un virage à 180^{o} lorsqu'il s'agit de faire davantage attention à ce que nous téléversons. Pour les clients, le plus important, c'est d'être conscients de ce qui se trouve dans le nuage.

[*Français*]

M. Sébastien Lemire: Votre message a été entendu.

J'ai une dernière question. M. Lawford a parlé plus tôt du besoin d'une enquête publique: êtes-vous d'accord avec lui?

[*Traduction*]

M. Randall Baran-Chong: Tout à fait. Nous sommes pratiquement des âmes sœurs. J'ai pris connaissance de sa lettre lorsque nous étions en train de voir quelles parties prenantes étaient intéressées. Si nous avions fait part des solutions auxquelles nous avions pensé — qui étaient très similaires à celle mise en œuvre en Australie — et si elles avaient été mises en place il y a quelques mois, lorsque la méthode par message texte a été adoptée en novembre, certaines personnes ne feraient pas partie de notre groupe parce qu'elles auraient été prévenues. Elles auraient été informées au préalable.

[*Français*]

M. Sébastien Lemire: Merci beaucoup.

Ma prochaine question s'adresse à vous, madame Schroeder. Vous avez parlé d'une campagne de prévention et du défi que présente le transport, particulièrement en zone rurale. Pourriez-vous nous en dire plus sur cette situation? Est-elle effectivement plus grave dans les zones rurales? Y a-t-il proportionnellement plus de victimes dans ces zones? Unprogramme d'aide et de sensibilisation à l'achat en ligne pourrait-il faire partie de la solution? Est-ce qu'il existe une technologie plus adaptée aux aînés et qui pourrait mieux les protéger?

● (1245)

[*Traduction*]

Mme Kate Schroeder: Pour faire suite à ce commentaire, je recommanderais... Dans les collectivités rurales, les gens n'ont pas nécessairement accès à de nombreux services sociaux. Plus la population est grande, plus il y a de services sociaux, d'établissements et d'activités auxquelles les gens peuvent participer. Dans les collectivités rurales, les documents de sensibilisation, les programmes et toute la documentation sont fournis en format papier, alors...

La présidente: Madame Schroeder, votre temps est malheureusement écoulé. Peut-être que la prochaine personne vous laissera continuer.

Monsieur Masse, la parole est à vous.

M. Brian Masse: Merci.

Madame Schroeder, si vous voulez terminer, allez-y.

Mme Kate Schroeder: Il faut entreprendre une campagne de sensibilisation ou veiller à ce que ces ressources... Il faut adopter une approche axée sur la collaboration. Il faut s'assurer que l'information qui existe est transmise aux différents services sociaux, ainsi qu'aux banques, aux compagnies d'assurances et aux entreprises de télécommunications. Dans les régions rurales ou peu peuplées, la même information et les mêmes ressources doivent être mises à la disposition de tout le monde.

M. Brian Masse: Comment les aînés avec lesquels vous travaillez en ce moment suivent-ils les conseils des entreprises de télécommunications relativement à la protection de la vie privée? Je ne suis pas très convaincu que c'est une priorité pour elles vu la frustration et la situation actuelle. En fait, nous savons qu'il n'y a pas beaucoup de ressources consacrées à la prévention de la fraude. Même la GRC a admis ici même que la police n'oriente pas bien les gens.

Compte tenu du fait que les gens paient cher pour ces choses, qu'il s'agisse d'une ligne terrestre ou d'un téléphone cellulaire, savez-vous si les entreprises de télécommunications prennent des mesures pour prévenir les fraudes ciblant les aînés?

Mme Kate Schroeder: Je dois dire honnêtement que je n'ai pas vu beaucoup d'entreprises de télécommunications prendre des mesures pour prévenir ces fraudes.

Malheureusement, mon travail s'effectue habituellement après que la fraude a été commise. La fraude a déjà eu lieu, ce qui signifie que les mesures de prévention n'ont pas vraiment fonctionné.

Cependant, je conviens avec vous qu'il semble y avoir un manque de soutien pour le signalement des cas de fraude. Les gens ne savent pas à qui s'adresser ni comment signaler les fraudes. Je crois qu'il y a un manque de soutien de la part des entreprises de télécommunications. Elles ne fournissent pas suffisamment de renseignements sur les principales escroqueries qui ont une incidence sur leurs clients actuellement. Je suis tout à fait d'avis qu'il faudrait adopter une approche davantage axée sur la collaboration en ce qui a trait à la sensibilisation des clients.

M. Brian Masse: Il doit y avoir un équilibre. Les clients génèrent des recettes très importantes et des sommes d'argent énormes vont au crime organisé ou aux fraudeurs, qu'ils soient petits ou non, et il ne semble pas y avoir une réaction proportionnée à ce problème pour les gens qui continuent à être des victimes.

Quelles mesures de soutien sont offertes aux victimes dans votre collectivité? Existe-t-il des services de counselling? Il y a des gens qui non seulement deviennent des victimes — comme M. Lawford l'a mentionné, ce n'est pas un crime jusqu'à ce qu'on perde de l'argent — mais qui aussi ne signalent pas la fraude. Ils ressentent de la honte, ils perdent leur estime de soi et ils sont gênés.

Savez-vous s'il existe des mesures de soutien? Je sais que la police de Windsor et d'autres entités essaient de faire ce qu'elles peuvent, mais il n'y a pas de services de base. Il faut mettre en place des services pour les victimes.

Mme Kate Schroeder: Nous avons remarqué que le soutien diffère d'une province à l'autre et d'un territoire à l'autre. Chaque administration a ses propres mesures de soutien. Je pense qu'en Alberta et en Colombie-Britannique, il existe des services d'assistance téléphonique.

Toutefois, je crois qu'un système de soutien général, un système de soutien centralisé s'impose. Je peux vous dire que, lorsque nous nous sommes adressés à la police pour signaler une fraude, la réaction n'a pas toujours été la même. Dans certains cas, des agents dans des détachements locaux ont rencontré les clients pour les aider et leur indiquer ce qu'ils devaient faire. Dans d'autres cas, je dois dire, honnêtement, que nous avons observé le contraire.

Je crois fermement que nous avons besoin d'adopter une approche simple et rigoureuse quant à ce que les gens, les aînés, doivent faire.

Il est aussi très difficile de signaler une fraude à une institution financière. Les gens trouvent que les formulaires sont longs et qu'ils ne sont pas clairs, et ils ne bénéficient pas de beaucoup de soutien à cet égard.

Il est certes nécessaire que les entités et les organismes collaborent pour assurer un meilleur soutien.

● (1250)

M. Brian Masse: Monsieur Baran-Chong, vous avez mentionné qu'on vous a offert 100 $, mais je crois que le message que vous voulez transmettre, qui est celui que nous avons entendu de la part de nombreux experts déjà, c'est que la prévention constitue la meilleure stratégie.

Comment évaluez-vous la réaction et les mesures de prévention des entreprises avec lesquelles vous avez communiqué à ce sujet? Où croyez-vous en être quant à l'obtention de certaines des mesures que vous avez mentionnées, qui pourraient prévenir certaines des fraudes dont vous avez été victime, dans le cadre de vos démarches pour la coalition que vous représentez?

M. Randall Baran-Chong: D'autres victimes et moi-même avons offert notre soutien aux entreprises de télécommunications à de nombreuses reprises, mais nous n'avons reçu aucune réponse de leur part jusqu'ici.

S'il s'agit d'une industrie qui est véritablement axée sur le service à la clientèle et qui affirme qu'il est dans son intérêt de bien servir et protéger les clients, elle ne fait pourtant pas appel à nous du tout. Jusqu'à maintenant, lorsqu'elle a essayé de mettre des mesures en place... sans consulter les clients, ces mesures n'ont manifestement pas fonctionné.

M. Brian Masse: Vous déclenchez des signaux d'alarme.

Pour ce qui est de la direction que nous prenons en ce moment, quel sera l'enjeu selon vous, si nous agissons maintenant — je sais que je vous demande une prévision — dans six mois ou dans un an? Que se passera-t-il à votre avis si nous ne tenons pas compte de ces signaux d'alarme déclenchés par les personnes qui ont été victimes de fraude?

La présidente: Vous avez cinq secondes.

M. Randall Baran-Chong: Comme le sénateur Wyden aux États-Unis l'a souligné, cela deviendra un risque pour la sécurité nationale. Par exemple, il pourrait y avoir une prise de contrôle des comptes de représentants du gouvernement.

La présidente: Je vous remercie.

Je vais demander aux membres du Comité s'ils souhaitent que nous passions à un autre tour. Nous devons approuver des choses liées à des études.

Voulez-vous poursuivre avec un autre tour et rester un peu au-delà de 13 heures, ou préférez-vous mettre fin aux questions pour passer aux affaires concernant les études?

Mme Emmanuella Lambropoulos (Saint-Laurent, Lib.): Je préfère que nous mettions fin aux questions.

La présidente: D'accord.

M. Brian Masse: J'aurais une dernière question à poser.

La présidente: Malheureusement, votre temps est complètement écoulé, monsieur Masse.

M. Brian Masse: Dans ce cas, j'aimerais que nous poursuivions avec les témoins puisqu'ils sont ici.

The Chair: D'accord.

Madame Gray, la parole est à vous.

Mme Tracy Gray: Je suis désolée, madame la présidente, mais je ne suis pas libre après la réunion, alors je ne pourrai pas rester plus longtemps.

M. Majid Jowhari: Il en va de même pour moi, madame la présidente.

La présidente: Nous pouvons faire des tours plus rapides. Nous pouvons peut-être faire deux tours de deux minutes et demie. Est-ce que cela vous convient? D'accord.

Monsieur Dreeshen, vous disposez de deux minutes et demie.

M. Earl Dreeshen (Red Deer—Mountain View, PCC): Je vous remercie beaucoup.

Premièrement, madame Schroeder, vos propos donnent à penser que, lorsqu'un aîné a été victime de fraude, peu importe laquelle, il y a toujours cette crainte que les enfants lui disent qu'il n'est pas en mesure de gérer son argent et qu'ils vont alors devoir le faire pour lui. Je crois vraiment qu'il faudrait davantage faire savoir aux aînés qu'ils ne sont pas à blâmer, car cela arrive à n'importe qui.

Je crois que c'est l'une des choses auxquelles vous avez fait référence, mais j'essaie simplement de le dire un peu plus clairement. Je crois que nous devrions réfléchir à cela durant nos discussions.

Monsieur Baran-Chong, vous avez parlé de différentes mesures que nous pouvons prendre, comme je l'ai mentionné plus tôt, en ce qui concerne les aînés. Je crois que d'investir dans l'éducation du public serait utile, afin que ces personnes comprennent le problème.

Une de vos diapositives porte sur un appel à l'action de la part des Canadiens. Vous avez mentionné que le CRTC ne semble pas intéressé et vous avez également dit que les entreprises de télécommunication semblent se mettre la tête dans le sable.

Pouvez-vous nous expliquer, en une minute et 10 secondes, ce que nous pourrions faire?

M. Randall Baran-Chong: Je crois qu'il vaudrait la peine d'effectuer une étude pour voir comment les industries utilisent les méthodes d'authentification.

En particulier, par exemple, beaucoup de banques encouragent encore le recours à l'authentification à deux facteurs par message texte. Comme nous l'avons mentionné, nous essayons vraiment d'abandonner cette méthode. Nous devons encourager les industries qui détiennent des renseignements sensibles de nature financière ou personnelle à non seulement adopter des méthodes d'authentification à deux facteurs autres que par message texte, mais aussi à encourager leurs clients à utiliser ces méthodes. De nombreuses applications vous demandent votre numéro de téléphone, et c'est la première chose qu'on veut obtenir. On pourrait penser que c'est parce qu'on veut davantage de données sur vous, mais nous devons amener les industries à promouvoir l'authentification à deux facteurs qui ne s'effectue pas par message texte.

● (1255)

M. Earl Dreeshen: Merci.

La présidente: Je vous remercie beaucoup.

La dernière question de deux minutes et demie sera pour Mme Lambropoulos.

Mme Emmanuella Lambropoulos: Merci.

Je tiens à remercier M. Baran-Chong et Mme Schroeder d'être ici aujourd'hui pour répondre à nos questions. Puisque j'ai obtenu une réponse à la plupart de mes questions, je vais poser à Mme Schroeder des questions plus précises.

Vous avez donné des statistiques tout à l'heure. Vous avez dit que, cette année, il y a eu environ 4 000 cas de fraude au Canada. Est-ce que ce chiffre concerne les aînés précisément ou la population en général?

Mme Kate Schroeder: Vous parlez de cette statistique en particulier?

Mme Emmanuella Lambropoulos: S'agit-il du nombre d'aînés qui ont été victimes de fraude ou du nombre de personnes dans la population en général?

Mme Kate Schroeder: C'est le nombre de Canadiens en général.

Mme Emmanuella Lambropoulos: Savez-vous combien d'aînés ont été victimes de fraude?

Mme Kate Schroeder: Je n'ai pas ce chiffre en ce moment, mais, compte tenu de ce que nous savons, ce qui est inquiétant, c'est que les taux de signalement sont extrêmement bas.

Mme Emmanuella Lambropoulos: Est-ce que les aînés avec lesquels vous avez travaillé se plaignent principalement d'avoir été victimes de fraude sur un téléphone fixe ou un téléphone cellulaire? Quel est le plus...

Mme Kate Schroeder: Je crois que c'est les deux. Il y a encore beaucoup de lignes terrestres, mais il y a aussi de la fraude sur les téléphones cellulaires... Alors, oui, il y a les deux.

Mme Emmanuella Lambropoulos: Merci.

Monsieur Baran-Chong, vous avez dit quelque chose qui m'a frappée. Vous avez dit que les entreprises de téléphonie cellulaire sont souvent ouvertes, particulièrement pour les clients commerciaux, de 8 heures à 16 heures, alors que les gens peuvent être victimes de fraude à toute heure de la journée.

Quelles recommandations précises feriez-vous dans le but d'aider les gens dans votre situation?

M. Randall Baran-Chong: Après ce qui m'est arrivé avec mon téléphone cellulaire, j'ai été en mesure de communiquer avec Visa immédiatement. Cette compagnie dispose d'une ligne d'urgence accessible 24 heures sur 24 pour signaler les fraudes. Pourquoi est-ce que ce n'est pas la même chose pour les entreprises de télécommunications? J'ai même essayé d'appeler le service à la clientèle, accessible 24 heures sur 24, mais le représentant n'avait pas accès à mes renseignements commerciaux.

Si une entreprise détient des renseignements sensibles de nature financière ou personnelle, elle devrait disposer d'une ligne d'urgence accessible 24 heures sur 24 pour signaler les fraudes et bloquer l'accès pour empêcher les fraudeurs d'aller plus loin.

Mme Emmanuella Lambropoulos: Est-ce qu'il me reste du temps?

La présidente: Dix secondes.

M. Brian Masse: J'invoque le Règlement, madame la présidente.

Je ne veux pas interrompre la discussion, mais l'ordre du jour indique que la réunion doit se terminer à 13 heures. J'ai une brève question à poser au témoin. J'aimerais demander la permission, ou le consentement unanime, pour poser cette question. C'est une question simple, et ensuite, nous pourrons continuer. Je vous en serais reconnaissant.

La présidente: Y a-t-il consentement unanime?

Des députés: D'accord.

La présidente: Allez-y, monsieur Masse.

M. Brian Masse: Je vous remercie beaucoup, madame la présidente.

Très rapidement, en ce qui concerne l'étude du CRTC, pouvez-vous me dire dans quelle mesure il est important selon vous que cette étude s'effectue immédiatement?

M. Randall Baran-Chong: Tant que la porte sera ouverte, il y aura des victimes. Le CRTC doit obtenir le plan des entreprises de télécommunications. Il doit savoir comment les entreprises prévoient le mettre en oeuvre. Il doit s'assurer de la mise en oeuvre de ce plan. Le public, les clients et les personnes qui sont exposées à ces menaces devraient apporter leur contribution.

La présidente: J'aimerais remercier les témoins d'avoir fait part de leurs histoires et de nous avoir renseignés sur la réalité à laquelle font face les Canadiens de nos jours.

J'aimerais demander aux membres de rester encore un instant. Nous devons examiner rapidement les budgets pour trois études, y compris celle sur le projet de loi C-4, qui a déjà été effectuée, afin que nous puissions rembourser certaines dépenses des témoins.

Je vais laisser le greffier expliquer le document que vous avez en main concernant les budgets pour les trois études.

Le greffier du comité (M. Michael MacPherson): Je n'ai pas grand-chose à ajouter. Il s'agit de budgets fondés sur les dépenses globales des témoins. L'argent qui ne sera pas dépensé sera récupéré.

M. Brian Masse: Je propose que les trois budgets fassent l'objet d'une seule motion.

(La motion est adoptée.)

La présidente: Merci.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : https://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: https://www.ourcommons.ca