CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

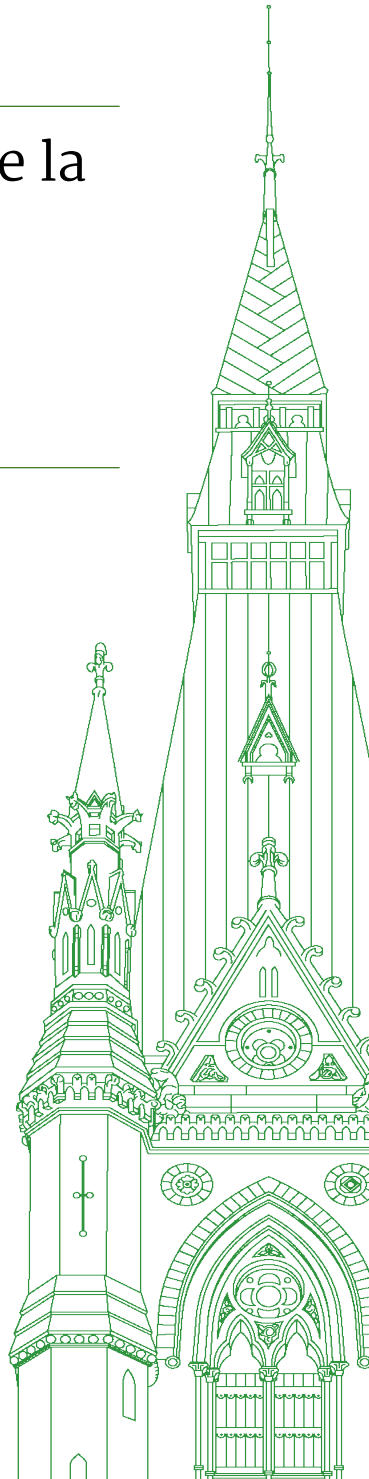
44e LÉGISLATURE, 1re SESSION

# Comité permanent de l'industrie et de la technologie

TÉMOIGNAGES

**NUMÉRO 036**

Le lundi 3 octobre 2022



Président : M. Joël Lightbound

# Comité permanent de l'industrie et de la technologie

**Le lundi 3 octobre 2022**

● (1100)

[*Français*]

**Le président (M. Joël Lightbound (Louis-Hébert, Lib.)):** Je déclare la séance ouverte.

[*Traduction*]

Bienvenue à la 36e réunion du Comité permanent de l'industrie et de la technologie de la Chambre des communes.

Conformément au paragraphe 108(2) du Règlement et à la motion adoptée par le Comité le lundi 26 septembre, notre réunion portera sur le thème des appels frauduleux au Canada.

[*Français*]

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre adopté par la Chambre le jeudi 23 juin 2022. D'ailleurs, je suis désolé de me joindre à vous virtuellement aujourd'hui. Je préfère toujours être là en personne, mais cela m'est impossible aujourd'hui.

Cependant, nous avons la chance de recevoir plusieurs témoins qui se joignent à nous en personne au cours de la première heure aujourd'hui, dont des représentants de la Gendarmerie royale du Canada: le superintendant Denis Beaudoin, directeur, Criminalité financière; le sergent Guy Paul Larocque, officier responsable intérimaire du Centre antifraude du Canada; et M. Chris Lynam, directeur général, Coordination nationale contre la cybercriminalité.

Lors de la deuxième heure, nous recevrons M. Randall Baran-Chong, cofondateur de Canadian SIM-swap Victims United; M. Kevin Cosgrove, éducateur en sécurité numérique et conseiller civil; et finalement, M. John Mecher, enquêteur de la GRC à la retraite. Ces derniers témoigneront à titre personnel.

Sans plus tarder, je cède la parole aux représentants de la Gendarmerie royale du Canada pour cinq minutes.

[*Traduction*]

**M. Chris Lynam (directeur général, Coordination nationale contre la cybercriminalité, Gendarmerie royale du Canada):** Bonjour.

Monsieur le président, distingués membres du Comité, je suis heureux de me joindre à vous aujourd'hui pour discuter de l'importance des appels frauduleux et autres escroqueries au Canada, ainsi que des efforts que la GRC a entrepris depuis la dernière fois où nous nous sommes rencontrés à ce sujet en mai 2020.

Je m'appelle Chris Lynam. Je suis le directeur général du Groupe national de coordination contre la cybercriminalité, le GNC3, et du Centre antifraude du Canada, le CAFC, de la Gendarmerie royale du Canada, la GRC. Se joignent à moi aujourd'hui le sergent Guy Paul Larocque, qui est officier responsable intérimaire du CAFC, ainsi que le surintendant Denis Beaudoin, le directeur, Criminalité financière au sein des Opérations criminelles de la Police fédérale.

Avant de parler des appels frauduleux et des autres escroqueries qui touchent les Canadiens, j'aimerais décrire brièvement les mandats du CAFC et du GNC3. Premièrement, le CAFC comprend un partenariat de longue date entre la GRC, la Police provinciale de l'Ontario et le Bureau de la concurrence Canada. Le CAFC travaille en étroite collaboration avec ses partenaires canadiens et internationaux chargés de l'application de la loi pour lutter contre la fraude par marketing de masse et d'autres types de fraude, notamment les appels frauduleux.

En 2021, le CAFC a aligné ses activités opérationnelles sur celles du GNC3, un autre service national de police de la GRC axé sur la lutte contre la cybercriminalité. Alors que le CAFC se concentre sur la fraude et les escroqueries en ligne, le GNC3 se concentre davantage sur la lutte contre la cybercriminalité axée sur la technologie, comme les rançongiciels, les atteintes à la protection des données et autres cyberintrusions. Le CAFC et le GNC3 travaillent en étroite collaboration étant donné les liens étroits entre la fraude et la cybercriminalité et son objectif de fournir des services hautement coordonnés à la communauté canadienne et internationale d'application de la loi.

Depuis notre dernière comparution devant le Comité en 2020, le CAFC et le GNC3 ont constaté une augmentation importante des activités frauduleuses au Canada. En 2021, le CAFC a reçu des rapports indiquant que les victimes avaient subi des pertes de 379 millions de dollars dues à la fraude. Il s'agit d'une année historique sur le plan des pertes de ce type qui ont été signalées, avec une augmentation de 130 % par rapport à l'année précédente. En même temps, le CAFC estime que seulement 5 à 10 % des victimes signalent ces fraudes à la police.

Parmi les pertes liées à la fraude signalées par les victimes en 2021, plus de 70 % étaient cybernétisées, ce qui signifie que l'activité frauduleuse a été commise par l'intermédiaire d'Internet ou de plateformes numériques connexes comme le courriel ou les médias sociaux. Ces tendances et la convergence de la fraude cybernétique avec d'autres activités de cybercriminalité soulignent l'importance de la collaboration entre le CAFC et le GNC3, et la nécessité pour les organismes canadiens d'application de la loi de s'adapter continuellement et de suivre la cadence.

Malgré l'augmentation des escroqueries en ligne, les Canadiens continuent d'être ciblés par des appels frauduleux.

[*Français*]

En 2021, le Centre antifraude du Canada, le CAFC, a reçu plus de 32 000 signalements de tentative de fraude dont la victime a été contactée par téléphone par le fraudeur. Les appels téléphoniques frauduleux peuvent inclure, entre autres, des tentatives de criminels prétendant représenter des forces de l'ordre ou l'Agence du revenu du Canada, des banques ou d'autres institutions financières.

● (1105)

[*Traduction*]

Détrompez-vous, il est incroyablement difficile d'enquêter et d'appréhender les fraudeurs et les cybercriminels. Souvent, nous avons affaire à des milliers de victimes, à de multiples autorités policières, à des infrastructures de cybercriminalité et à des preuves numériques dans des pays étrangers.

[*Français*]

En revanche, ces défis ont également servi de catalyseur pour les services de police canadiens. Nous nous sommes adaptés, nous avons accéléré nos efforts de collaboration avec des partenaires aux vues similaires, et nous avons adopté une approche plus globale quant à la lutte contre la fraude et la cybercriminalité.

Divers programmes de la GRC continuent de jouer un rôle clé dans plusieurs opérations internationales de lutte contre la cybercriminalité et la fraude. Cependant, nous reconnaissons également que la fraude sous toutes ses formes est un défi omniprésent et durable et que nous ne pouvons simplement pas procéder à des arrestations pour échapper à ce problème. Notre réponse à la fraude nécessite des efforts plus importants.

[*Traduction*]

Par exemple, dans certains cas et lorsque cela est possible, nous travaillons en étroite collaboration avec des partenaires nationaux et internationaux pour aider au recouvrement de fonds dérobés par des stratagèmes de fraude. En 2021, le CAFC a collaboré à 36 cas de gel ou de recouvrement de fonds totalisant environ 3,4 millions de dollars.

Un autre aspect essentiel de la lutte contre la fraude et la cybercriminalité est la prévention, l'information et la sensibilisation. C'est une heureuse coïncidence que je puisse m'adresser à vous pendant le mois d'octobre, mois de la sensibilisation à la cybersécurité. L'un des thèmes clés de nos activités de prévention ce mois-ci est le matériel de sensibilisation et de prévention sur les techniques d'hameçonnage, ou *phishing*, utilisées par les fraudeurs. Nos efforts de prévention se poursuivent tout au long de l'année, avec un autre mois notable en mars consacré à la prévention de la fraude. L'année dernière, pour le mois de la prévention de la fraude, nous avons mis l'accent sur la sensibilisation aux escroqueries par usurpation d'identité.

En conclusion, nos efforts au cours des dernières années ont été importants. Insuffisants, mais significatifs, et nous restons déterminés à trouver de nouvelles façons de protéger les Canadiens et de réduire la victimisation associée à la fraude et à la cybercriminalité.

J'aimerais vous remercier de m'avoir donné l'occasion de m'adresser à vous aujourd'hui. Nous sommes prêts à répondre à vos questions.

**Le président:** Merci beaucoup, monsieur Lynam.

Je donne la parole aux députés, en commençant par M. Michael Kram. Vous avez six minutes.

**M. Michael Kram (Regina—Wascana, PCC):** Merci beaucoup, monsieur le président.

Merci aux témoins qui comparaissent devant nous aujourd'hui. Je devrais sans doute commencer par souligner l'immense travail de la GRC et l'en remercier. Je pense que les politiciens et le public en général semblent trouver tout naturel que le travail des forces de l'ordre soit difficile. Certes, mais je tiens quand même à vous remercier pour tout ce que vous accomplissez.

La fraude par télémarketing n'est pas un mince problème. Pourriez-vous nous expliquer un peu de quoi il retourne? Quand vous menez une enquête sur un incident de fraude par télémarketing, en quoi vos méthodes diffèrent-elles selon que les auteurs se trouvent au Canada ou à l'étranger?

**Surint. Denis Beaudoin (directeur, Criminalité financière, Gendarmerie royale du Canada):** Les méthodes ne sont pas vraiment différentes de celles que nous appliquons pour d'autres types d'enquêtes. Si les suspects sont au Canada, nous faisons appel à la vaste gamme d'outils à notre disposition, y compris les ordonnances de communication et les mandats de perquisition. S'ils ne sont pas au Canada, nous devrons travailler en partenariat et solliciter l'aide de gouvernements étrangers, ce qui retarde souvent l'enquête. C'est une des grandes différences.

Il y en a d'autres, mais je crois que c'est la principale. Pour obtenir des éléments de preuve à l'extérieur du Canada, nous avons besoin de l'appui d'une autorité étrangère.

**M. Michael Kram:** Pouvez-vous nous en dire davantage au sujet de votre coopération avec des autorités étrangères? Est-ce que cette coopération est généralement aisée ou plus souvent un parcours d'obstacles?

**Surint. Denis Beaudoin:** Bien entendu, tout dépend du pays dont l'aide est sollicitée. Nous entretenons des relations très étroites avec nos proches alliés, mais c'est plus difficile avec d'autres pays. Comme de raison, c'est le ministère de la Justice qui transmet les demandes d'assistance en vue de l'obtention d'éléments de preuve à son homologue du pays visé.

Un processus est en place, mais il peut être difficile d'obtenir un élément de preuve si nous faisons face à un pays qui refuse de collaborer ou qui est réticent. Inutile de vous dire que c'est un des grands enjeux qui compliquent nos enquêtes.

● (1110)

**M. Michael Kram:** Quand le Comité a étudié cette question il y a deux ans, il a recommandé dans son rapport d'inclure la collaboration en matière de fraude par télémarketing dans les futurs accords de libre-échange. La semaine dernière, nous avons reçu des représentants du Conseil de la radiodiffusion et des télécommunications canadiennes, le CRTC, qui nous ont suggéré qu'il serait plus productif de recourir à d'autres cadres ou accords que les accords de libre-échange avec d'autres pays.

J'aimerais entendre les témoins au sujet des cadres ou des accords que le Canada pourrait conclure avec d'autres pays pour lutter contre ce problème.

**M. Chris Lynam:** Je ne crois pas que nous aurons besoin de nouveaux cadres. Je peux vous parler de certains mécanismes déjà en place.

Comme l'a mentionné le surintendant Beaudoin, il y a une collaboration à l'échelle nationale et internationale. C'est une bonne partie du mandat du CAFC et du GNC3, qui collaborent avec les partenaires chargés de l'application de la loi au Canada pour établir des liens entre leur travail et celui des organismes étrangers. La collaboration avec d'autres pays peut être bilatérale ou multilatérale.

Par exemple, dans le domaine de la cybercriminalité, nous collaborons activement avec le Centre européen de lutte contre la cybercriminalité. Le Centre a établi un groupe de travail conjoint, le Joint Cybercrime Action Task Force, formé de 18 États membres de l'Office européen de police, Europol, ainsi que du Canada, des États-Unis et de l'Australie. Par l'intermédiaire du quartier général d'Europol, nous restons constamment en contact pour la conduite d'enquêtes internationales.

C'est un très bon exemple de collaboration multilatérale. Elle nous permet de faire avancer les enquêtes et, même si elle ne mène pas à l'arrestation ou à la poursuite de cybercriminels ou de fraudeurs, nous pouvons nous en prendre à leurs infrastructures. Et je peux vous dire qu'il y a eu un bon nombre de victoires sur ce front.

**M. Michael Kram:** Si le Canada songe à conclure des accords avec de nouveaux pays, lesquels devraient-ils mettre en priorité selon vous?

**M. Chris Lynam:** Je ne crois pas que je peux recommander une liste de pays. Le Canada doit plutôt continuer d'approfondir ses liens avec ses partenaires les plus proches, soit beaucoup de pays européens et nos alliés du Groupe des cinq, les États-Unis, le Royaume-Uni, la Nouvelle-Zélande et l'Australie. Nous travaillons déjà en collaboration très étroite avec ces partenaires dans de nombreux dossiers internationaux.

**M. Michael Kram:** Dans quelle proportion les incidents sont-ils entièrement tramés au Canada et dans quelle proportion les artisans opèrent-ils à partir d'un autre pays?

**Serg. Guy Paul Larocque (officier responsable intérimaire, Centre antifraude du Canada, Gendarmerie royale du Canada):** C'est assez difficile d'établir un portrait exact de la situation considérant que la majorité des escroqueries ont des ramifications dans plusieurs pays. Pour ce genre de crimes, les auteurs se trouvent au point A, ils ciblent des victimes au point B et ils déplacent l'argent vers le point C. C'est un schéma très fréquent selon les données du Centre antifraude.

La proportion des activités menées ici… Nous savons qu'il y a des activités au Canada, mais beaucoup d'escroqueries qui visent des Canadiens sont commises ailleurs dans le monde. C'est difficile pour moi de vous donner des chiffres précis. Tout ce que je peux vous dire, c'est que les Canadiens sont indéniablement la cible d'escroqueries. Il suffit de jeter un œil aux pertes rapportées par le Centre antifraude pour vous en convaincre.

**M. Michael Kram:** Pour ce qui concerne…

**Le président:** Merci, monsieur Kram. C'est tout le temps que vous aviez. Je suis désolé. Merci beaucoup.

C'est au tour du député Dong. Vous avez six minutes.

**M. Han Dong (Don Valley-Nord, Lib.):** Merci beaucoup, monsieur le président.

Je voudrais à mon tour remercier nos témoins. Bonjour à tous.

Le dernier rapport remonte à deux ans. La technologie a beaucoup évolué en matière de criminalité et de fraude. Pouvez-vous nous expliquer ce que vous avez fait pour vous adapter aux progrès technologiques des criminels?

**M. Chris Lynam:** Une partie du défi, comme vous l'avez dit, consiste à suivre la cadence imposée par des gens qui ont une impressionnante capacité d'adaptation et qui sont des criminels. C'est très facile pour eux de faire volte-face et d'adopter les technologies de pointe ou de trouver une technique plus efficace. Ils observent ce qui se passe quand il y a un incident ou un nouveau programme gouvernemental de remise et, très vite, ils concoctent un scénario pour escroquer les Canadiens.

Ils adaptent également les technologies utilisées en conséquence. Comme nous l'avons évoqué, nous pensons que plus de 70 % de ces activités sont également cybernétiques. Nous collaborons avec nos partenaires chargés de l'application de la loi à l'échelle du pays pour soutenir le développement ou l'acquisition de logiciels et la mise en commun de techniques particulièrement efficaces. Il existe des techniques et nous devons poursuivre les formations sur ces techniques et dans d'autres domaines pour nous assurer d'être mieux préparés.

En quelque sorte, les criminels haussent constamment la barre et nous devons faire de notre mieux pour ne pas être devancés.

● (1115)

**M. Han Dong:** Effectivement. J'ai l'impression que vous êtes condamnés à essayer de rattraper le retard par rapport à leurs technologies et à leurs méthodes.

Avez-vous des statistiques sur les arrestations effectuées au Canada depuis deux ans?

**M. Chris Lynam:** Nous ne recueillons pas de statistiques sur le nombre d'arrestations. Je sais que Statistique Canada publie des rapports périodiques sur la criminalité et la prévalence de la fraude et de la cybercriminalité. Dans certains cas… Année après année, la tendance a été à la hausse dans le domaine de la cybercriminalité.

J'ajouterai à cela que nos activités ne se limitent pas à arrêter les criminels, à porter des accusations ou à les condamner. Nous essayons d'avoir une approche globale pour réduire le nombre de victimes. Nous pouvons par exemple mettre l'accent sur la récupération pour aider les victimes à bloquer ou à récupérer des fonds, comme je l'ai dit tout à l'heure.

Nous tablons aussi sur la coopération avec des fournisseurs de services. Si nous soupçonnons que des fraudeurs utilisent une infrastructure, un domaine Internet ou un site Web quelconque, nous en informons les fournisseurs de services. Ils peuvent ensuite faire le nécessaire pour les mettre hors ligne et prendre d'autres mesures.

La prévention, je le répète, est aussi au cœur de nos efforts. Nous adoptons une approche très globale pour nous attaquer au problème et réduire le nombre de victimes.

**M. Han Dong:** Si vous pouviez nous fournir le nombre exact d'arrestations et de condamnations qui en ont résulté, ce serait très intéressant. Ce genre d'information nous serait très utile. Si vous pouvez mettre la main sur ces chiffres et les transmettre au Comité après la réunion, je vous en serais très reconnaissant.

Pour ce qui est de la méthode, j'ai l'impression que vos efforts sont davantage axés sur la prévention et la récupération des pertes que sur les enquêtes et l'arrestation des criminels. Tant qu'ils resteront libres, ils trouveront le moyen de multiplier les victimes. Cela explique peut-être en partie l'impression générale que les criminels ont toujours une longueur d'avance sur le plan des moyens technologiques et des méthodes.

Dans un autre registre, j'aimerais revenir sur ce que nous a révélé le CRTC la semaine dernière concernant les métadonnées que lui transmettent les industries ou les entreprises de télécommunications. Vous rendez des comptes au CRTC. À votre avis, l'échange d'information entre le CRTC et la GRC, ou ses services, est-il problématique? Par ailleurs, pour ce qui concerne les secteurs des télécommunications et des finances, êtes-vous en mesure d'obtenir des données ou des signalements de leur part en cas d'activités suspectes?

**M. Chris Lynam:** Oui, tout à fait. Si vous me le permettez, je vais revenir sur l'une de vos questions. Je m'en voudrais de laisser le Comité sous l'impression que la police ne fait pas tout en son pouvoir pour mener des enquêtes contre les fraudeurs et les cybercriminels. Une partie très importante du mandat du CAFC et du GNC3 consiste à aider les organismes canadiens d'application de la loi à mener ces enquêtes, de même que la conduite du volet des services de police fédéraux de la GRC. De nombreuses enquêtes sont en cours. Je voulais simplement souligner que nos activités sont plus larges.

Pour ce qui a trait à l'échange d'information entre le CRTC et d'autres organismes, nous nous conformons aux pouvoirs que nous avons en la matière. Nous pouvons communiquer certains éléments d'information au CRTC et vice versa. La plupart des organismes vous diraient qu'il est toujours possible de faire mieux en matière d'échange d'information, mais nous en faisons déjà beaucoup dans ce domaine.

Quant aux organismes du secteur privé comme les entreprises de télécommunications et les établissements financiers, nous devons respecter le fonctionnement des autorités policières. Si nous avons besoin de renseignements de l'une d'elles, il faut généralement obtenir une ordonnance de communication ou suivre un autre processus en place.

Nous recevons souvent des demandes de banques qui pensent qu'elles ou leurs clients ont été victimes d'un crime. Nous avons des contacts réguliers. Nous avons parlé de ce que nous faisons pour les informer d'incidents qui à notre avis pourraient viser des clients de ces établissements.

Bref, de manière générale, nous pouvons toujours apporter des améliorations en matière d'échange d'information.

● (1120)

**M. Han Dong:** Et comment nous, les législateurs, pourrions-nous vous aider à apporter ces améliorations?

**Le président:** Je suis désolé, monsieur Dong, mais nous devons passer à la prochaine série de questions. Votre temps est écoulé.

Je donne la parole au député Masse. C'était au tour de M. Lemire, mais il s'est absenté pour quelques minutes.

Monsieur Masse, allez-y.

**M. Brian Masse (Windsor-Ouest, NPD):** Merci, monsieur le président, et merci à nos témoins. Je sais que M. Lemire reviendra bientôt et je tiens à dire que ses interventions sont toujours fort appréciées.

La dernière question était très intéressante. Pourquoi ce sujet se retrouve-t-il devant le comité de l'industrie? C'est quelque chose qui m'exaspère depuis que je siège à ce comité, et cela fait quelques années. Nous parlons d'un secteur réglementé dans lequel nous laissons des criminels s'adonner à leurs activités sans vraiment être inquiétés. Le secteur des télécommunications… Rien de tout cela ne serait possible et les citoyens n'auraient pas ces problèmes sans la mise aux enchères des fréquences, le libre-accès à notre infrastructure et la réglementation par le CRTC. C'est le cadre idéal pour ce genre d'activités. Cela dit, je salue les efforts déployés, pas seulement maintenant devant notre comité, mais depuis quelques années pour changer les choses.

Ce qui me préoccupe et dont j'aimerais discuter dans le cadre de cette étude est la grande similarité avec la criminalité en col blanc. Cela me semble évident, mais je crois que c'est loin d'être le cas pour le Parlement, à bien des égards. Nous traquons les travailleurs et les criminels urbains, mais je me demande si la législation est assez sévère.

Je vais donner un bref exemple. Dernièrement, à cause de Rogers, les citoyens ont perdu l'accès au service 911… Selon des témoignages que nous avons entendus, il n'y a eu aucune entraide entre les entreprises de télécommunications pour garantir l'accès au service 911. N'est-ce pas le moment de montrer les dents et d'élargir les pouvoirs ou d'améliorer ce qui doit l'être pour que la GRC et d'autres forces policières puissent exiger une meilleure coopération des entreprises de télécommunications?

J'aimerais entendre ce que vous avez à dire à ce sujet.

**M. Chris Lynam:** De toute évidence, le CRTC et le gouvernement du Canada devraient avoir davantage de pouvoirs pour ce qui est de la teneur ou de l'élargissement de la réglementation qui encadre les entreprises de télécommunications. Je peux vous affirmer que la GRC et les autres organismes chargés de l'application de la loi entretiennent de bonnes relations avec ces entreprises. Nous faisons de notre mieux pour collaborer avec elles conformément à nos pouvoirs actuels. Ce n'est toutefois pas à moi de vous dire si le gouvernement devrait resserrer la réglementation de ce secteur. Notre travail est de faire appliquer les dispositions du Code criminel.

**M. Brian Masse:** Oui, je comprends. Je suis fier aussi d'entretenir de bonnes relations avec les entreprises de télécommunications, même si je critique ce qui se passe actuellement. Cela dit, compte tenu des rapports que nous avons reçus non seulement sur les crimes subis par les consommateurs… Le Bureau de la concurrence a mis au jour et documenté certaines tactiques de marketing abusives et agressives que les entreprises de télécommunications intègrent à leurs propres activités, et je me demande s'il y a lieu de revoir les règles qui encadrent ce service prioritaire.

Je sais que vous ne recueillez pas de statistiques à ce sujet, mais y a-t-il des arrestations et des saisies de biens ou d'infrastructures de ce type? Vous avez évoqué dans votre exposé que c'était le cas. En quelques mots, êtes-vous habilités à faire ce genre d'interventions ou devez-vous vous contenter de traquer les individus à l'autre bout de la ligne? Je fais référence à l'infrastructure qu'ils utilisent. Je comprends à quel point c'est difficile étant donné la portée nationale et internationale de tout cela.

**M. Chris Lynam:** Je dirais que c'est un mélange des deux, ou qu'il y a plusieurs facettes. La GRC a pris part à certaines opérations multinationales de grande envergure. Nous avons contribué aux efforts mondiaux pour démanteler des infrastructures et saisir du matériel informatique, des serveurs et d'autres dispositifs utilisés par les cybercriminels et les fraudeurs. Il y a eu des interventions au Canada également.

D'un projet à l'autre, selon l'échelon… Des activités relèvent d'une municipalité ou d'une province. Il y a eu beaucoup d'exemples de belles réussites d'interventions lancées à ces échelons.

**M. Brian Masse:** Il me reste peu de temps. Pourriez-vous nommer deux choses qui vous seraient utiles pour vous attaquer à ce problème? Souhaiteriez-vous que les produits de la criminalité soient réinvestis, que l'argent que vous faites économiser aux Canadiens serve à renforcer vos ressources? Ou pensez-vous qu'une réforme législative est nécessaire? Je vous demande en fait de nous faire quelques suggestions qui nous permettront de vous aider à aider les agents.

● (1125)

**M. Chris Lynam:** La mesure la plus facile à mettre en place, surtout en ce mois d'octobre consacré à la sensibilisation à la cybersécurité, serait de conscientiser tous les Canadiens à ce qui se passe. Tous ceux qui peuvent diffuser ce message, y compris les membres assidus du Comité ici présents, doivent contribuer aux efforts de prévention. C'est un volet central du travail policier. Si nous parvenons à éradiquer une bonne partie de ces activités à la source, nous réduirons le nombre de victimes. Nous avons tous un rôle à jouer dans les efforts pour réduire le nombre de victimes.

[*Français*]

**Le président:** Merci beaucoup, monsieur Masse.

Monsieur Lemire, vous avez la parole pour six minutes.

**M. Sébastien Lemire (Abitibi—Témiscamingue, BQ):** Merci, monsieur le président. Je vous remercie de votre flexibilité.

Je suis désolé s'il y a des éléments redondants. Parfois, la vie de parlementaire nous oblige à être à deux endroits en même temps.

Dans le contexte des appels frauduleux, je m'inquiète beaucoup de la vulnérabilité des personnes aînées.

Pouvez-vous nous dire si de nouveaux types de fraudes touchent les aînés et nécessitent une meilleure sensibilisation?

Les campagnes de sensibilisation sont-elles assez incisives pour bien toucher nos aînés? Conséquemment, à quel point ceux-ci sont-ils vulnérables?

**M. Chris Lynam:** Je vais laisser le sergent Larocque vous parler de la vulnérabilité des aînés au Canada.

Au Centre antifraude du Canada, il y a aussi un programme qui a pour but d'aider les citoyens canadiens.

**Serg. Guy Paul Larocque:** Merci, monsieur Lynam.

Il est certain que les aînés forment une population que les fraudeurs semblent toujours viser. Ils sont souvent perçus comme des proies faciles.

Si je regarde nos données statistiques, les pertes associées aux personnes âgées — chez nous, ce sont celles de 60 ans et plus — représentent environ 30 % des pertes qui nous sont signalées sur une base annuelle. C'est quand même assez important.

Au Centre antifraude du Canada, un programme en place offre du soutien aux aînés. Lorsque c'est détecté par nos analystes à la réception des plaintes, les personnes plus vulnérables ou à risque sont redirigées vers l'Unité de support aux aînés du CAFC.

Il s'agit d'un programme assez particulier et assez spécial dans la mesure où nous avons des aînés bénévoles qui viennent nous aider à faire cette partie du travail. Ces personnes sont souvent à la retraite et viennent de l'industrie, soit du domaine des télécommunications, du secteur bancaire ou d'autres secteurs. Des enseignants à la retraite nous soutiennent aussi. Ces personnes assurent le suivi d'appels auprès des aînés. De plus, elles nous aident aussi à faire des présentations à des groupes cibles, souvent auprès des groupes d'aînés.

Notre programme est principalement centré en Ontario. Nous visons présentement à étendre ce programme d'est en ouest pour assurer une meilleure présence au Canada. L'Ontario est la province qui a le bassin de victimes le plus important étant donné qu'elle est la plus populeuse. À cet égard, nos efforts sont bien dirigés de ce côté.

Nous faisons d'autres efforts pour tenter de minimiser les répercussions de la fraude, que ce soit par nos campagnes de sensibilisation sur les médias sociaux ou par les nombreuses réponses médiatiques que nous recevons.

Par exemple, au cours de la dernière année, seulement au centre antifraude, nous avons reçu près de 400 demandes médiatiques. La communauté médiatique nous aide beaucoup à véhiculer notre message et à tenter de joindre le plus grand nombre de personnes vulnérables possible.

Le plus important, et c'est souvent le plus difficile, c'est d'encourager les victimes à reconnaître qu'elles sont victimes de fraude et à signaler leur cas aux autorités. Signaler la fraude demeure un élément clé. Notre but est de comprendre les stratagèmes qui ciblent les Canadiens et les Canadiennes afin de pouvoir ajuster nos messages en conséquence.

**M. Sébastien Lemire:** Ce que vous dites me semble important.

Vous dites qu'il est important que les victimes signalent les fraudes aux autorités pour que celles-ci comprennent mieux les stratagèmes. Vous avez aussi mentionné l'influence des médias dans tout cela.

C'est sûr que mes réflexes sont ceux d'un francophone. Si je reçois un appel en anglais, je me doute bien que cela peut être une fraude. Je peux raccrocher immédiatement.

Êtes-vous témoin de cas d'appels frauduleux en français? Sincèrement, j'ai l'impression que cela se passe beaucoup plus en anglais qu'en français. Qu'en est-il du côté francophone?

● (1130)

**Serg. Guy Paul Larocque:** En effet, la plupart des situations frauduleuses se font en anglais.

**M. Sébastien Lemire:** C'est en raison du fait que c'est international.

**Serg. Guy Paul Larocque:** Dans une approche de masse, on va cibler le plus grand nombre de personnes possible.

Cela dit, la fraude se fait aussi en français, par téléphone. Je n'ai pas l'information sur l'ampleur de la fraude et sur la quantité de signalements de fraude où l'interaction initiale est en français. Cependant, il existe beaucoup de stratagèmes frauduleux qui utilisent la langue française. C'est certain que cela démontre le modèle adaptatif des fraudeurs. Ces derniers vont s'ajuster à leur « clientèle », si je peux m'exprimer ainsi, ou à leur public cible, dans le but de maximiser leurs profits.

**M. Sébastien Lemire:** On dit souvent que ce sont des proches des aînés qui les fraudent. Parfois, ils peuvent même fonctionner par téléphone en se faisant passer pour une compagnie ou autre.

Ce stratagème est-il utilisé par des proches pour frauder leurs propres aînés?

**Serg. Guy Paul Larocque:** Je n'ai pas d'information précise à ce sujet. Il existe un stratagème qu'on voit et qui circule encore beaucoup ces temps-ci, c'est ce qu'on appelle « l'arnaque des grands-parents ».

Des fraudeurs se font passer pour un proche de la famille qui est dans le pétrin. Il a soit été arrêté, soit eu un accident ou soit besoin de fonds d'urgence. Vous verrez que ces différents stratagèmes comportent toujours le même genre de dynamique. Il y a souvent une situation d'urgence. On veut que les personnes agissent de façon rapide.

Dans l'arnaque des grands-parents, c'est souvent le cas. Le fraudeur se fait passer pour un proche qui a besoin d'aide — ce peut-être un petit-fils ou une petite-fille —, et qui est pris à l'extérieur, dans une autre province ou dans une autre communauté. On amplifie ainsi le facteur d'urgence et on tente de faire réagir la victime afin qu'elle cède à la pression et qu'elle envoie des fonds au fraudeur.

**M. Sébastien Lemire:** Nous avons eu la chance de faire une étude sur le sujet, il y a deux ans, à l'initiative de mon collègue M. Masse, et nous revenons sur le sujet.

Avez-vous l'impression que, depuis deux ans, la question des appels frauduleux est traitée avec plus de sérieux et que les recommandations découlant de la première étude vous ont donné des ressources supplémentaires?

**Serg. Guy Paul Larocque:** Pour ce qui est des ressources, de notre côté, il y a certainement eu des investissements dans la lutte contre la cybercriminalité. Notre directeur général peut vous parler davantage des avancées concernant le Groupe national de coordination contre la cybercriminalité.

[*Traduction*]

Monsieur Lynam, avez-vous quelque chose à ajouter?

**M. Chris Lynam:** Oui.

Dans les dernières années, nous avons investi pour favoriser la collaboration entre le Groupe national de coordination contre la cybercriminalité et le CAFC. C'est important car, comme je l'ai dit, la cybernétisation est importante et les crimes peuvent être commis en ligne et au téléphone. Une escroquerie fréquente ces derniers temps consiste à solliciter un clic ou à attirer l'attention sur quelque chose et à inviter la victime à donner son numéro de téléphone ou d'autres renseignements. On rappelle la victime pour la piéger encore plus dans un stratagème frauduleux d'investissement, ou pour la convaincre, en temps réel, d'autoriser l'accès d'une entreprise à son système. Les escrocs ont mis le pied dans la porte.

Il y a donc eu passablement d'argent investi pour soutenir le GNC3 au sein de la GRC et d'autres groupes d'enquête sur la cybercriminalité afin de favoriser une approche plus globale du problème.

[*Français*]

**M. Sébastien Lemire:** Je vous remercie.

**Le président:** Merci, monsieur Lemire.

Je vais maintenant céder la parole à Mme Gray pour cinq minutes.

[*Traduction*]

**Mme Tracy Gray (Kelowna—Lake Country, PCC):** Merci, monsieur le président.

Je remercie les témoins de leur présence. Merci de votre travail.

Je vais poser des questions qui concernent un type de fraude qui n'a pas été abordé jusqu'ici, soit l'échange de carte SIM et le portage des numéros de téléphone. Ce type de fraudes a été qualifié de préoccupant quand le Comité s'est penché sur cette question en 2020.

Selon un rapport soumis en septembre 2021, le CRTC aurait enregistré près de 25 000 fraudes liées au portage et à l'échange de carte SIM entre août 2019 et mai 2020. Je me demandais si la GRC a des statistiques sur le nombre de signalements d'incidents criminels de ce genre, de même que sur le nombre d'arrestations, d'enquêtes et autres éléments liés de 2019 à maintenant.

**Serg. Guy Paul Larocque:** Merci.

Je n'ai pas de chiffres précis sur les échanges de carte SIM, mais je sais que le Centre reçoit peu de signalements à ce sujet. Il peut toutefois y avoir un lien direct avec les usurpations d'identité et, si nous établissons ce lien, alors je peux vous affirmer que les vols d'identité signalés sont en forte croissance depuis deux ou trois ans.

Pour notre part, donc, nous avons constaté que les fraudes par échange de carte SIM ont diminué après la mise en place de mesures par l'industrie. Il est beaucoup plus difficile maintenant de prendre la carte SIM de votre téléphone et de l'installer dans un autre appareil parce que les étapes de contrôle sont plus nombreuses.

● (1135)

**M. Chris Lynam:** J'aurais une petite remarque au sujet des fraudes par échange de carte SIM et d'autres types.

Vous avez sans doute remarqué que pour beaucoup d'applications, il faut maintenant passer par les étapes de l'authentification multifacteur. Pour ouvrir une session dans l'application d'une banque ou d'un autre organisme, le mot de passe ne suffit plus. Il faut donner d'autres renseignements comme un code reçu par texto. Les résultats sont impressionnants. C'est un mécanisme très efficace pour empêcher les fraudeurs ou les cybercriminels de nous escroquer ou d'accéder à notre système.

Le déploiement de ce mécanisme dans différents secteurs a vraiment contribué à réduire ces incidents.

**Mme Tracy Gray:** Très bien. Je vous remercie.

Avez-vous bien dit qu'il se pouvait que certains de ces chiffres aient été regroupés ensemble dans le signalement de fraudes en général et qu'ils ne soient peut-être pas autant séparés qu'avant? Est-ce que c'est ce que vous dites, potentiellement?

**Serg. Guy Paul Larocque:** C'est parce que nous ne suivons pas une catégorie particulière d'échanges de cartes SIM. Généralement, quand on nous signale un échange de carte, on le classe dans une sous-catégorie, c'est-à-dire la fraude liée à l'identité ou l'usurpation d'identité, parce que nous suivons les deux.

Au cours des deux dernières années, comme je le mentionnais, nous avons assisté à une forte augmentation de ces activités, mais la principale raison en est que des fraudeurs ont utilisé l'identité de beaucoup de Canadiens pour obtenir une aide financière. Avec ce phénomène, nous avons vu une augmentation des signalements de fraudes à l'identité.

Comme je le mentionnais à propos de l'échange de cartes SIM même, je n'ai pas de chiffres précis à ce sujet. Il m'est donc difficile de vous donner un nombre exact quand je n'ai pas ce genre de données.

**Mme Tracy Gray:** D'accord. Je vous remercie.

Avez-vous des chiffres — et vous ne les avez peut-être pas ici aujourd'hui, mais c'est quelque chose que vous pourriez fournir — en ce qui concerne les signalements que vous recevez ainsi que les enquêtes et les arrestations? Évidemment, le CRTC publie des rapports, mais vous menez vos propres enquêtes. Est-ce que vous pouvez fournir ce genre de données au comité pour que nous les incluions dans ce rapport?

**M. Chris Lynam:** Voulez-vous dire sur les enquêtes concernant les échanges de cartes SIM précisément ou...?

**Mme Tracy Gray:** Par exemple, mais il semble qu'il ne soit peut-être pas possible de séparer les données. Ce sont donc les données sur la fraude en général. Ce serait utile pour cette étude d'avoir vos données. Si vous avez des chiffres, ce serait utile.

**M. Chris Lynam:** Nous allons vérifier.

J'ajouterai que, comme les gens le savent, la GRC n'est pas le service de police compétent dans toutes les régions du Canada. Les données ne dresseront donc peut-être pas un tableau complet de ce qui se passe au niveau municipal ou provincial lorsque la GRC n'est pas le service de police compétent.

**Mme Tracy Gray:** C'est parfait. Je vous remercie.

Vous avez également mentionné qu'il est vraiment important, sans même parler des arnaques liées à l'échange de carte SIM et au transfert de numéros de téléphone, que les Canadiens prennent conscience d'autres types de fraude. Est-ce que la GRC mène activement une campagne d'information, en particulier ce mois-ci? Menez-vous une campagne en ce moment même?

**M. Chris Lynam:** Oui, à l'occasion du Mois de la sensibilisation à la cybersécurité, une initiative pangouvernementale est en cours. À bien des égards, la partie liée à la cybersécurité est menée par le Centre canadien pour la cybersécurité. Il s'agit d'une initiative qui faisait partie de la nouvelle Stratégie nationale de cybersécurité publiée en 2018.

Ainsi, comme je le mentionnais, ce mois-ci, nous expliquons comment ne pas être victime d'hameçonnage. Nous nous concentrons uniquement sur l'hameçonnage. Nous soutenons tous deux des activités. Nous aidons le Centre canadien pour la cybersécurité à ce sujet dans le cadre de sa campagne « Pensez cybersécurité ».

Comme je le mentionnais dans mes observations, nous avons fait du mois de mars le Mois de la prévention de la fraude, qui est un événement important. L'an dernier, je crois que nous avons enregistré au cours de ce mois plus de 300 000 visites sur le site Web du Centre antifraude du Canada, le CAC, et nous pensons avoir touché quelque 700 000 personnes par les médias sociaux. Cela montre qu'en concevant le...

**Mme Tracy Gray:** Puis-je poser juste une autre petite question? Je sais que nous n'avons plus de temps. Je suis désolée de vous interrompre.

**M. Chris Lynam:** Certainement.

**Mme Tracy Gray:** Ces communications se font-elles aussi dans d'autres langues? Nous savons que les communautés culturelles et les néo-Canadiens en particulier risquent d'être victimes de fraude. La sensibilisation se fait-elle aussi dans d'autres communautés culturelles dans d'autres langues?

**M. Chris Lynam:** C'est un bon point. La majorité de ces communications sont dans les deux langues officielles du Canada, mais je reconnais qu'il faut trouver un moyen de sensibiliser davantage les néo-Canadiens ou les personnes qui ne parlent ni anglais ni français. À différents niveaux ou, dans certains cas, le secteur à but non lucratif ou les ONG font pas mal de travail dans ce domaine, mais il y a certainement plus à faire.

● (1140)

**Le président:** Je vous remercie.

[*Français*]

Je cède maintenant la parole à Mme Lapointe pour cinq minutes.

[*Traduction*]

**Mme Viviane Lapointe (Sudbury, Lib.):** J'aimerais revenir aux questions que mes collègues, Mme Gray et M. Lemire, ont posées à propos de la sensibilisation. Ce qui m'intéresse tout particulièrement, c'est de savoir comment aider des populations vulnérables, comme les aînés.

Vous avez parlé de ce qui se passe quand des plaintes sont déposées, mais comment pouvons-nous faire de la prévention en amont pour ces populations vulnérables? Vous avez parlé de campagnes avec 300 000 visites sur un site Web et des médias sociaux, mais bon nombre de nos aînés n'ont pas de téléphone intelligent et ne savent pas forcément se servir d'un ordinateur. Que pouvons-nous faire, par exemple, pour aider ces populations vulnérables?

**M. Chris Lynam:** Je répondrai en premier, puis je céderai la parole au sergent Larocque qui parlera un peu plus du programme de soutien aux aînés.

Je suis d'accord. À l'heure actuelle, en matière de programme de prévention et de sensibilisation, nous essayons notamment d'adapter l'approche aux différents publics, afin de déterminer ce qui leur parle et ce dont ils ont besoin pour se protéger en ligne ou pour ne pas être victimes d'une arnaque téléphonique.

Vous avez raison quand vous dites que les aînés préféreraient sans doute recevoir des dépliants ou des brochures. Nous avons produit des brochures dans le passé et utilisé d'autres formules, comme les rencontres ou les réunions en personne pour promouvoir la sécurité en ligne. La COVID a beaucoup compliqué la tâche pendant deux ou trois ans, mais nous avons repris le collier dans ce domaine.

Je vais laisser le sergent Larocque parler un peu plus du programme de soutien aux aînés et des activités de sensibilisation qui existent.

**Serg. Guy Paul Larocque:** Pour ce qui est de la sensibilisation, nous avons des exposés proactifs qui sont présentés en personne, dans la mesure du possible. Évidemment, comme l'a expliqué M. Lynam, la COVID a mis un frein à nos efforts, mais nous avons quand même trouvé des moyens de communiquer. Nous avons eu des exposés virtuels quand il n'était pas possible de les présenter en personne. Nos aînés bénévoles ont maintenant commencé les rendez-vous en personne.

Pas plus tard que la semaine dernière ou celle d'avant, un de mes agents de communications a présenté un exposé devant de nouveaux arrivants. C'était vraiment bien de pouvoir les familiariser avec toutes les menaces frauduleuses qui existent et de les aider à les contrer.

Je reconnais que la prévention restera essentielle. Nous ne ferons jamais assez de prévention. Nous pouvons toujours faire plus, et ce sera toujours un défi de réussir à communiquer avec le plus de personnes possible.

Au centre, nous avons notamment repris le mot-clic #ParlerA2. L'idée est que si vous parlez à deux personnes d'une histoire de fraude ou d'une menace de fraude et qu'elles en parlent à deux autres, le message sera diffusé plus largement.

Vous avez mentionné les aînés victimes de fraude, qui peuvent être plus vulnérables et avec qui il peut être plus difficile de communiquer. C'est pourquoi nous demandons à leur famille de nous aider à faire de la sensibilisation et à avoir ces conversations avec eux.

**Mme Viviane Lapointe:** Monsieur Lynam, vous nous avez dit ce matin — et le CRTC nous a dit la même chose la semaine dernière — que seulement 10 à 15 % des victimes d'appels frauduleux font un signalement.

La question que je me pose est la suivante: comment les législateurs peuvent-ils aider à faire en sorte qu'il y ait plus de signalements? À l'heure actuelle, il faut contacter le CRTC et remplir un formulaire, ce qui est très contraignant pour les victimes.

Et s'il y avait un système automatisé national que toutes les entreprises de télécommunications seraient obligées de mettre en œuvre et avec lequel il suffirait d'utiliser un code comme *555 pour mettre fin immédiatement à l'appel frauduleux et le bloquer? Cet appel serait signalé aussitôt et cela aiderait à retracer tous ces appels.

Ce genre de système a-t-il été envisagé?

**M. Chris Lynam:** Je n'ai pas connaissance d'une solution comme celle-là. Je pense qu'il nous faut plus d'idées pour qu'il soit plus facile pour les victimes de signaler la fraude. Le Groupe national de coordination contre la cybercriminalité, le GNC3, a notamment pour mandat de travailler avec le Centre antifraude du Canada, le CAFC, pour y parvenir.

Par exemple, nous créons et mettons en place un nouveau système en ligne appelé système de signalement des incidents de cybercriminalité et de fraude. Nous nous y sommes attelés et nous sommes tout de suite revenus aux principes de base. Nous sommes allés parler avec des aînés pour leur demander s'ils devaient signaler quelque chose en ligne, quels termes leur parleraient le plus et comment nous pourrions leur faciliter la tâche. Nous avons revu notre approche pour tenir compte de leurs réponses. Nous sommes en train de mettre en place le système. Nous en sommes actuellement à la version bêta. Nous avons environ 25 victimes par jour et nous travaillons constamment sur le système pour le rendre plus convivial.

Ce n'est qu'un exemple. Nous devons faire en sorte qu'il soit plus simple de signaler les incidents de fraude et étudier d'autres moyens d'aider les Canadiens à les signaler. Cette information alimente l'écosystème qui peut ensuite aider les enquêtes ou permettre d'intensifier les efforts de prévention.

● (1145)

**Le président:** Je vous remercie.

La parole est maintenant à M. Lemire.

[*Français*]

Monsieur Lemire, vous disposez de deux minutes et trente secondes.

**M. Sébastien Lemire:** Le dernier rapport que nous avons adopté contenait trois recommandations qui pouvaient vous concerner.

D'abord, la Recommandation 1 parlait des données:

> Que le gouvernement du Canada travaille avec le Centre antifraude du Canada, Statistique Canada, les gouvernements provinciaux et les services policiers chargés de l'application des lois de partout au pays pour améliorer la disponibilité et l'accessibilité des données sur les appels frauduleux au Canada.

La Recommandation 2 parlait des données et de l'information:

> Que le gouvernement du Canada travaille avec le Conseil de la radiodiffusion et des télécommunications canadiennes, les fournisseurs de services de télécommunications et les services de police dans le but d'augmenter et d'améliorer l'information mise à la disposition des Canadiens concernant les appels frauduleux.

Finalement, il y avait la Recommandation 5:

> Que le gouvernement du Canada présente un projet de loi pour faciliter l'échange d'informations confidentielles entre la Gendarmerie royale du Canada, le Conseil de la radiodiffusion et des télécommunications canadiennes et d'autres instances gouvernementales au pays, afin d'assurer la coordination d'interventions efficaces contre les appels frauduleux tout en garantissant la protection de la vie privée.

Il était donc question du partage de données, de l'information et, particulièrement, de l'échange d'informations confidentielles.

Le gouvernement vous a-t-il sollicités, depuis deux ans, pour améliorer les pratiques? A-t-il assumé un rôle de direction? Finalement, ces recommandations ont-elles été mises en place?

[*Traduction*]

**M. Chris Lynam:** Ce sont trois bonnes recommandations.

Pour ce qui est de la première, beaucoup a été fait pour communiquer plus de données et d'information sur la fraude. Nous allons très bientôt publier un rapport sur les activités annuelles du CAFC qui contiendra beaucoup d'autres données sur la fraude et le reste. Il devrait être publié dans peu de temps.

Nous réfléchissons continuellement à des mécanismes d'échange d'informations avec d'autres organismes, etc. Nous avons parlé tout à l'heure de collaborer avec le CRTC à ce propos. Je dirai que nous avons progressé dans notre façon de travailler avec les autres organismes, mais qu'il reste encore beaucoup à faire.

Je vais céder la parole au sergent Larocque qui vous parlera de notre approche de données ouvertes au CAFC.

**Serg. Guy Paul Larocque:** Il y a de récents développements sur ce front. Nous voulons publier plus de données et les rendre plus accessibles au public. Nous travaillons donc en ce moment avec une de nos unités à la GRC afin de publier ce type de données en utilisant le concept des données gouvernementales ouvertes. Par exemple, nous publions certains rapports à des fins de prévention, comme les bulletins, entre autres. Ce sera le type de rapports que nous chercherons à télécharger sur ce portail, ainsi que des données à venir sur les incidents de fraude.

Même pour le secteur universitaire, par exemple, s'il souhaite faire de la recherche, les données seront beaucoup plus accessibles parce que certaines données sur les tendances deviendront disponibles prochainement, nous l'espérons.

Bien entendu, les données seront anonymisées pour protéger les renseignements concernant les victimes et les suspects, mais les données suffiront quand même pour voir certaines tendances. Comme le mentionnait M. Lynam, le rapport annuel fournira aussi de bonnes données contextuelles.

[*Français*]

**M. Sébastien Lemire:** Je vous remercie.

**Le président:** Merci, monsieur Larocque.

Merci, monsieur Lemire.

Je vais maintenant donner la parole à M. Masse pour deux minutes et demie.

[*Traduction*]

**M. Brian Masse:** Je vous remercie, monsieur le président.

La prévention est essentielle à bien des égards. M. Mecher va témoigner. Il était enquêteur à la GRC dans des affaires de fraude. Il a travaillé sur le dossier de la Western Union. Il a fait un travail formidable et il témoignera devant le comité.

Nous avons envoyé un courriel aux députés pour qu'on en parle. Une dizaine d'autres députés ont répondu. Nous l'avons envoyé deux fois. Il est toujours difficile d'en faire une priorité.

En 2018, le ministre de la Sécurité publique de l'époque, Ralph Goodale, a organisé un sommet ici, à Ottawa, sur les armes à feu, les drogues, la contrebande, etc. Dites-moi sincèrement, pensez-vous qu'un sommet soit une bonne ou une mauvaise idée? En sommes-nous à un point où nous avons besoin d'un sommet sur la fraude ou quelque chose comme cela pour réunir les élus provinciaux, municipaux, fédéraux et autres afin d'avoir quelque chose de plus solide pour les relations publiques?

Je ne veux pas de réunions pour le plaisir d'en tenir, loin de là. J'en ai assez comme cela. Ce qui m'a plu dans le sommet organisé par M. Goodale, c'est qu'il a réuni beaucoup de personnes qui n'avaient pas travaillé ensemble auparavant. Les aspects formels et informels sont venus après.

Étant donné votre temps et l'engagement que cela représente, serait-il utile pour le pays d'organiser maintenant un sommet sur la fraude et la cybersécurité?

Vous ne m'insulterez pas si vous répondez seulement par un non.

● (1150)

**M. Chris Lynam:** Je pense que l'idée de réunir les intervenants de différentes manières — que ce soit un sommet ou un autre type d'activité — pour parler des conséquences et trouver des solutions serait très bien accueillie.

Par exemple, il y a déjà beaucoup d'activités, avec le gouvernement qui a demandé dernièrement des consultations pour le renouvellement de la Stratégie nationale de cybersécurité. C'était un moyen à la fois de solliciter des commentaires en ligne et de rencontrer différents intervenants.

Nous parlons de lutter contre la cybercriminalité et la fraude en équipe, comme dans un sport. Cela fait intervenir les organismes d'application de la loi, d'autres organismes gouvernementaux et les secteurs public et privé. Je vais souvent à des conférences ou à des rencontres dont c'est le thème, et les personnes présentes sont déterminées à trouver des solutions pour réduire le nombre de victimes.

Je pense que des rencontres ou des activités réunissant ces intervenants pour dire, « Voici ce que je vois et voici les solutions que je vous propose », seraient bénéfiques.

**Le président:** Je vous remercie.

Monsieur Masse, allez-y si vous voulez, mais soyez bref.

**M. Brian Masse:** Je vous remercie, monsieur le président. Je vais poursuivre avec M. Larocque.

Vous avez parlé de distribuer à la population des documents multilingues, par exemple en arabe et dans d'autres langues. Est-ce que c'est juste une question de ressources? Est-ce qu'une bonne traduction coûte cher? Je le sais par expérience dans ma circonscription, etc. Est-ce le cas?

**Serg. Guy Paul Larocque:** C'est le cas.

Je précise que cela se fait, dans une certaine mesure, dans les régions. Nous ne sommes pas les seuls à produire les documents de sensibilisation à la fraude. Par exemple, nous collaborons avec mes collègues en Colombie-Britannique. Ils ont placardé des affiches et distribué des brochures dans plusieurs langues pour alerter les citoyens au danger de l'utilisation des distributeurs de cryptomonnaies. L'information est donc traduite dans plusieurs langues dans certaines régions. Le travail est très régional, mais évidemment, il y a toujours des aspects que nous pourrions améliorer sur ce front.

**M. Chris Lynam:** Si je pouvais juste ajouter, rapidement...

**Le président:** Très rapidement.

**M. Chris Lynam:** Oui, la traduction est un des éléments, mais nous devons aussi adopter le point de vue holistique selon lequel, culturellement, ce n'est peut-être pas la question de la traduction. Quand on essaie de communiquer des renseignements aux néo-Canadiens, aux collectivités autochtones et à d'autres personnes dans ce genre de situation, et de les mobiliser, il faut trouver la bonne approche pour faire passer le message de prévention et se demander ce qui fait écho chez eux et comment ils veulent entendre et recevoir ces renseignements.

[*Français*]

**Le président:** Je vous remercie.

Je cède maintenant la parole à M. Généreux, pour cinq minutes.

**M. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, PCC):** Merci, monsieur le président.

Je remercie également les témoins.

Monsieur Lynam, plus tôt, vous avez utilisé les mots « défi omniprésent et durable ». Si j'ai bien compris, il s'agit d'un défi qui perdure. Entendons-nous bien: les technologies d'aujourd'hui font que ce défi va demeurer, inévitablement.

Sachant cela, quels sont vos objectifs?

Tantôt, vous avez mentionné que les pertes relatives aux fraudes s'élèvent à 379 millions de dollars et que la récupération s'élevait à 3,4 millions de dollars. Pouvons-nous associer ces deux chiffres? La récupération ne représente même pas 1 % des pertes.

Est-ce possible? Mon calcul est-il bon?

**Serg. Guy Paul Larocque:** Récupérer l'argent des fraudes va certainement toujours demeurer un défi, puisque le modèle des fraudeurs est très adaptatif. À partir du moment où l'on aura établi une barrière ou un moyen de protection, le fraudeur va certainement travailler fort pour contourner ces mesures. On le voit tous les jours: de nouvelles fraudes font surface et d'anciennes fraudes sont remises à la saveur du jour. La prévention demeure l'élément clé pour enrayer la fraude. Comme vous pouvez le constater, les sommes récupérées ou rendues aux victimes sont bien moindres, et de loin, que les pertes signalées.

En effet, lorsque l'argent est transféré à un fraudeur, ce dernier va le déplacer assez rapidement. Dans la majorité des situations, lorsqu'un transfert bancaire est fait, les fonds disparaissent vers d'autres comptes au cours de la même journée. La trace s'efface donc assez rapidement.

C'est la raison pour laquelle il faut que les gens comprennent que, lorsqu'ils font face à une demande frauduleuse, ils doivent prendre du recul, afin d'éviter de transférer de l'argent à des fraudeurs. Le temps joue en leur faveur. Malheureusement, lorsque le transfert est fait, la côte à remonter pour récupérer les fonds peut être très abrupte.

● (1155)

**M. Bernard Généreux:** Monsieur Larocque, vous avez dit plutôt que vous utilisiez des bénévoles, des gens qui travaillent dans les télécommunications, pour vous aider à mettre en place des façons d'améliorer vos types de recherche.

Utilisez-vous les services de pirates informatiques? Engagez-vous des gens qui ont déjà été actifs dans le Web clandestin et qui ont des connaissances technologiques avancées? Ces gens ont les compétences des fraudeurs, mais ils seraient là pour vous aider et pour éviter que cela se reproduise.

C'est une drôle de question, mais je pense que...

**Serg. Guy Paul Larocque:** En fait, c'est une très bonne question. Je vais laisser notre directeur y répondre, afin qu'il puisse aussi vous parler d'une de nos sous-unités en lien avec la cybercriminalité.

[*Traduction*]

**M. Chris Lynam:** Je dirai que nous n'utilisons pas de pirates informatiques ou de cybercriminels, mais curieusement, il y a de bons enseignements à tirer de leurs activités criminelles et de la façon dont ils les mènent, entre autres.

En tirant ces enseignements, il devient possible de renforcer nos systèmes ou de comprendre comment quelqu'un est entré dans un système afin d'adopter les méthodes de prévention voulues. En fait, il existe une industrie qui fait notamment des essais de pénétration, et c'est un service que proposent des entreprises. Elles vont essayer de pénétrer dans un réseau, et ces entreprises doivent généralement faire l'objet d'une réglementation très stricte.

Nous devons nous montrer prudents, mais nous avons des enseignements à tirer de la façon dont les pirates agissent. Nous voyons comment ils procèdent, puis nous essayons d'en tenir compte dans la façon dont nous protégeons et faisons le suivi.

[*Français*]

**M. Bernard Généreux:** Est-ce que je peux...

**Le président:** Monsieur Généreux, votre temps de parole est écoulé. Je vous remercie.

Monsieur Erskine-Smith, vous avez la parole pour quelques minutes.

[*Traduction*]

**M. Nathaniel Erskine-Smith (Beaches—East York, Lib.):** Je vous remercie.

Ma première question concerne certains chiffres sur le site Web du CAC. Les sommes semblent en voie d'égaler en 2022 celles de 2021, avec bien plus de 300 millions de dollars perdus pour l'instant, et en voie peut-être même de dépasser les chiffres de l'an dernier, mais le nombre de victimes de fraude semble beaucoup baisser. Comment l'expliquez-vous?

**Serg. Guy Paul Larocque:** La réponse est qu'en moyenne, les pertes pour les victimes ont augmenté. Il y a des tendances dans les placements frauduleux, surtout liés au secteur des cryptomonnaies, comme les bitcoins, et à toute utilisation de cryptomonnaies qui permet aux escrocs...

**M. Nathaniel Erskine-Smith:** Y a-t-il une explication, pas aux disparités, mais à la baisse du nombre de victimes?

**Serg. Guy Paul Larocque:** Oui. C'est parce que les pertes sont, en moyenne, plus élevées pour les victimes. Nous avons moins de victimes qui signalent des pertes beaucoup plus importantes. Cela peut expliquer pourquoi...

**M. Nathaniel Erskine-Smith:** Non, ma question ne porte pas sur la disparité. Je demande si nos mesures portent plus leurs fruits. Y a-t-il quelque chose, selon vous, qui montre que nous réussissons mieux, d'où la baisse du nombre de victimes dont nous sommes témoins?

**Serg. Guy Paul Larocque:** Non, je suis désolé. Je ne vois aucune corrélation particulière dans ce cas.

**M. Nathaniel Erskine-Smith:** D'accord.

[ *Difficultés techniques*] mesures, ont-elles porté leurs fruits?

**Serg. Guy Paul Larocque:** Pardon?

**M. Nathaniel Erskine-Smith:** [*Difficultés techniques*]

[*Français*]

**M. Sébastien Lemire:** Monsieur le président, j'invoque le Règlement.

Il y a un problème de son qui rend difficile le travail des interprètes, alors j'aimerais qu'on en tienne compte, s'il vous plaît.

[*Traduction*]

**M. Nathaniel Erskine-Smith:** [*Difficultés techniques*] Les mesures STIR/SHAKEN, les mesures mêmes qui faisaient partie de notre rapport de 2020 [*difficultés techniques*] qui sont venues ensuite, qu'ont-elles donné...

[*Français*]

**M. Sébastien Lemire:** Je suis désolé de vous interrompre, monsieur Erskine-Smith, mais les interprètes ne peuvent pas faire leur travail parce que la connexion Internet n'est pas assez bonne.

● (1200)

[*Traduction*]

**M. Brian Masse:** Je crois que vous demandiez si la mise en œuvre de la technologie STIR/SHAKEN a porté ses fruits. Est-ce bien cela, monsieur Erskine-Smith?

**M. Nathaniel Erskine-Smith:** C'est cela.

**Serg. Guy Paul Larocque:** Pour autant que je sache, la technologie STIR/SHAKEN n'est pas complètement mise en oeuvre. Il m'est donc difficile de dire si elle est efficace.

Cependant, nous avons remarqué, entre autres, en ce qui concerne la fraude amorcée au téléphone, c'est que les fraudeurs utilisent beaucoup de technologies de mystification pour vous faire croire que le numéro qui vous appelle est local, alors qu'il ne l'est pas.

Ce que cela nous dit, au Centre antifraude, c'est que c'est encore un exemple de la faculté d'adaptation des fraudeurs qui continuent de pouvoir joindre leurs victimes.

**Le vice-président (M. Michael Kram):** Je remercie tous les témoins présents aujourd'hui.

Nous venons de terminer la première heure de réunion. Nous allons la suspendre quelques minutes, le temps de permuter les groupes de témoins.

Je vous remercie tous infiniment.

● (1200)

_____(Pause)_____

● (1205)

**Le président:** Mes excuses, chers collègues. J'ai perdu ma connexion Internet vers la fin de la réunion. Je remercie donc notre vice-président, M. Kram, d'avoir pris le relais.

Nous reprenons pour la deuxième heure de réunion, et nous accueillons Randall Baran-Chong, Kevin Cosgrove et John Mecher. Je vous remercie d'être des nôtres cet après-midi.

Sans plus attendre, je cède la parole à M. Baran-Chong, qui dispose de cinq minutes pour son témoignage.

**M. Randall Baran-Chong (co-fondateur, Canadian SIM-swap Victims United, à titre personnel):** Bonjour. Je m'appelle Randall Baran-Chong et je suis le cofondateur de Canadian SIM-swap Victims United.

Je remercie le comité de m'avoir invité à comparaître de nouveau devant lui. La dernière fois, le confinement a été annoncé l'après-midi même. J'espère donc que ma présence n'augurera pas l'arrivée d'une autre pandémie.

Pour vous rafraîchir la mémoire, la transférabilité des numéros, autorisée à partir de 2007, visait à permettre aux clients de changer de fournisseurs de services de télécommunications tout en conservant leur numéro de téléphone, mais des fraudeurs exploitent cette possibilité pour se transférer la propriété d'un numéro de téléphone, souvent en manipulant le représentant du service à la clientèle d'une entreprise de télécommunications.

Une fois en possession de votre numéro de téléphone, ils utilisent des méthodes d'authentification par message texte et SMS et cliquent sur « Mot de passe oublié » pour accéder aux comptes de la victime et en prendre le contrôle. Quand on y pense, cela peut aller de votre courriel aux portefeuilles de cryptomonnaies, en passant par les services bancaires et le stockage infonuagique. Dans notre organisation, qui compte plus de 20 défenseurs des victimes, nous avons des personnes qui ont été dépossédées de toutes leurs données et à qui on a volé des centaines de milliers de dollars. Pour ma part, j'ai vu mon moyen de subsistance menacé par une extorsion.

Que s'est-il passé depuis cette dernière réunion fortuite? Dans son rapport de novembre 2020, le comité — qui compte de nouveaux visages aujourd'hui — formulait deux principales recommandations, que je paraphrase. L'une était qu'une audience soit organisée et, à défaut, qu'une mesure législative soit proposée.

Le ministre a répondu en disant que nous faisons confiance au CRTC et au Conseil de la transférabilité des numéros sans fil, qui est composé des entreprises de télécommunications elles-mêmes, pour gérer la situation et s'autoréglementer et qu'une mesure législative est inutile, car le transfert non autorisé est considéré comme un crime.

Je peux parler pour presque toutes les victimes dans notre groupe en disant que notre problème, ce n'est pas la répression de la criminalité ou les criminels eux-mêmes. En revanche, nous nous méfions des entreprises de télécommunications et de leur organisme de réglementation. Ce sera probablement une première dans ces lieux, mais je vais paraphraser le rapper Ice-T et dire que nous ne détestons pas le joueur, mais le jeu.

Ce que je veux dire par là, c'est que nous savons que les criminels chercheront toujours les points faibles à exploiter, mais que c'est au système, aux entreprises de télécommunications que nous confions la protection de nos données personnelles, et elles calculent ce que cela coûte de prévenir les fraudes en comparaison du coût proche de zéro des sanctions en cas d'échec, et l'organisme de réglementation qui a pour rôle de protéger le public nous laisse tomber. En fait, jusqu'ici, les entreprises comme l'organisme de réglementation se préoccupent peu des victimes, ne compatissent pas à leur sort et les ignorent.

Depuis notre dernière réunion, voici ce qui a été révélé: la fraude est plus fréquente qu'on ne le pensait.

Mme Gray y a fait allusion. Une demande d'accès à l'information présentée par un journaliste de Globe Telecom — qui, ironie du sort, a fini par être victime d'une fraude liée à un échange de carte SIM — a révélé 24 627 cas, pour être exact, de transferts non autorisés sur les 10 mois allant d'août 2019 à mai 2020. Cela correspond à 1 % des transferts.

Si nous comparons avec les fraudes à la carte de crédit, seulement 0,17 % des transactions sont frauduleuses. Au plus fort de la fraude, 2,5 % des transferts étaient frauduleux. Son ampleur peut être massive. Des accusations ont été portées contre deux Canadiens, un à Montréal et un à Hamilton. Il leur est reproché d'avoir volé entre 40 et 50 millions de dollars en cryptomonnaies et par des fraudes à la carte de crédit au Canada et aux États-Unis.

Pendant ce temps, d'autres victimes dans nos groupes essaient de récupérer des millions en fonds volés parce que les représentants du service à la clientèle des entreprises de télécommunications donnent des renseignements personnels aux fraudeurs, ce qui leur permet de procéder au transfert non autorisé de numéro.

Enfin, les entreprises de télécommunications ont appliqué volontairement la réglementation, sans succès au début. Après plusieurs tentatives infructueuses pour régler le problème, elles ont mis en place des notifications par texte vers l'été 2020. Solution qui ne donne toujours rien. Nous le savons à cause des victimes découvertes après. Il y a un groupe de 14 victimes dont nous savons qu'elles essayaient de récupérer plusieurs millions de dollars en 2021. Les entreprises de télécommunications n'ont pas réussi à empêcher l'exploitation de leurs représentants et elles n'envoient pas toujours de notification.

Le fait est que nos identités numériques et nos numéros de téléphone sont de plus en plus exposés. Votre SIM est le nouveau numéro NAS — cela jusqu'à ce que l'authentification à deux facteurs par SMS soit remplacée systématiquement.

Le deuxième point est que la sécurité de notre identité numérique dépend de la résistance du maillon le plus faible et, dans ce cas, les représentants des services à la clientèle des entreprises de télécommunications sont le maillon le plus faible de la ligne de défense de nos numéros de téléphone.

Des enquêtes ont révélé que les conversations téléphoniques et les journaux de clavardage des représentants des services à la clientèle font l'objet d'une ingénierie sociale qui incite à fournir des renseignements aux fraudeurs. Cela en dit long sur le manque de formation, les incitatifs inappropriés qui font passer le rendement avant la protection des clients, et l'absence de mesures punitives pour les entreprises de télécommunications elles-mêmes en cas de manquement.

● (1210)

Enfin, les progrès et les pratiques en ce qui concerne les transferts non autorisés demeurent opaques. Le fait que nous n'ayons pas pu produire de chiffres et qu'il soit seulement possible d'en produire en présentant des demandes d'accès à l'information en dit long à ce sujet. Il n'y a pas de communication proactive de données sur les taux de pratique et sur leur efficacité.

Une audience est nécessaire pour mieux comprendre la situation et les ripostes et pour permettre aux victimes de s'exprimer. Deuxièmement, nous devons codifier des règles qui rendent les pratiques cohérentes et durables, y compris en ce qui concerne la transparence des paramètres. Troisièmement, nous devons adopter des mécanismes d'application en cas de non-conformité, comme je le proposais en 2020 quand l'Australie a instauré des amendes pour non-conformité allant jusqu'à 250 000 dollars australiens.

Ces trois recommandations sont toutes approuvées par les plus de 12 500 Canadiens qui ont signé une pétition OpenMedia à cet effet.

N'attendons pas une autre pandémie pour agir contre ce type de fraude. Je répondrai volontiers à vos questions et suis ouvert à des solutions.

Je vous remercie.

**Le président:** Je vous remercie, monsieur Baran-Chong.

Je cède la parole à M. Cosgrove, qui dispose de cinq minutes.

**M. Kevin Cosgrove (éducateur à la sécurité numérique et conseiller civil, à titre personnel):** Bonjour à toutes et à tous.

Je remercie les membres du Comité de m'offrir cette occasion de parler aujourd'hui.

Je m'appelle Kevin Cosgrove. Je suis technicien de réseau, éducateur et je fais la promotion de la sécurité numérique dans le comté de Windsor-Essex, en Ontario. Je travaille dans le domaine des TI depuis près de 30 ans, mais à présent, je travaille plus avec de vraies personnes, par des contacts, dans toute notre collectivité. Je travaille avec les services de police sur la fraude numérique et j'éduque le public dans ce domaine.

Je donne des cours chaque semestre à des aînés plus précisément. Comme nous le savons, les aînés sont une cible importante de la fraude en ligne, numérique et téléphonique. D'après les statistiques que je reçois à ma petite échelle, près de 25 % des victimes sont des aînés. Chaque année, nous passons du temps avec la police locale à expliquer aux aînés comment éviter d'être victime de fraude.

Je sais que le Comité se concentre certainement sur des choses à un niveau plus élevé — qui concernent les entreprises de télécommunications et d'autres choses à l'échelle internationale —, mais je suis le gars en première ligne que la petite dame âgée vient trouver pour me raconter qu'elle est victime d'une arnaque, qu'elle a besoin de ce type d'aide et qui me demande qui elle devrait appeler.

Ma plus grande frustration en travaillant à l'échelle locale et en tant qu'éducateur qui se concentre tout particulièrement sur ces questions, c'est que l'information existe déjà et qu'elle est diffusée. La GRC, notamment, a une quantité phénoménale d'information. Quand je parle aux personnes qui suivent mes cours, cependant, aucune n'en a entendu parler. Ce n'est pas que la GRC ne fait pas un bon travail ou ne fait aucune activité de sensibilisation, mais quand je parle aux gens, ils ne sont pas au courant.

Comme le Comité le sait, la GRC a une publication fabuleuse intitulée *Le petit livre noir de la fraude*. C'est une merveilleuse publication, et elle existe depuis des années. Depuis près de 20 ans que je fais cela, je ne connais qu'une personne qui en a vu une copie papier. Voilà bien le problème, entre autres, avec certains de nos programmes. Une partie de l'information et de la sensibilisation faites par la GRC ne touche pas tout le monde.

Évidemment, il y a aussi parfois un décalage quand la GRC n'est pas la principale autorité dans un endroit et qu'elle s'en remet plus à la police locale pour s'en occuper. Celle-ci fait son propre travail. En fait, chaque petite région à qui nous avons affaire essaie de réinventer la roue, au lieu d'adopter une réponse concertée pour certains aspects.

Quand je donne des cours à des aînés et que je distribue de l'information dans la collectivité, je cherche en priorité à ce que ce soit accessible. Quand j'ai commencé, il y a près de 20 ans, j'ai remarqué que l'accent sur les détails et les définitions, par exemple, complique les choses pour le simple citoyen qui prend une brochure et essaie de la comprendre. Je ne dénigre pas une partie de l'information publiée, mais une femme de 84 ans n'a rien à faire des différences entre l'hameçonnage, l'hameçonnage par SMS, le harponnage et le harponnage de baleine. Peu lui importe ce genre de détails. Elle a besoin d'information pour être en sécurité sans lire un message d'intérêt public dans une brochure qui ne choisit pas la bonne solution pour éduquer le public.

Je suis tout à fait prêt à répondre à vos questions. Je pense que j'avais quelques questions pour la GRC quand j'étais assis derrière, mais il ne m'appartient pas de les poser.

Je vous remercie de m'avoir invité.

Il a été question tout à l'heure de STIR/SHAKEN et des progrès accomplis par rapport à cette technologie. Même si je suis un civil, je parle avec des analystes des renseignements criminels du CAFC et du groupe des crimes financiers à Windsor. D'après eux, les types d'appels que cible spécifiquement la technologie STIR/SHAKEN ont diminué. Les gens ne signalent plus qu'ils ont reçu des appels téléphoniques s'annonçant comme venant de Revenu Canada. Il leur arrive de voir le même appel téléphonique s'afficher avec un numéro d'interurbain, mais pour ce qui est des appels frauduleux s'affichant comme venant de la police ou de Revenu Canada, il y en a beaucoup moins, d'après ce qu'on m'a dit.

● (1215)

[*Français*]

**Le président:** Merci beaucoup, monsieur Cosgrove.

Je cède la parole à M. Mecher pour cinq minutes.

[*Traduction*]

**M. John Mecher (enquêteur de la GRC à la retraite, à titre personnel):** Bonjour. Je vous remercie, monsieur le président, mesdames et messieurs les membres du Comité.

Je m'appelle John Mecher — ce qui rime avec « teacher » — et j'ai été membre de la GRC pendant plus de 32 ans, dont 10 ans environ passés à enquêter sur des fraudes, surtout dans la région métropolitaine de Toronto. J'ai enquêté sur différentes fraudes, y compris la fameuse arnaque liée à l'Agence du revenu du Canada. Après avoir pris ma retraite en 2019, j'ai continué de travailler bénévolement pour sensibiliser à la fraude.

Bien que je sois prêt à discuter de nombreux aspects de la fraude, y compris des occasions manquées par le gouvernement et par les organisations, j'ai choisi de me concentrer sur un élément fondamental de la prévention de la fraude. Pour être précis, je parlerai de la différence entre « la sensibilisation à la fraude » et ce que j'appelle « la véritable sensibilisation à la fraude ».

Tout d'abord, il est toujours bon de rappeler les pertes, qui continuent d'augmenter d'année en année et qui atteignent actuellement un niveau record. D'après le Centre antifraude du Canada, l'an dernier, ces pertes se chiffraient à plus de 383 millions de dollars. Pire encore, ce montant, d'après le Centre antifraude du Canada, ne représente que 5 % des pertes réelles.

La fraude perpétrée au Canada rapporte plusieurs milliards de dollars à des fraudeurs du monde entier. Ces mêmes fraudeurs s'en prennent généralement à ce que j'appelle les victimes traditionnelles de la fraude, comme les aînés, les nouveaux arrivants, les réfugiés et les personnes ayant une déficience intellectuelle. Je peux donner plusieurs exemples flagrants de fraudeurs qui prennent pour cibles des membres de ces communautés, mais je vous rappelle que, si les circonstances s'y prêtent, pratiquement tout le monde peut se faire avoir.

Il faut aussi se rappeler que, souvent, les conséquences pour les victimes ne se limitent pas à une perte financière. Dans certains cas, les économies d'une vie disparaissent et il est rare qu'elles soient récupérées. Hélas, les victimes subissent des contrecoups émotionnels qui vont de l'embarras à la dépression et, dans des cas extrêmes, malheureusement, bien des victimes finissent par se suicider.

Dans le cas des fraudes téléphoniques, même si ces arnaques existent depuis des décennies, nous n'avons toujours pas mis en oeuvre de mesures qui fassent qu'il soit moins facile d'accéder à nos réseaux téléphoniques. Les statistiques du Centre antifraude du Canada le confirment, puisque le téléphone est et continue d'être la méthode préférée de sollicitation en vue d'une fraude.

En outre, en pensant à l'arnaque liée à l'ARC qui est arrivée au Canada en 2014, et aux variantes qui ont suivi, je ne suis toujours pas convaincu qu'il soit considéré comme urgent de créer un obstacle à l'exploitation de nos réseaux téléphoniques. Pour cela, nous devons aussi être conscients que nous ne pouvons pas nous reposer sur les services de police — certes nécessaires — ou sur les tribunaux pour vraiment dissuader les fraudeurs. Malheureusement, il ne nous reste pas beaucoup d'options pour protéger les communautés vulnérables face aux fraudes.

Cela dit, la sensibilisation à la fraude est la solution, et il faut l'employer. Cependant, elle doit l'être de manière utile, ciblée et constante, ce qui n'est pas toujours le cas. Si le statu quo en matière de sensibilisation à la fraude fonctionnait, nous ne verrions pas les pertes augmenter d'année en année. Par ailleurs, bien que nombre de gens au Canada fassent un travail remarquable sur ce front, nous devons faire beaucoup plus et nous devons le faire maintenant.

La sensibilisation à la fraude peut se faire sur des sites Web et dans les médias sociaux, mais si les victimes potentielles ne connaissent pas ces plateformes, il est vain de croire qu'une série de gazouillis ou de messages publiés en ligne peuvent sensibiliser à la fraude. À mon avis, la règle d'or d'une véritable sensibilisation à la fraude doit être de savoir communiquer le message aux personnes qui ont le plus besoin de l'entendre. Autrement, nous continuerons de voir augmenter le nombre de victimes.

Enfin, je suis disposé à travailler avec tout parlementaire en toute impartialité, comme je l'ai fait avec M. Masse sur le dossier de la Western Union, qui a été une occasion unique pour les victimes de la fraude de récupérer leur argent.

Je vous remercie.

● (1220)

**Le président:** Je vous remercie.

[*Français*]

Monsieur Deltell, vous disposez de six minutes.

**M. Gérard Deltell (Louis-Saint-Laurent, PCC):** Merci beaucoup, monsieur le président.

Messieurs, soyez les bienvenus à votre Chambre des communes.

[*Traduction*]

J'ai une question pour vous trois, mais j'aimerais d'abord m'arrêter sur certains points au sujet de la GRC avec M. Cosgrove.

Votre témoignage est très intéressant. Si vous rencontrez des agents de la GRC dans le coin, vous pouvez leur parler. Ils sont très ouverts d'esprit. Ne craignez rien.

Monsieur Cosgrove, vous avez souligné que la GRC a beaucoup d'outils, mais que, malheureusement, les citoyens ne le savent pas. Est-ce que cela veut dire qu'ils ne sont pas informés ou que la GRC cache des renseignements?

**M. Kevin Cosgrove:** À mon niveau, et juste du point de vue de l'éducation, je regarde ce que font le CAFC et la GRC, ainsi que leurs ressources, et les ressources sont excellentes. Je réécris parfois des choses pour mes cours ou j'utilise directement leurs documents. Il n'est pas nécessaire de réinventer la roue dans ce domaine. Je me contente de parler aux gens et beaucoup ne savent pas que ces ressources existent.

Je ne sais pas du tout pourquoi il n'y a pas assez d'information diffusée ou pourquoi il y a une séparation des compétences qui fait que le service de police local ou la GRC ne s'intéresse pas à ce qui se passe localement. Je n'en connais pas la raison exacte. La documentation existe. De votre côté, et du côté du Comité, vous vous intéressez aux données concrètes et aux chiffres. Cette information n'intéresse pas le simple citoyen.

Pour ce qui est de la prévention de la fraude, de la sensibilisation et de tout le reste, j'enseigne un programme spécial dans notre université locale. Il est destiné aux personnes à partir de 55 ans. Je donne ces cours chaque semestre depuis huit ans maintenant, et il y a toujours assez d'inscrits pour constituer une classe. Je présente aussi des exposés avec nos policiers. L'intérêt existe vraiment. Cela ne fait aucun doute. Des gens viennent me voir, et pas seulement moi, pour essayer de trouver des personnes pour leur remettre des brochures en mains propres, mais l'information est déjà disponible. On peut la trouver en ligne. On peut obtenir des brochures. On peut aller voir la police locale. Il existe un nombre illimité de façons d'éduquer les citoyens pour éviter ces problèmes, mais il semble y avoir un décalage. C'est pourquoi je cherche surtout, même en travaillant avec le député Brian Masse, à éduquer le public précisément.

Cela se passe bien. J'espère qu'au bout de quelques années, il y aura un grand trou sur la carte des signalements et des fraudes. C'est peut-être un peu optimiste, mais à mon avis, pour faire passer l'information, il n'y a pas besoin de STIR/SHAKEN. Il n'y a pas besoin de la police. Il n'y a pas besoin de la coopération de la police américaine. Si toutes les personnes à qui j'ai parlé jusqu'ici savent ce qu'est une arnaque, que ce soit par SMS, message texte, en ligne ou par appel téléphonique, elles peuvent déjà repérer la fraude. Aucune des autres méthodes n'est efficace.

● (1225)

**M. Gérard Deltell:** Monsieur Cosgrove, aucun représentant de la GRC n'est avec nous aujourd'hui, mais nous avons M. Mecher qui est un ancien agent de la GRC.

Monsieur Mecher, j'aimerais savoir ce que vous pensez lorsque vous entendez M. Cosgrove dire qu'il y a beaucoup d'information, mais que les gens n'en savent rien.

**M. John Mecher:** Cela revient en grande partie à ce dont je parlais, et je suis tout à fait d'accord avec lui. L'existence de l'information n'est pas le problème, le problème est de faire en sorte qu'elle soit accessible aux personnes qui en ont le plus besoin. Cela veut dire qu'il faut un environnement de communication adéquat.

Je tiens à répéter que beaucoup de gens font du bon travail. M. Cosgrove en est un bon exemple. Au plan national, j'ai l'impression que la GRC, et par extension le gouvernement fédéral, ne considèrent pas la sensibilisation à la fraude comme une priorité.

Pour être honnête, depuis que je travaille dans ce domaine, je n'ai vu aucun gouvernement fédéral faire de la fraude ou de la sensibilisation à la fraude une priorité. Ce n'est donc pas quelque chose d'unique. Ce qui est le plus urgent maintenant, c'est que nous constatons que les pertes ont complètement explosé par rapport à ce que nous observions il y a 10 ans.

**M. Gérard Deltell:** Il ne faut pas oublier que vous parlez uniquement du 5 % des pertes recensées. Des milliards de dollars sont perdus.

S'il me reste du temps, monsieur le président, j'aimerais poser une question à M. Baran-Chong.

Monsieur Baran-Chong, j'apprécie beaucoup vos commentaires. J'aimerais revenir à votre troisième recommandation. Je n'étais peut-être pas très au courant, mais vous parlez de ceux qui ne se conforment pas et de l'obligation de se conformer.

Pouvez-vous expliquer votre troisième recommandation?

**M. Randall Baran-Chong:** Je crois que ma troisième recommandation portait sur ce que la commission australienne des communications a fait. Cette organisation a mis en place un processus très semblable à celui que nous avons proposé en 2020 pour essentiellement exiger d'obtenir l'autorisation du client avant d'effectuer un portage. Chaque fois qu'une entreprise ne respectait pas cette obligation, elle pouvait se voir imposer une amende maximale de 250 000 $. L'une des entreprises de télécommunications australiennes a payé plus de 200 000 $ pour 15 cas de non-conformité. Les autorités n'ont pas exigé le montant maximum dans ces cas, mais c'est ce qui a été fait, et cette politique a permis de constater des réductions. Il y a donc un effet dissuasif.

● (1230)

**M. Gérard Deltell:** Ai-je assez de temps, monsieur Lightbound?

[*Français*]

**Le président:** Vous disposez de vingt secondes, monsieur Deltell.

[*Traduction*]

**M. Gérard Deltell:** Je vous remercie beaucoup.

[*Français*]

**Le président:** Je vous remercie.

Je donne la parole à M. Gaheer, pour six minutes.

[*Traduction*]

**M. Iqwinder Gaheer (Mississauga—Malton, Lib.):** Merci, monsieur le président.

Je remercie les témoins d'avoir pris le temps de venir nous rencontrer.

Monsieur Baran-Chong, vous vous êtes montré un peu critique envers les entreprises de télécommunications, et je le dis avec sarcasme, bien sûr. Vous dites qu'elles ne « compatissent pas » au sort des victimes, qu'elles ne sont d'aucune aide et qu'elles ont carrément failli à la tâche.

Quelles sont les occasions manquées? Que pourraient-elles faire pour mieux prévenir la fraude?

**M. Randall Baran-Chong:** Je suppose que c'est parce que cela me touche personnellement, car je suis moi-même une victime. Depuis, j'ai pu entendre l'enregistrement de la police du représentant au service à la clientèle qui prétendait être un employé de Rogers, qui a appelé le magasin Rogers et qui a en fait obtenu mes renseignements personnels. Il a été très facile d'obtenir l'information. Le fraudeur a prétendu être cet employé et a pu fournir un numéro de client et tout le reste. Je pense que cela révèle un problème plus large au sein des entreprises de télécommunications et sur la capacité de faire de l'ingénierie sociale et d'exploiter les gens.

Je crois qu'une partie du problème est que si vous pensez à un incitatif, je peux vous donner un résultat. Le problème, c'est que ces préposés au service à la clientèle — et j'ai de la sympathie pour eux — ne sont pas très bien payés et ne sont pas très bien formés. Une grande partie de leurs évaluations repose sur le nombre de clients auxquels ils répondent pendant leurs quarts de travail. En quoi cela serait-il satisfaisant? Leurs incitatifs sont plutôt de... Si quelqu'un veut faire le portage de son numéro, on le laisse faire. Ils ne veulent pas s'opposer. Ils ne veulent pas se demander s'il s'agit de la bonne personne, etc. Tant que les incitatifs feront qu'ils se concentrent sur le volume traité, les résultats opérationnels et d'autres aspects de ce genre, plutôt que sur la protection de la vie privée et des renseignements personnels des clients, je crois que le problème persistera.

En ce qui concerne la sensibilisation, la deuxième chose est, bien sûr, qu'il doit y avoir une sensibilisation plus générale à l'égard des bonnes pratiques. Laissons tomber l'authentification à deux facteurs par SMS. C'est quelque chose que la Federal Communications Commission des États-Unis encourage, car elle considère que l'échange de carte SIM avec authentification à deux facteurs par SMS est une menace à la sécurité nationale, mais il y a aussi la sensibilisation des entreprises. Par exemple, lorsque Rogers a fait sa première tentative infructueuse de notification par message texte, les clients ont cru que ces notifications étaient frauduleuses. Ils ont aussi pensé que c'était de pourriels, et les raisons pour lesquelles les clients ignoraient que les notifications visaient à les protéger, c'est que les pratiques de Rogers sont très obscures et qu'elles ne sont pas expliquées.

Il y a beaucoup de différentes possibilités, et plusieurs sont liées aux entreprises de télécommunications elles-mêmes.

**M. Iqwinder Gaheer:** Merci.

Vous critiquez aussi l'authentification à deux facteurs par SMS. Existe-t-il d'autres solutions, ou que recommanderiez-vous?

**M. Randall Baran-Chong:** Oui. Je suis plus critique à l'égard de l'authentification à deux facteurs par SMS, car la vulnérabilité est qu'après le vol du numéro, c'est le fraudeur qui reçoit le message texte. Par contre, il existe d'autres moyens, comme l'authentification à deux facteurs par une application. Vous avez peut-être entendu parler de Google Authenticator, qui est très couramment utilisé.

Le problème, c'est que Princeton a mené une étude sur 140 des sites Web les plus populaires. Dans plusieurs sites, le premier facteur d'authentification favorisé est l'authentification à deux facteurs par SMS. Nous devons nous éloigner de cela, surtout dans le cas des industries essentielles.

Je peux vous dire que certaines banques du Canada utilisent encore l'authentification à deux facteurs par SMS, et qu'il s'agit de leur seule méthode d'authentification à deux facteurs. Nous devons vraiment envisager d'abandonner cette méthode si cette vulnérabilité et cette méfiance à l'égard des entreprises de télécommunications persistent.

**M. Iqwinder Gaheer:** Dans votre témoignage, vous avez également dit qu'aucune donnée sur le nombre de cas n'avait été publiée. Cela m'étonne, car le CRTC ne devrait-il pas recueillir ces données?

**M. Randall Baran-Chong:** Oh, je suis certain qu'il recueille les données, mais qu'il ne veut tout simplement pas les partager. La seule façon dont cette personne — un journaliste spécialisé dans les télécommunications du *Globe and Mail*, ironiquement — a pu y avoir accès, c'est en présentant une demande d'accès à l'information.

Le Centre pour la défense de l'intérêt public, ou CDIP, a fait plusieurs demandes et le CRTC a répondu négativement en disant que ce n'est pas dans l'intérêt public ou que cela pourrait compromettre la sécurité des personnes et la sécurité dans les entreprises de télécommunications.

À mon avis, il s'agit d'un raisonnement absurde pour défendre les entreprises de télécommunications.

**M. Iqwinder Gaheer:** C'est excellent. Merci beaucoup.

**M. Randall Baran-Chong:** Merci.

[*Français*]

**Le président:** Je vous remercie, monsieur Gaheer.

Je donne maintenant la parole à M. Lemire pour six minutes.

● (1235)

**M. Sébastien Lemire:** Je vous remercie, monsieur le président.

Monsieur Cosgrove, vous étiez présent dans la salle quand des représentants de la GRC ont comparu. Nous avons posé des questions au sujet des aînés. Je l'ai fait, ma collègue Viviane Lapointe l'a fait, et peut-être d'autres députés aussi.

Avez-vous été satisfait des réponses que vous avez entendues?

[*Traduction*]

**M. Kevin Cosgrove:** Oui, j'ai été satisfait. J'ai eu des contacts avec eux au fil des ans dans le cadre de mes programmes locaux et de mes activités de sensibilisation. Ils ont communiqué avec moi.

En ce qui concerne le soutien supplémentaire ou la possibilité de considérer l'information de base dont nous disposions et de collaborer plus étroitement, non, ce n'est pas vraiment quelque chose que j'ai vécu, que ce soit parce que nous sommes à Windsor et juste mis de côté, ou parce que c'est notre service de police local qui s'en occupe. Je ne peux pas me prononcer sur cet aspect.

Il y a des moments, en faisant ce que je fais — travailler avec nos policiers locaux, faire de la sensibilisation et collaborer avec notre université — où j'ai vraiment l'impression de mettre en oeuvre un programme communautaire qui, après 10 ans, devrait être plus qu'un programme communautaire. Un soutien accru, peu importe l'orientation, serait certainement avantageux.

J'ai examiné leur documentation. Je n'ai certainement rien à redire à ce sujet. La documentation est bonne et suffisante. Elle est très étoffée, mais la question à laquelle nous cherchons probablement à répondre aujourd'hui est de savoir si la population en général en profite.

[*Français*]

**M. Sébastien Lemire:** Plusieurs de nos recommandations vont dans le sens d'une meilleure collaboration, une plus grande transparence, un partage des données, particulièrement avec l'industrie et les organismes gouvernementaux.

Avez-vous l'impression que cette collaboration est suffisamment mise en pratique actuellement? J'imagine que vous avez entendu également les réponses du CRTC, la semaine dernière.

J'aimerais surtout savoir ce que nous pourrions faire davantage, à ce stade-ci.

[*Traduction*]

**M. Kevin Cosgrove:** Il faut rendre l'information plus accessible. Comme je l'ai dit, les gens n'ont pas besoin de programmes ou d'information de niveau supérieur. L'information est très détaillée. On offre un dictionnaire aux personnes qui pourraient être victimes de fraude en espérant qu'elles le liront au complet plutôt que de simplement résumer ce qu'est réellement la fraude et d'expliquer comment l'éviter.

Pour la plupart des fraudes, peu importe qu'il s'agisse d'un message texte, d'un appel téléphonique ou d'un courriel, les mêmes types d'escroqueries sont utilisés. Cela peut être un courriel au sujet de la cryptomonnaie ou un appel téléphonique vous invitant à investir dans la cryptomonnaie. La méthode n'a pas d'importance.

Selon ce que j'ai vu, l'information se concentre beaucoup sur les méthodes utilisées, ce qui donne l'impression que les renseignements sont trop difficiles à comprendre. Je cherche à réduire l'information et à la simplifier. Il existe une publication dont la préparation a été financée par nos entreprises locales, la police de Windsor et quelques donateurs privés. Cette publication a été diffusée dans la collectivité et elle a reçu un accueil phénoménal. Il n'est pas question de prendre l'information de haut niveau et de voir ce que nous pouvons transmettre aux gens ou à quel point nous pouvons paraître intelligents; il s'agit de trouver comment nous pouvons utiliser cette information et la présenter aux gens de manière à ce qu'elle soit utile.

[*Français*]

**M. Sébastien Lemire:** Je vous remercie beaucoup.

Monsieur Baran-Chong, je pense que vous auriez beaucoup à dire sur ce sujet. Je vous pose donc la même question.

Quel est votre avis sur l'état actuel de l'industrie et, surtout, sur les recommandations pour nous assurer d'améliorer réellement la situation?

[*Traduction*]

**M. Randall Baran-Chong:** Merci.

Lorsque notre groupe a pris connaissance des recommandations figurant dans ce rapport, nous étions plutôt satisfaits, car je crois qu'elles reflétaient essentiellement ce que nous avions demandé concernant la tenue d'audiences. Dans sa réponse, le ministère a dit, je crois, qu'il ne jugeait pas approprié de tenir des audiences parce qu'il ne voulait pas obtenir l'opinion du public sur la façon dont les gens pouvaient se protéger; ce que j'ai trouvé un peu ridicule parce que la situation actuelle des entreprises de télécommunications repose sur une recommandation que nous avons faite en 2020. Cependant, parce qu'ils ont laissé traîner les choses ou qu'ils ne nous ont pas écoutés, les victimes se sont multipliées pendant ce temps.

Deuxièmement, le ministère ne comprend pas que la tenue d'audiences ne vise pas seulement, disons, à obtenir des recommandations ou autres choses du genre. Beaucoup de victimes ne se sentent pas écoutées. Vous vous souvenez peut-être que vous m'avez demandé en 2020 comment Rogers avait réagi à mon cas de fraude. Ils m'ont offert 100 $. Un de leurs représentants du service à la clientèle a communiqué mes renseignements personnels, et cela m'a fait perdre toutes mes données. Le fraudeur a menacé de ruiner ma vie, de briser ma carrière, à moins de lui donner 25 000 $. C'est ce qu'il m'a demandé, et Rogers m'a offert 100 $. C'était ses excuses.

D'autres personnes qui ont perdu des centaines de milliers de dollars ont préféré intenter des poursuites. Les entreprises ne coopèrent pas. Il faut des enquêtes criminelles pour révéler le désintéressement qui existe dans les pratiques des entreprises de télécommunications. C'est pourquoi nous continuons de croire que des audiences sont nécessaires pour avoir une transparence en ce qui concerne les chiffres. Quelles sont les pratiques? Quels sont les moyens et les différents modèles de victimisation?

Troisièmement, il faut normaliser ces pratiques. La Federal Communications Commission est également d'avis que ces pratiques ne sont ni cohérentes ni durables. Les entreprises peuvent choisir de ne pas le faire ou simplement de dire qu'il s'agit d'une simple erreur. Quatrièmement, nous avons besoin d'assurer le respect des obligations dans ce domaine, l'exemple australien montrant, selon nous, que cet aspect est essentiel pour assurer la conformité, etc.

Ce sont les trois ou quatre éléments auxquels nous tenons, et je crois que le Comité pensait de même la dernière fois.

● (1240)

[*Français*]

**M. Sébastien Lemire:** Je vous remercie de votre clarté et, surtout, de votre témoignage. Vous faites grandement avancer nos réflexions.

[*Traduction*]

**Le président:** Je vous remercie beaucoup, monsieur Baran-Chong.

Merci, monsieur Lemire.

Nous allons passer à M. Masse pour six minutes.

**M. Brian Masse:** Merci, monsieur le président.

Je vais poursuivre avec vous, monsieur Baran-Chong, en commençant par vous remercier. Vos efforts ont été tout simplement héroïques. Je pense à ce que vous avez vécu. Nous vous sommes très reconnaissants de nous en parler et de témoigner à nouveau aujourd'hui.

Nous avons reçu le CRTC vendredi, et je vous jure que j'ai failli me lancer dans une tirade à la Lewis Black devant les témoignages que nous avons entendus. Ce qui me préoccupe, c'est exactement ce que vous dites. J'envisage la tenue d'un sommet. C'est ce que je crois que cela doit être. Vous dites qu'il faut d'abord tenir des audiences — je pense que c'est le même genre d'exercice — qui nous permettraient d'obtenir, je pense, une reddition de comptes plus publique et aussi d'examiner ce que sont les attentes à l'égard de nos organismes intergouvernementaux, car lorsqu'ils siègent ici individuellement, il est difficile pour eux de critiquer et de faire des recommandations pour les autres. Peut-être que si nous avions une approche plus axée sur les gens... J'aimerais savoir ce que vous en pensez, puis je passerai à M. Cosgrove et à notre témoin sur les données relatives aux télécommunications.

Allez-y, je vous écoute.

**M. Randall Baran-Chong:** Oui, nous appuyons fortement cette idée. Peu importe la forme qu'elle prendra. Encore une fois, il s'agit de pouvoir se faire entendre. Parce que notre groupe est essentiellement communautaire, nous avons beaucoup appris en écoutant les différentes histoires des victimes. Je découvre des victimes en lisant des articles et je communique avec elles, ou elles viennent nous rencontrer pour nous parler des circonstances entourant ces problèmes.

Une approche publique peut aider les gens à comprendre comment la fraude elle-même se produit, ou les facteurs d'incertitude qui ouvrent la porte à la fraude, par exemple lorsque les gens reçoivent un message texte et qu'ils ne savent pas s'il s'agit d'une fraude ou non.

Deuxièmement, si vous pensez à la portabilité, c'est un jeu qui se joue à deux. Deux entreprises de télécommunications sont concernées, car il s'agit habituellement de laisser une entreprise pour passer à une autre, il doit donc y avoir des pratiques et des normes cohérentes dans l'ensemble de l'industrie.

Troisièmement, je pense qu'il faut intervenir beaucoup plus profondément dans les processus opérationnels relativement à ces vulnérabilités au sein des entreprises. Cela ne concerne pas seulement le Canada. C'est la même chose aux États-Unis et dans d'autres pays où des échanges de carte SIM se sont produits parce que des personnes en place, ou la capacité de faire de l'ingénierie sociale dans une organisation ouvre essentiellement la chasse aux données. Je suis d'accord avec votre idée.

**M. Brian Masse:** Je vais passer à M. Mecher et à M. Cosgrove. Je vais peut-être commencer par M. Cosgrove, puisqu'il est juste à côté de moi.

Je vous remercie, vous et M. Mecher, de vos efforts. J'ai eu du plaisir à travailler avec vous de bien des façons, car c'est un enjeu qui ressemble étrangement à la guerre contre la drogue, êtes-vous d'accord? Il est très difficile d'attraper certains des principaux acteurs, mais en même temps, la prévention est un outil très important. Par contre, j'aime l'approche proposée par M. Baran-Chong pour ce qui est d'assujettir les entreprises de télécommunications à une certaine obligation de rendre compte. Je ne pense pas que nous devons les laisser échapper totalement à toutes responsabilités.

Monsieur Cosgrove et monsieur Mecher, que pouvons-nous faire pour que vous puissiez déployer vos efforts dans la prévention? Je pense que dans un tel cas, cela va dans les deux sens.

**M. Kevin Cosgrove:** Pour ce qui est de mon travail de sensibilisation, je suis dans une impasse parce que je suis essentiellement coincé au niveau local. Nous sommes dans une ville frontalière, dans une ville où il y a une université et un collège. Notre population multiculturelle est très élevée et je ne peux même pas avoir de financement pour faire traduire de l'information générale. Je vis à Windsor, le français est notre deuxième langue officielle, et je n'ai rien en français en ce moment, même si c'est un domaine dans lequel je travaille depuis des années. Ce n'est pas quelque chose que je viens de commencer. C'est un problème que j'ai essayé de régler, et heureusement, M. Masse m'a invité à comparaître aujourd'hui, et ma comparution pourra peut-être nous donner quelques possibilités d'avancer.

Tout ce que j'ai fait au fil des ans est entièrement bénévole. C'est uniquement du travail bénévole. Je ne suis pas payé lorsque je parle publiquement, je ne suis pas payé pour les brochures ou les publications qui sont préparées. Tout est absolument fait bénévolement, et même à ce niveau, il est certainement difficile d'obtenir un soutien quelconque.

● (1245)

**M. Brian Masse:** Avant de donner la parole à M. Mecher, vous pourriez peut-être remettre votre brochure au greffier, et je demanderais à notre comité de la faire traduire pour que vous ayez votre publication. Nous pouvons le faire ici, sur la Colline.

Monsieur Mecher, pouvez-vous poursuivre sur ce sujet, s'il vous plaît?

**M. John Mecher:** D'accord.

Certaines des frustrations que j'avais lorsque je travaillais à la GRC demeurent présentes, et cela ne m'étonne pas. C'est un peu comme une passion de vouloir essayer de sensibiliser les gens. Je n'ai jamais eu l'impression que j'aurais moi-même une grande influence. M. Cosgrove a souvent utilisé le terme « communautaire », mais j'ai continué à pousser, à pousser, à pousser et, récemment, nous avons vécu l'affaire de la Western Union. C'est la Federal Trade Commission des États-Unis qui est derrière tout cela. Pratiquement, elle a forcé Western Union à verser plus d'un demi-milliard de dollars dans le cadre d'un processus de poursuite différée, et ces fonds ont ensuite été versés à des victimes de fraudes liées à Western Union partout dans le monde, ce qui est un cadeau incroyable pour les victimes de fraude.

Cependant, la diffusion de cette information aux victimes au Canada fut le gros problème. La Commission a continué à répéter le message, sans toutefois trouver d'écho au Canada.

En mars, j'ai publié l'information du mieux que je pouvais sur ma plateforme limitée de médias sociaux. N'ayant aucun succès, j'ai finalement perdu patience et j'ai écrit à la commissaire de la GRC le 1er et le 7 juin, en sachant à ce moment-là que l'offre de Western Union prenait fin à la fin de juin. L'offre se terminait à la fin de juin. Malheureusement, mon plaidoyer n'a abouti à rien.

J'ai expliqué qui j'étais, j'ai parlé de mon expérience auprès des victimes, de mon engagement dans la lutte contre la fraude, etc., mais il n'y a eu aucune réponse avant la fin de juin, je crois, alors que c'était pratiquement inutile. C'est à ce moment que l'information a été publiée sur le site Web du Centre antifraude du Canada. Ce qui était absurde, c'est que la publication a été faite le 26 juin, je crois, et qu'à ce moment, nous pensions alors que les demandes devaient être déposées avant la fin de juin. C'était inutile, car les victimes auraient eu besoin d'au moins une semaine pour rassembler tous les documents.

Cependant, deux jours plus tard, la Commission a annoncé qu'il y aurait une prolongation jusqu'à la fin d'août. La seule vraie façon dont j'ai pu faire avancer ce dossier fut de faire appel à M. Masse, qui s'en est ensuite occupé. Sa tribune est beaucoup plus grande que la mienne, alors je le remercie beaucoup pour ce qu'il a fait.

Ce que cela veut dire, et j'essaie de le dire le plus respectueusement possible, c'est qu'au plus haut niveau, la GRC ne comprend pas la fraude ni ses répercussions sur les victimes. C'est une frustration que j'éprouve actuellement, et c'était une frustration lorsque j'étais membre de la GRC et que j'enquêtais sur la fraude.

**Le président:** Merci beaucoup, monsieur Mecher et monsieur Masse.

Je cède maintenant la parole à M. Kram pour cinq minutes.

**M. Michael Kram:** Merci beaucoup, monsieur le président.

Je vais poser quelques questions à M. Baran-Chong et je partagerai ensuite mon temps avec Mme Gray.

Monsieur Baran-Chong, vous avez dit que Rogers vous avait offert une indemnisation de 100 $. Avez-vous poursuivi Rogers en dommages-intérêts devant un tribunal civil?

**M. Randall Baran-Chong:** Non, je ne l'ai pas fait.

**M. Michael Kram:** Pourquoi?

**M. Randall Baran-Chong:** Eh bien, j'ai consulté plusieurs avocats. C'est intéressant, parce que contrairement à d'autres qui ont connu d'importantes pertes financières... Dans le cas d'une fraude par carte de crédit, par exemple, la société émettrice ou les banques finissent par indemniser les gens pour ces pertes. Des personnes qui ont été victimes de vols de cryptomonnaie tentent toujours de recouvrer leurs pertes, et il y a dans nos groupes de nombreuses victimes qui essaient de recouvrer des centaines de milliers jusqu'à des millions de dollars. Par contre, dans mon cas, le vol était négligeable du point de vue financier. Les fraudeurs avaient pris possession de toutes mes données et ils ont essayé d'obtenir de l'argent. Il est très difficile de quantifier l'extorsion et la détresse psychologique que l'on éprouve lorsque l'on pense que notre vie sera ruinée. Cela ne valait donc pas la peine d'entamer des poursuites.

Ce que j'ai fait est ma façon d'obtenir un dédommagement.

● (1250)

**M. Michael Kram:** D'accord.

Lors de votre comparution précédente, vous avez formulé ce que je pense être une recommandation très réaliste concernant l'échange de carte SIM. J'aimerais vous lire un extrait de ce que vous avez dit il y a deux ans et qui figure au procès-verbal:

> 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.

Cela semble être une solution assez pratique et efficace. Est-ce encore votre recommandation?

**M. Randall Baran-Chong:** Cela s'applique à un téléphone volé. Il faut trouver un certain équilibre, n'est-ce pas? Le CRTC veut nous permettre d'effectuer facilement le portage de notre numéro. Il existe en fait une règle selon laquelle le portage doit être fait en moins de deux heures et demie. Ma recommandation la plus importante, qui ne s'applique pas uniquement aux téléphones volés, c'est que si vous recevez une notification par message texte indiquant que votre numéro a fait l'objet d'une demande de portage, vous devez consentir de façon proactive en répondant « oui » par message texte, c'est-à-dire que vous confirmez que vous voulez exécuter ce portage.

Considérons, par exemple, ce qui m'est arrivé. Si j'avais reçu ce message texte à 11 heures un mardi, aurais-je exécuté un portage? Absolument pas. Il n'y aurait pas eu de portage et je ne serais pas devant vous aujourd'hui, mais ce processus n'existait pas à l'époque.

Par la suite, les entreprises de télécommunications ont transmis un message sans exiger de notification proactive. C'était ça le problème, les gens ne réagissaient pas parce qu'ils croyaient qu'il s'agissait d'un message frauduleux et le portage était exécuté. Ce n'est que beaucoup plus tard qu'elles ont... Rogers affirme sur son site Web actuel qu'elle a adopté cette pratique que j'ai proposée en 2020 devant votre comité. Rogers dit qu'elle l'applique aujourd'hui, mais je le répète, il y a des pratiques incohérentes et ce genre de choses.

La notification proactive devrait aider à déjouer un nombre considérable de ces fraudes.

**M. Michael Kram:** C'est bien.

Je vais céder la parole à ma collègue, Mme Gray.

**Mme Tracy Gray:** Parfait. Merci beaucoup.

Mes questions s'adressent également à M. Baran-Chong.

Dans votre témoignage, vous avez parlé de ce que vous avez vécu avec Rogers. Bien sûr, nous avons entendu des représentants de Rogers lors d'une réunion d'urgence du Comité cet été, et le CRTC semblait vraiment défendre les entreprises de télécommunications plutôt que d'être un organisme de réglementation. Vous avez fait une observation en fait très semblable lorsque vous avez dit que le CRTC semblait parler au nom des entreprises de télécommunications.

J'aimerais que vous nous donniez plus de détails. En fait, le CRTC devrait tenir les entreprises de télécommunications responsables et défendre les intérêts des Canadiens. Il semble que ce soit l'inverse. Pouvez-vous expliquer vos commentaires de façon un peu plus détaillée?

**M. Randall Baran-Chong:** Absolument. On peut se demander de quel côté le CRTC se trouve.

Nous avons beaucoup consulté le Centre pour la défense de l'intérêt public. Nous avons notamment essayé d'obtenir ces données. On pourrait penser que de demander des données macroéconomiques, ce n'est pas demander la lune ni une grande menace à la sécurité. Nous ne voulions même pas obtenir les données sur le nombre d'échanges de cartes SIM détenues par les entreprises de télécommunications. Le CRTC a rejeté cette demande. Le CRTC a dit qu'il n'était pas nécessaire de tenir des audiences parce que le public ne peut pas vraiment aider à résoudre le problème.

La question est donc la suivante: l'organisme de réglementation essaie-t-il de protéger les entreprises de télécommunications contre les situations embarrassantes ou de nouvelles poursuites? Je sais que bien souvent, au début, lorsque les gens essayaient d'intenter des poursuites, ils avaient l'impression d'être des cas isolés. Lorsque nous avons appris qu'il y avait eu 25 000 cas au cours de cette période de 10 mois, nous avons été stupéfaits. Nous pensions qu'il y en avait quelques milliers. Quand on y pense, la prévalence et l'ampleur de ce crime sont énormes. Nous pensons que le CRTC protège les entreprises de télécommunications parce qu'il pourrait s'agir d'une fraude gigantesque et absolument honteuse.

**Le président:** Merci beaucoup, madame Gray et monsieur Baran-Chong.

La parole est maintenant à M. Fillmore pour cinq minutes.

**M. Andy Fillmore (Halifax, Lib.):** Je remercie beaucoup nos témoins. Merci, monsieur le président.

J'aimerais revenir à la question des données puisque la protection de la vie privée des citoyens suscite actuellement un vif intérêt.

Voici ce que je veux dire. Il y a environ six mois, j'ai visité le cybercentre d'excellence de Vancouver. Ce centre est intégré à Mastercard et le gouvernement y a investi environ 50 millions de dollars. Son objectif est d'élaborer des techniques et des algorithmes qui aideront à déceler les transactions frauduleuses.

J'ai appris plusieurs choses. Par exemple, dans le cas de téléphones dont les numéros ont été portés ou de téléphones clonés, Mastercard peut conclure que ce n'est pas moi qui tiens le téléphone parce que la personne ne le tient pas comme je le fais habituellement. Mastercard sait quelle est ma façon de tenir mon téléphone, horizontalement ou verticalement, avec quelle force j'appuie sur les touches ou si j'écris avec mes deux pouces ou un seul doigt. Certaines des nouvelles techniques utilisées pour établir si la bonne personne tient le téléphone sont incroyables. Cela se passe du côté des banques et de la société émettrice de cartes de crédit.

Ensuite, il y a les commerçants. Les commerçants sont eux aussi concernés dans la fraude. Ils créent des profils sur nous tous en consignant l'heure à laquelle nos achats sont effectués, nos heures de magasinage, ce que nous achetons et ce genre de choses.

En fait, il y a trois parties prenantes. Les consommateurs, les banques et les commerçants participent à plusieurs différents aspects, et tout le monde détient des données. Beaucoup de données sont générées.

Je vais peut-être commencer par M. Mecher.

D'après vous, existe-t-il des mécanismes adéquats de rétroaction ou de partage de données entre la GRC, le CRTC, les banques et les commerçants? Faisons-nous du bon travail dans ce domaine? Y a-t-il des exigences en matière de déclaration? Est-il obligatoire de signaler les transactions frauduleuses à la GRC? Les banques le font-elles de façon volontaire?

Pouvez-vous nous parler un peu de la réflexion sur le partage des données à l'ère de la protection de la vie privée?

● (1255)

**M. John Mecher:** Je ne peux vraiment pas parler des enjeux relatifs à la vie privée. Ce n'est pas vraiment mon domaine.

Je peux dire qu'auparavant les banques en particulier se sont régulièrement pleinement engagées dans la lutte contre la fraude. En même temps, certaines banques sont allées dans la direction opposée et, par aveuglement volontaire ou autre, elles ont en fait aidé des fraudeurs. Cela les rattrape habituellement.

**M. Andy Fillmore:** Prenons l'exemple de Mastercard. Lorsqu'elle détecte une transaction frauduleuse, a-t-elle l'obligation d'informer la GRC, ou est-ce vraiment quelque chose qui reste entre elle et son client?

**M. John Mecher:** Honnêtement, je n'en sais rien. Je pourrais faire des suppositions, mais je ne veux pas vous répondre par une supposition.

**M. Andy Fillmore:** Est-ce que M. Cosgrove ou M. Baran-Chong aurait quelque chose à ajouter à ce sujet?

**M. Randall Baran-Chong:** Je mentionnerais l'entreprise EnStream, qui est le fruit d'un partenariat entre les grandes entreprises de télécommunications. L'un des services offerts par cette société est la vérification de l'identité afin de prévenir des choses comme la fraude par échange de cartes SIM. Ce produit est vendu aux banques.

J'ai parlé à des gens qui travaillent dans les équipes de cybersécurité des banques. Ils connaissent bien la fraude liée à l'échange de carte SIM, parce que ce sont les banques qui, en fin de compte, en font les frais. Ce sont elles qui remboursent les pertes reliées aux cartes de crédit, aux autres types de vol, etc. Les entreprises de télécommunications vendent aux banques un produit qui aide les entreprises de télécommunications à repérer les fraudes. Ce genre de système pernicieux existe.

Quelques pays ont pris des mesures comme celles auxquelles vous faites allusion. Ils peuvent par exemple, bloquer les transactions bancaires après un portage. Il y aura une certaine période de gel. Ils savent que ce genre d'activités comporte un risque élevé.

Entre les banques, les entreprises de télécommunications, la protection des renseignements personnels et la sécurité, il existe des interactions qui facilitent la fraude.

**M. Andy Fillmore:** Merci.

**Le président:** Merci beaucoup, monsieur Fillmore.

Je dois vous interrompre parce que nous n'avons presque plus de temps. Il reste deux intervenants.

Je vais donner la parole à M. Lemire pour deux minutes et 30 secondes.

[*Français*]

**M. Sébastien Lemire:** Je vous remercie, monsieur le président.

J'ai écouté les témoins et je vois l'importance de légiférer en faveur des victimes de fraude. Le gouvernement a déposé le projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois.

Quel est votre avis sur ce projet de loi? Va-t-il assez loin?

Avez-vous des recommandations à nous faire en ce sens?

[*Traduction*]

**M. Randall Baran-Chong:** J'avoue que je ne connais pas le projet de loi C-27.

[*Français*]

**M. Sébastien Lemire:** D'accord.

Monsieur Mecher, qu'en pensez-vous?

[*Traduction*]

**M. John Mecher:** Je suis désolé. Je n'ai pas entendu votre question.

[*Français*]

**M. Sébastien Lemire:** Avez-vous entendu parler du nouveau projet de loi C-27?

Va-t-il assez loin pour la protection des victimes?

[*Traduction*]

**M. John Mecher:** Non, je n'en ai pas entendu parler.

[*Français*]

**M. Sébastien Lemire:** D'accord.

Je vous remercie.

● (1300)

**Le président:** Merci beaucoup, monsieur Lemire.

Je cède la parole à M. Masse pour deux minutes et demie.

[*Traduction*]

**M. Brian Masse:** Très rapidement, monsieur Mecher, croyez-vous qu'une initiative dirigée par des citoyens pour rassembler les différentes administrations serait appropriée en ce moment, que ce soit pour aider à coordonner...? Il n'est pas nécessaire d'aller à l'encontre de la GRC, du CRTC et des autres, mais je me demande si une tierce partie est requise ou non pour aider à coordonner le partage des ressources et de l'information.

Monsieur Mecher, avez-vous entendu?

**M. John Mecher:** J'avais un problème technique.

Tout vaut la peine d'être essayé. Je ne pense pas que cette approche soit absolument unique. Elle pourrait être avantageuse. Ce qui est bien, c'est qu'en allant au-delà de l'application de la loi, je suppose qu'il serait beaucoup plus facile d'être transparent.

**M. Brian Masse:** Monsieur Cosgrove, je vais vous demander rapidement ce que vous pensez d'une approche dirigée par des citoyens, puis je suis certain que mon temps sera écoulé.

**M. Kevin Cosgrove:** Oui, absolument. Selon ce que j'ai constaté personnellement, il y a une tendance à trop compliquer les choses, à trop les présenter et à trop formaliser une partie de l'information. Si l'on considère que les aînés sont une cible importante de presque tous les types de fraudes, le fait de produire de gros documents officiels, des factures en ligne, etc., ne rend pas ces gens plus attentifs.

Nous devons travailler sur le terrain et résoudre ces problèmes en personne ou avec des renseignements plus faciles à obtenir.

**M. Brian Masse:** Merci, monsieur le président.

[*Français*]

**Le président:** Merci beaucoup, monsieur Masse.

Je remercie nos témoins de leur présence aujourd'hui, qui a été précieuse pour les travaux du Comité.

Je vous souhaite une belle semaine et un bel après-midi.

La séance est levée.