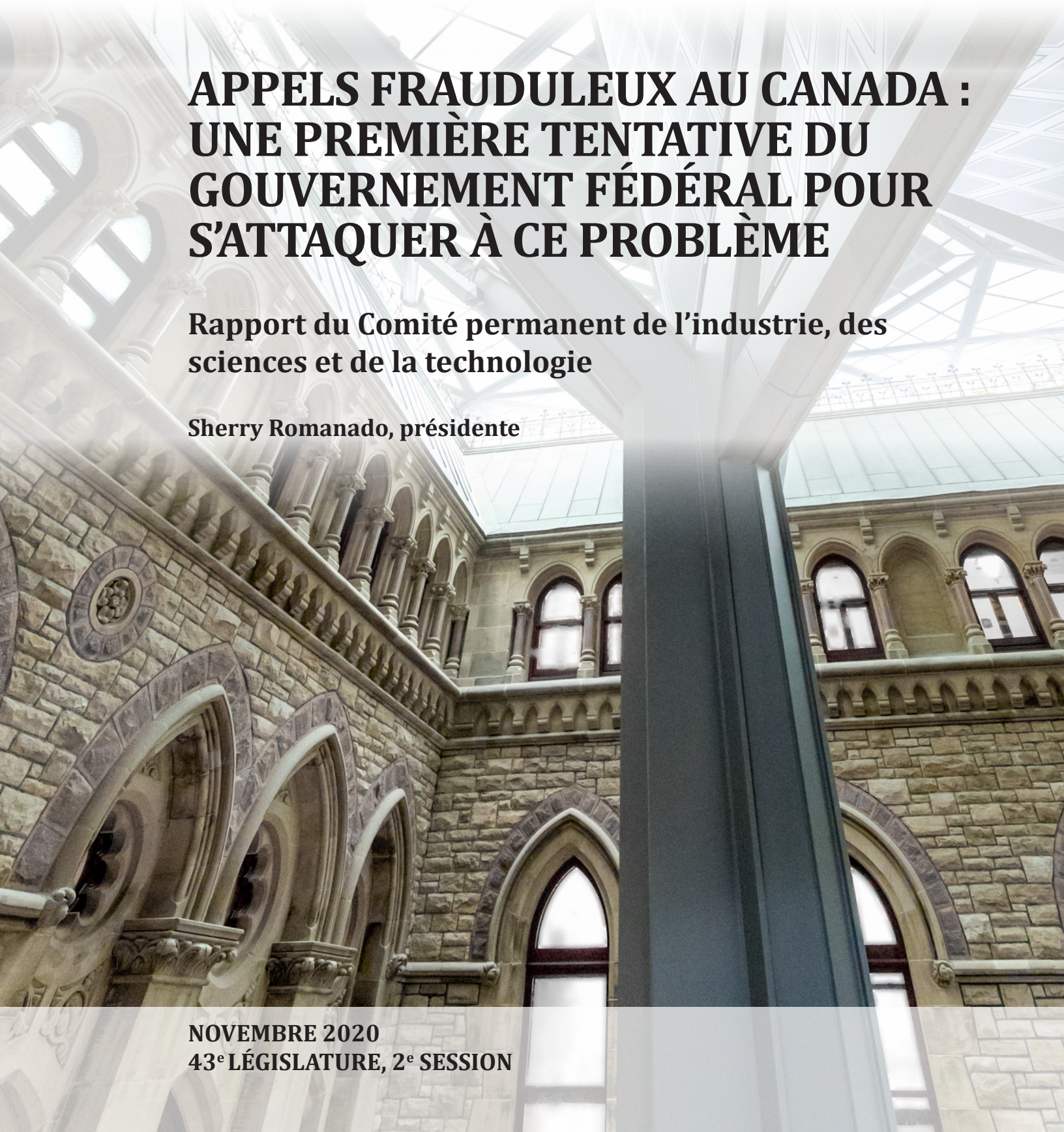
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

APPELS FRAUDULEUX AU CANADA : UNE PREMIÈRE TENTATIVE DU GOUVERNEMENT FÉDÉRAL POUR S'ATTAQUER À CE PROBLÈME

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

Sherry Romanado, présidente



NOVEMBRE 2020
43e LÉGISLATURE, 2e SESSION

APPELS FRAUDULEUX AU CANADA : UNE PREMIÈRE TENTATIVE DU GOUVERNEMENT FÉDÉRAL POUR S'ATTAQUER À CE PROBLÈME

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

La présidente
Sherry Romanado

NOVEMBRE 2020

43e LÉGISLATURE, 2e SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE

43E LÉGISLATURE – 1RE SESSION

PRÉSIDENTE

Sherry Romanado

VICE-PRÉSIDENTS

L'hon. Michelle Rempel Garner

Sébastien Lemire

MEMBRES

Earl Dreeshen

Ali Ehsassi

Nathaniel Erskine-Smith

Tracy Gray

Helena Jaczek

Majid Jowhari

Emmanuella Lambropoulos

Brian Masse

Jeremy Patzer

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Sean Casey

Julie Dabrusin

Marie-Hélène Gaudreau

Chris Lewis

Lloyd Longfield

Paul Manly

Simon-Pierre Savard-Tremblay

Tako Van Popta

GREFFIER DU COMITÉ

Michael MacPherson

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Francis Lord, analyste

Sarah Lemelin-Bellerose, analyste

COMITÉ PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE

43E LÉGISLATURE – 2E SESSION

PRÉSIDENTE

Sherry Romanado

VICE-PRÉSIDENTS

James Cumming

Sébastien Lemire

MEMBRES

Earl Dreeshen

Ali Ehsassi

Nathaniel Erskine-Smith

Helena Jaczek

Majid Jowhari

Emmanuella Lambropoulos

Brian Masse

John Nater

Derek Sloan

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Taylor Bachrach

Tony Baldinelli

GREFFIER DU COMITÉ

Michael MacPherson

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Francis Lord, analyste

Sarah Lemelin-Bellerose, analyste

LE COMITÉ PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE

a l'honneur de présenter son

PREMIER RAPPORT

Conformément au mandat que lui confère l'article 108(2) du Règlement, le Comité a étudié les appels frauduleux au Canada et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

SOMMAIRE

Les appels frauduleux entrainent des pertes importantes pour les Canadiens. Les fraudeurs, qui peuvent compter sur des centres d'appels situés à l'étranger et sur de nombreuses technologies simples d'accès, comme les appels automatisés et l'usurpation d'identité, réussissent à parvenir à leurs fins malgré les nombreux efforts des organismes d'application de la loi, du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et des fournisseurs de services de télécommunications. Pour mieux protéger le public, le gouvernement fédéral doit faciliter la mise en œuvre de nouvelles techniques et technologies, par exemple en adoptant rapidement les normes STIR/SHAKEN tout en tenant adéquatement compte des enjeux liés à la concurrence et à la protection des renseignements personnels. Il devrait en outre renforcer la coopération entre les autorités publiques compétentes, qu'elles soient d'ici ou d'ailleurs, améliorer les pratiques liées à la collecte des données, à la sensibilisation du public et à la transparence, et améliorer la législation pénale et son application.

Le gouvernement fédéral devrait prêter une oreille attentive aux personnes qui soutiennent que les fraudeurs exploitent les règles fédérales concernant la transférabilité des numéros sans fil pour échafauder des stratagèmes de portage non autorisé. Même si le CRTC et les fournisseurs de services de télécommunications s'emploient déjà à trouver des moyens de lutter contre le portage non autorisé, il faut faire plus pour protéger les Canadiens. Plus précisément, le Comité invite le gouvernement fédéral à presser le CRTC de lancer une enquête publique sur le portage non autorisé, voire à réglementer lui-même la question si le CRTC n'agit pas.

Les fraudes ciblant les Canadiens ont augmenté en flèche depuis le début de la pandémie de COVID-19. Selon la Gendarmerie royale du Canada, il y en a eu 25 % de plus de janvier à avril 2020 qu'au cours de la même période l'année dernière. La pandémie actuelle constitue un danger pour la vie des Canadiens et leur gagne-pain, mais aussi pour l'économie canadienne. Le gouvernement fédéral doit tout faire pour éviter que les Canadiens subissent d'autres préjudices. Dans l'immédiat, la sensibilisation du public demeure le moyen le plus efficace de contrer la fraude liée à la COVID-19. Le gouvernement fédéral devrait agir sans tarder et lancer une campagne de sensibilisation dans les médias locaux et nationaux afin de mettre en garde les Canadiens contre la fraude liée à la COVID-19.

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

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. 30

Recommandation 2

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. 30

Recommandation 3

Que le gouvernement du Canada présente un projet de loi visant à obliger les entreprises des secteurs sous réglementation fédérale, telles que les banques et les entreprises de télécommunications, à rendre public chaque année le nombre de comptes qu'elles ont ouverts sur présentation de renseignements obtenus par la fraude et le nombre de personnes qu'elles ont avisées de l'utilisation de leurs renseignements à des fins frauduleuses. 31

Recommandation 4

Que le gouvernement du Canada collabore davantage avec les gouvernements d'autres pays et les organisations internationales dans le but de fermer les centres d'appels frauduleux établis à l'étranger et de poursuivre les fraudeurs qui ciblent des Canadiens. 31

APPELS FRAUDULEUX, PORTAGE NON AUTORISÉ ET FRAUDE LIÉE À LA COVID-19 : METTRE LES ESCROCS HORS D'ÉTAT DE NUIRE

AIDEZ À PROTÉGER LES CANADIENS

Si vous avez été victime d'une fraude, signalez-le au Centre antifraude du Canada (CAFC) et à votre service de police local. Vos gestes contribueront à protéger tous les Canadiens. Pour en savoir plus sur les stratagèmes de fraude en cours, consultez la page Web du CAFC.

INTRODUCTION

Le 20 février 2020, le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes (le Comité) a convenu de :

> Tenir immédiatement des audiences avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), la Gendarmerie royale du Canada (GRC), des entreprises de télécommunications canadiennes ainsi que d'autres spécialistes en télécommunications et groupes de défense d'intérêts afin de : a) mieux comprendre l'afflux d'appels frauduleux comme les appels automatisés, les appels fantômes et les appels indésirables sur les téléphones résidentiels et les téléphones cellulaires des Canadiens; b) faire le point sur les réussites et les échecs de la Liste nationale de numéros de télécommunication exclus; c) présenter les normes STIR/SHAKEN, dont la mise en œuvre est prévue pour septembre 2020, et expliquer en quoi elles seront avantageuses pour les consommateurs canadiens.

Le Comité s'est réuni trois fois, a entendu 21 témoins et a reçu six mémoires.

APPELS FRAUDULEUX ET AUTRES APPELS INDÉSIRABLES

Comprendre le problème

Le terme « appel indésirable » désigne les télécommunications vocales importunes et non sollicitées. Un « appel frauduleux » est quant à lui un appel indésirable effectué avec l'intention d'escroquer la personne qui y répond par la supercherie, le mensonge ou d'autres moyens dolosifs. Comme l'a dit Kate Schroeder, du Réseau canadien pour la prévention du mauvais traitement des aînés (RCPMTA), la fraude « vise à tromper la

victime dans le dessein de contrôler un aspect – financier ou autre – de sa vie ou de son identité[1] ». Tandis que les appels indésirables ou importuns peuvent déranger et exaspérer leurs destinataires, ou, dans certains cas, compromettre la jouissance des services téléphoniques d'une personne, les appels frauduleux peuvent quant à eux avoir des conséquences bien pires – financières ou autres – pour ceux qui en sont victimes, et relèvent de comportements criminels[2].

Un type d'appel frauduleux courant est celui de l'escroquerie qui vise les contribuables et concerne l'Agence du revenu du Canada (ARC). Voici comment le CAFC décrit cette escroquerie :

> Un fraudeur se fait passer pour un employé de l'Agence du revenu du Canada ou de Service Canada et affirme que vous :
>
> - avez des arriérés d'impôt à payer;
> - avez des soldes en souffrance;
> - avez commis un crime financier.
>
> Il insiste pour que vous versiez l'argent immédiatement, à défaut de quoi vous serez arrêté, recevrez une amende ou pourriez même vous faire expulser du pays.
>
> Le fraudeur peut demander que le paiement soit fait par l'intermédiaire d'une entreprise de transfert de fonds, par carte de crédit prépayée ou par carte-cadeau (iTunes, Google Play ou Steam), ou par bitcoin.

À l'instar de nombreux autres types d'appels frauduleux, les appels téléphoniques provenant soi-disant de l'ARC sont d'abord des « appels automatisés » : des messages vocaux sont envoyés au moyen d'un dispositif capable de stocker ou de composer des numéros de téléphone. Habituellement, le message vocal encourage la victime à appeler un numéro. En composant le numéro, la victime entre en contact avec un fraudeur qui tentera par divers stratagèmes d'arriver à ses fins[3]. La GRC estime qu'entre 2014 et 2019,

---

1 Chambre des communes, Comité permanent de l'industrie, des sciences et de la technologie (INDU), *Témoignages*, 43e législature, 1re session, 12 mars 2020, 1205 (Réseau canadien pour la prévention du mauvais traitement des aînés [RCPMTA], Kate Schroeder). Voir également RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

2 INDU, *Témoignages*, 43e législature, 1re session, 10 mars 2020, 1140 (Conseil de la radiodiffusion et des télécommunications canadiennes [CRTC], Ian Scott); *Ibid*., 1210, 1255 (Rogers Communications Inc., Howard Slawner et Deborah Evans). Mais voir aussi *ibid*., 1205 (Bell Canada, Jonathan Daniels).

3 Voir, de manière générale, INDU, *Témoignages*, 12 mars 2020, 1110-1115 (Centre pour la défense de l'intérêt public [CDIP], John Lawford).

cette escroquerie a entraîné, à elle seule, des pertes totalisant plus de 16,8 millions de dollars[4].

L'Association canadienne de l'électricité (ACE) – qui regroupe les services publics et les entreprises du Canada qui produisent, transportent et distribuent de l'électricité – a signalé que les fraudeurs ciblent régulièrement les clients de ses membres. Ils appellent leurs victimes potentielles en se faisant passer pour des agents d'un service public et les intimident en les menaçant de couper l'électricité immédiatement avant les heures de pointe, à moins qu'elles ne s'acquittent des « frais de comptes en souffrance ». Si les gens tombent dans le piège, les fraudeurs leur demanderont d'effectuer le paiement par carte de crédit prépayée ou en bitcoins. L'ACE a indiqué qu'au cours des deux dernières années, un de ses membres a reçu en moyenne 150 signalements de clients par mois concernant des fraudeurs se faisant passer pour des agents du service public. Selon les estimations d'un autre membre de l'ACE, ses clients pourraient avoir perdu plus de 18 000 $, sur une période de quatre mois en 2018, à cause de ces appels frauduleux, sans parler des atteintes à la réputation subies par le service lui-même[5].

Parmi les victimes de fraudeurs, on compte un nombre disproportionné de personnes âgées, de ménages à faible revenu et de néo-Canadiens[6]. Selon des témoins, les aînés se méfient moins des étrangers et ont tendance à souffrir d'isolement social, ce qui les rend particulièrement vulnérables aux fraudes où l'on a recours à des tactiques d'intimidation ou fait preuve de fausse gentillesse pour tromper la victime[7]. Il existe d'autres facteurs qui augmentent les risques pour les personnes âgées de se faire berner, comme l'insécurité économique, d'éventuels troubles cognitifs et le manque de compréhension des stratagèmes de fraude courants. Les personnes âgées peuvent également se buter à des difficultés lorsqu'elles tentent de dénoncer une fraude; par exemple, elles peuvent craindre que le fait d'être des victimes ne les fasse paraître incompétentes, ou ne pas savoir comment s'y prendre pour signaler la fraude. En réaction à un grand nombre d'appels frauduleux, certaines personnes âgées peuvent décider de faire couper leurs services de télécommunications, ce qui a pour effet de les isoler davantage socialement. Avec le vieillissement de la population, il pourrait y avoir plus de Canadiens vulnérables à la fraude[8].

---

4 INDU, *Témoignages*, 10 mars 2020, 1115 (Gendarmerie royale du Canada [GRC], Eric Slinn).

5 Association canadienne de l'électricité (ACE), *Mémoire présenté à INDU*, 28 avril 2020.

6 INDU, *Témoignages*, 12 mars 2020, 1110, 1140 (Lawford); *Ibid*., 1205 (Schroeder); RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

7 INDU, *Témoignages*, 12 mars 2020, 1125 (Lawford).

8 *Ibid*., 1205-1210, 1230, 1255 (Schroeder); RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

Des technologies aisément accessibles facilitent l'automatisation et l'anonymat des appels frauduleux[9]. La téléphonie par Internet permet de faire un très grand nombre d'appels automatisés en un court laps de temps et à moins de frais, ce qui rend des machinations comme l'escroquerie concernant l'ARC peu coûteuses à monter par rapport à ce qu'elles peuvent rapporter. Par conséquent, les fraudeurs sont en mesure de créer et d'exploiter des centres d'appels qui mettent en place des stratagèmes de fraude sur une grande échelle et qui sont pour la plupart basés à l'étranger[10]. Les fraudeurs s'arrangent aussi pour masquer ou modifier l'identification de l'appelant au moyen d'une technique dite de « mystification »[11]. Bien que ce genre de duperie ne soit pas illégal en soi, les fraudeurs font des appels en se faisant passer pour d'autres personnes ou organisations afin de tromper leurs victimes, de leur soutirer de précieuses informations personnelles et de les escroquer plus facilement. La mystification a rendu les fonctions d'identification de l'appelant essentiellement inefficaces quand il s'agit de contrer les appels importuns et frauduleux[12].

Étant donné que les techniques et la technologie évoluent sans cesse, les autorités, les fournisseurs de services de télécommunications (FST) et d'autres acteurs ont du mal à se tenir informés des façons dont s'y prennent les fraudeurs pour choisir leurs cibles et transmettre des appels malveillants aux Canadiens – certains témoins allant jusqu'à évoquer une « course aux armements[13] ». C'est la raison pour laquelle des témoins ont insisté sur la nécessité de sensibiliser le public aux techniques et stratagèmes frauduleux qui ont cours[14].

Plus précisément, le Centre pour la défense de l'intérêt public (CDIP) et le RCPMTA ont proposé que les autorités et les FST diffusent, par des voies de communication fiables et dans un langage que les groupes vulnérables comprendront, des informations sur les stratagèmes de fraude courants. Bien qu'il soit urgent de faire davantage de sensibilisation auprès des personnes âgées, ces informations devraient être envoyées aux personnes de tous âges. Les autorités devraient également mobiliser les acteurs

9 INDU, *Témoignages*, 12 mars 2020, 1110-1115 (Lawford).

10 INDU, *Témoignages*, 10 mars 2020, 1100 (Scott).

11 D'après le CRTC : « Il y a mystification lorsqu'un appelant falsifie délibérément l'information sur son identité (p. ex., son numéro de téléphone) qui est transmise à l'appelé dans le but de cacher sa véritable identité ».

12 INDU, *Témoignages*, 10 mars 2020, 1135 (GRC, Guy Paul Larocque); INDU, *Témoignages*, 12 mars 2020, 1105 (Section canadienne de l'Internet Society, Matthew Gamble); ACE, *Mémoire présenté à INDU*, 28 avril 2020.

13 INDU, *Témoignages*, 10 mars 2020, 1125 (Slinn); *Ibid*., 1210, 1255 (Slawner et Evans); INDU, *Témoignages*, 12 mars 2020, 1135 (Gamble).

14 Voir, par exemple, INDU, *Témoignages*, 10 mars 2020, 1130, 1155 (Scott).

susceptibles de contribuer à la protection des Canadiens contre la fraude, comme les institutions financières, les FST et les compagnies d'assurances. Le RCPMTA a ajouté qu'il faudrait réfléchir à la façon dont les campagnes de sensibilisation permettront d'informer les Canadiens vivant dans des régions rurales ou éloignées[15].

Même si les Canadiens reçoivent régulièrement des appels frauduleux, peu de témoins ont été en mesure de fournir des données précises sur l'ampleur du problème. Citant des données de 2019 du CAFC, John Lawford, directeur exécutif et avocat général du CDIP, a souligné qu'il n'existe pas de source de données officielle ou faisant autorité sur la fraude en général et sur les appels frauduleux en particulier[16]. Les données sont limitées, car à peine 5 % des Canadiens ayant été victimes de fraude le signalent[17]. À cause du manque de données fiables et exactes, il est plus difficile d'intercepter les appels frauduleux[18]. M. Lawford a donc insisté sur la nécessité d'améliorer l'accès aux statistiques relatives à la fraude ainsi que leur qualité, et de rendre publiques ces données régulièrement[19].

Selon le CAFC, sur les 98 millions de dollars de pertes dues à la fraude en 2019, 25 millions de dollars sont attribuables aux appels frauduleux[20]. Le RCPMTA estime qu'un quart de ces pertes touche des victimes âgées[21]. Matthew Gamble, directeur de la section canadienne de l'Internet Society, a cité une étude menée par Truecaller selon laquelle les Canadiens reçoivent en moyenne 12 appels frauduleux ou importuns par mois, et ce nombre augmente, car l'évolution de la technologie réduit le coût des appels automatisés et permet aux fraudeurs de contourner les lois[22]. Le CRTC a fait part de données provenant des États-Unis selon lesquelles, au mois de février 2020 seulement, les Américains ont reçu plus de deux milliards d'appels automatisés frauduleux[23].

15 INDU, *Témoignages*, 12 mars 2020, 1120, 1135 (Lawford); *Ibid*., 1210, 1230, 1245 (Schroeder).

16 *Ibid*., 1110 (Lawford).

17 Centre antifraude du Canada, « Palmarès des 10 fraudes de 2019 », 20 février 2020. Voir aussi INDU, *Témoignages*, 12 mars 2020, 1205 (Schroeder); RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

18 INDU, *Témoignages*, 12 mars 2020, 1130 (Gamble).

19 *Ibid*., 1115 (Lawford).

20 INDU, *Témoignages*, 10 mars 2020, 1150 (Slinn).

21 INDU, *Témoignages*, 12 mars 2020, 1205 (Schroeder); RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

22 INDU, *Témoignages*, 12 mars 2020, 1105 (Gamble).

23 INDU, *Témoignages*, 10 mars 2020, 1150 (Scott).

La riposte actuelle

Les témoins ont mis l'accent sur la nécessité d'une étroite collaboration entre les organismes gouvernementaux, les FST, les groupes de défense des consommateurs et d'autres intervenants, tant au pays qu'à l'étranger, pour accroître efficacement la lutte et la protection contre les appels frauduleux au Canada[24].

Autorités fédérales

La GRC et le CRTC mettent en œuvre une bonne partie des mesures fédérales visant à contrer les appels frauduleux et importuns. Les deux institutions travaillent en collaboration avec les FST et d'autres acteurs pour prévenir ou réduire ce genre d'appels et atténuer leurs effets. La GRC et le CRTC jouissent d'un niveau élevé d'indépendance par rapport au gouvernement fédéral. M. Lawford a proposé néanmoins que le Parlement et le gouvernement fédéral prennent une place plus prépondérante dans la lutte contre les appels frauduleux : le Parlement pourrait effectuer un contrôle continu des mesures prises, et le gouvernement pourrait intégrer plus activement la lutte contre la fraude par téléphone et par Internet dans les politiques sur le numérique[25]. Pour faciliter l'application des lois contre les fraudeurs, M. Lawford a aussi suggéré que l'on criminalise le recours aux appels automatisés à des fins d'escroqueries[26].

Gendarmerie royale du Canada

Le commissaire adjoint de la GRC Eric Slinn a rappelé que la lutte contre la criminalité financière, y compris la fraude, est une priorité de la police fédérale. C'est pourquoi l'organisation enquête sur les stratagèmes d'appels frauduleux pouvant donner lieu à des poursuites pénales. Par exemple, en février 2020, dans le cadre de son Projet Octavia, la GRC a arrêté et accusé deux personnes impliquées dans un stratagème de faux représentants de l'ARC.

Le commissaire adjoint Slinn a insisté sur la nécessité d'informer le public pour prévenir la fraude et a décrit comment la GRC participe aux campagnes de sensibilisation en ce sens. Par exemple, en réaction aux signalements de fraudes par cartes-cadeaux en Alberta, la GRC a préparé des fiches de conseils qu'elle a distribuées dans les commerces

---

24 Voir, par exemple, *Ibid*., 1205, 1245 (Daniels); *Ibid*., 1210, 1255 (Slawner et Evans); INDU, *Témoignages*, 12 mars 2020, 1210 (Schroeder); RCPMTA, *Mémoire présenté à INDU*, 28 avril 2020.

25 INDU, *Témoignages*, 12 mars 2020, 1115 (Lawford).

26 *Ibid*., 1145.

locaux pour que les clients ne se fassent pas piéger par ce genre d'escroquerie[27]. Le CAFC occupe aussi une place centrale dans la lutte de la GRC contre la fraude. La GRC gère en effet le CAFC en partenariat avec le Bureau de la concurrence et la Police provinciale de l'Ontario. Servant de dépositaire central de renseignements, le CAFC joue un important rôle préventif en diffusant de l'information sur la fraude auprès des organismes chargés de l'application des lois, des acteurs privés, comme les FST et les institutions financières, et de la population canadienne. Le CAFC s'appuie sur les renseignements que lui transmettent les Canadiens pour faire son travail, mais M. Slinn a souligné que son personnel est débordé à cause du nombre croissant de fraudes[28].

La coopération entre la GRC et d'autres entités, au pays comme à l'étranger, est une composante essentielle de la stratégie de lutte contre la fraude. La GRC travaille en collaboration avec de multiples partenaires pour protéger les Canadiens, notamment l'ARC, le Centre d'analyse des opérations et déclarations financières du Canada, les FST et les institutions financières. Étant donné que la fraude ne connaît pas de frontières, la GRC collabore étroitement avec les autorités étrangères et les organismes internationaux chargés de l'application des lois, comme le Groupe des cinq pays sur l'application de la loi[29].

Le commissaire adjoint Slinn a souligné l'importance de la coopération internationale dans la lutte contre la fraude ciblant des Canadiens, puisque la GRC n'a pas compétence pour enquêter et porter des accusations contre des fraudeurs faisant leurs manœuvres depuis l'étranger[30]. M. Slinn a demandé que le gouvernement fédéral presse les gouvernements d'autres pays de fermer les centres d'appels qui se trouvent à l'intérieur de leurs frontières et d'où proviennent un grand nombre, pour ne pas dire la plupart, des appels frauduleux, et de combattre la criminalité contre les Canadiens perpétrée depuis leur territoire[31].

L'ACE a expliqué qu'il lui est difficile d'obtenir le soutien des organismes chargés de l'application des lois parce que leurs agents n'ont souvent pas le temps et les ressources nécessaires pour les aider :

> Une entreprise d'électricité a fait part d'une situation où elle a transmis rapidement les renseignements voulus selon les modalités requises à l'agent des autorités concerné.

---

27 INDU, *Témoignages*, 10 mars 2020, 1110-1115 (Slinn).

28 *Ibid.*, 1115-1120, 1155.

29 *Ibid.*, 1110, 1120.

30 *Ibid.*, 1155.

31 *Ibid*. Voir aussi INDU, *Témoignages*, 10 mars 2020, 1215, 1245 (Slawner).

> Elle a appris par la suite que rien n'avait été fait parce que l'agent en question devait s'occuper d'un dossier plus pressant. Les entreprises d'électricité entendent rarement parler d'un quelconque suivi auprès des victimes après la première plainte aux autorités locales[32].

Le commissaire adjoint Slinn a reconnu que les responsables de l'application des lois au Canada doivent en faire encore plus pour s'attaquer à la fraude. La GRC travaille d'ailleurs avec l'Association canadienne des chefs de police à l'élaboration d'une approche plus coordonnée en ce qui concerne les interventions policières et la mobilisation accrue contre la fraude[33]. M. Slinn a expliqué que les policiers devraient enquêter sur les appels frauduleux et ne pas simplement dire aux victimes de s'adresser au CACF, dont la mission se limite à collecter des informations et qui ne mène pas des enquêtes policières. Même s'il est difficile d'enquêter sur ce genre d'appels, surtout parce qu'ils proviennent souvent de l'étranger, les enquêtes demeurent importantes, ne serait-ce que pour recueillir des renseignements[34]. Le RCPMTA a abondé dans le même sens, ajoutant que le gouvernement fédéral devrait venir en aide aux Canadiens qui ont signalé une fraude pour aider à prévenir la re-victimisation[35].

Conseil de la radiodiffusion et des télécommunications canadiennes

Mandat et activités principales

Le CRTC combat la fraude moins directement que la GRC. Ian Scott, président et dirigeant principal du CRTC, ainsi que ses collègues, ont répété à plusieurs reprises que, contrairement à la GRC, le CRTC ne fait pas de répression contre la fraude; il concentre ses activités sur la diminution du télémarketing non sollicité[36]. Le CRTC joue néanmoins un rôle structurel en réglementant et en coordonnant les activités des FST pour réduire les appels frauduleux et permettre aux consommateurs d'utiliser les services de télécommunications en toute sécurité. C'est ce qui explique le rôle que joue le CRTC dans le déploiement des normes STIR/SHAKEN au Canada, comme on le précise plus loin dans le présent rapport.

---

32 ACE, *Mémoire présenté à INDU*, 28 avril 2020.

33 INDU, *Témoignages*, 10 mars 2020, 1145 (Slinn).

34 *Ibid.*, 1150.

35 INDU, *Témoignages*, 12 mars 2020, 1210, 1245 (Schroeder).

36 INDU, *Témoignages*, 10 mars 2020, 1100 (Scott).

M. Lawford voudrait que le CRTC adopte une approche plus directe à l'égard des appels frauduleux[37]. À ce propos, il a recommandé que l'on modifie la *Loi sur les télécommunications* ou que l'on adopte une loi visant à lutter expressément contre les « fraudes téléphoniques », afin de conférer au CRTC davantage de pouvoirs – et de responsabilités – pour s'attaquer aux appels frauduleux. M. Lawford a ajouté que l'on pourrait prendre comme modèle la *Telemarketing Consumer Fraud and Abuse Prevention Act* des États-Unis. De tels changements législatifs permettraient d'étendre directement le mandat du CRTC du télémarketing à la fraude[38]. Rogers Communications Inc. (Rogers) a aussi proposé que le CRTC s'inspire des mesures prises par les agences américaines pour bloquer les appels automatisés venant de l'étranger afin de les empêcher d'entrer dans les réseaux nationaux[39].

Tout comme la GRC, le CRTC travaille en étroite collaboration avec de multiples entités pour s'acquitter de son mandat, comme les FST, les ministères et organismes fédéraux, les organismes chargés de l'application des lois, ses homologues étrangers et des organisations internationales[40]. Cette collaboration permet de mettre en commun des connaissances, d'harmoniser les pratiques et de coordonner les activités de lutte contre la fraude et d'autres menaces qui pèsent sur les réseaux de télécommunications, et ainsi de renforcer les mesures prises à l'échelle internationale pour combattre la fraude[41].

À l'appui de ces initiatives, le CRTC échange des renseignements avec d'autres organisations. Par exemple, il a signé un protocole d'entente pour le partage d'informations avec ses homologues aux États-Unis, au Japon, au Royaume-Uni, en Australie et en Nouvelle-Zélande. Cependant, le CRTC ne dispose pas de la latitude nécessaire pour en faire autant avec des organisations canadiennes. C'est pourquoi le CRTC a proposé que le Parlement modifie sa loi habilitante pour lui permettre de communiquer les renseignements qu'il recueille aux agences chargées de l'application des lois et aux organismes gouvernementaux canadiens[42].

Liste nationale des numéros de télécommunication exclus

En 2008, le CRTC a créé la Liste nationale des numéros de télécommunication exclus (LNNTE) dans le but de réduire les appels de télémarketing non sollicités, grâce à un

37 Voir aussi *ibid.*, 1215 (Slawner).

38 INDU, *Témoignages*, 12 mars 2020, 1115, 1135, 1145 (Lawford).

39 INDU, *Témoignages*, 10 mars 2020, 1215 (Slawner).

40 *Ibid.*, 1005-1110, 1135 (Scott).

41 *Ibid*. Voir, par exemple, *ibid*., 1210 (Slawner).

42 *Ibid.*, 1110, 1140 (Scott).

cadre législatif prévu dans la *Loi sur les télécommunications*. La LNNTE est un registre des numéros de téléphone personnels qui ne peuvent être appelés à des fins de sollicitation. Le CRTC formule et applique les règles régissant la LNNTE, tandis qu'un exploitant national – en ce moment Raymond Chabot Grant Thornton Consulting – administre cette liste en percevant les droits applicables auprès des spécialistes du télémarketing abonnés.

En vertu des règles régissant la LNNTE, les spécialistes du télémarketing ne peuvent faire d'appels de télémarketing à moins qu'eux-mêmes ou leurs clients ne soient abonnés à la LNNTE. Les règles de la LNNTE interdisent aux spécialistes du télémarketing d'appeler à des fins de sollicitation les consommateurs dont le numéro de téléphone personnel figure sur la LNNTE, à moins que les consommateurs n'aient consenti expressément à être contactés par les spécialistes du télémarketing ou leurs clients. Les règles relatives à la LNNTE exemptent également certaines organisations, comme les organismes de bienfaisance et les partis politiques. Le CRTC a expliqué que, même si l'inscription est gratuite, les spécialistes du télémarketing doivent payer des frais d'abonnement pour obtenir une copie à jour de la LNNTE[43].

Les consommateurs peuvent déposer une plainte auprès du CRTC si les spécialistes du télémarketing les sollicitent en contravention des règles de la LNNTE. Quatorze millions de Canadiens se sont inscrits sur cette liste depuis sa création; ils étaient en moyenne 858 à s'y ajouter chaque jour l'an dernier. Le CRTC voit ces chiffres comme la preuve que les Canadiens ont confiance dans l'efficacité de la LNNTE[44]. Cependant, comme l'ont fait valoir Bell Canada (Bell) et Rogers, cette liste permet seulement d'empêcher les appels de spécialistes du télémarketing exerçant leurs activités au Canada, alors que la majorité des appels importuns sont faits depuis l'étranger par des acteurs qui n'ont nullement l'intention de se conformer aux règles de la LNNTE[45].

Le CRTC a reçu environ 84 000 plaintes concernant la LNNTE en 2018-2019, mais seulement environ 500 d'entre elles ont donné lieu à des mesures visant à faire respecter la loi. Le CRTC a défendu son bilan en la matière en expliquant que le nombre total de plaintes peut être trompeur, car il contient des plaintes non validées et des plaintes concernant la même campagne de télémarketing. En outre, le CRTC considère les mesures qu'il prend, notamment les sanctions administratives, non pas comme des punitions pour avoir enfreint les règles, mais plutôt comme une incitation à les respecter. C'est ce qui explique pourquoi, dans son approche, le CRTC fait preuve de

43 *Ibid*., 1125 (CRTC, Alain Garneau).

44 *Ibid*., 1100 (Scott).

45 *Ibid*., 1205 (Daniels); *Ibid*., 1210, 1250 (Slawner).

retenue dans l'application des règles relatives à la LNNTE. Bien que les plaintes ne justifient pas toutes l'imposition de sanctions administratives ou d'autres mesures coercitives officielles, le CRTC s'efforce d'informer les spécialistes du télémarketing de leurs obligations, notamment au moyen de programmes de conformité et d'audits[46].

Fournisseurs de services de télécommunications

Les FST jouent un rôle important dans la prévention et la réduction des appels frauduleux faits par l'intermédiaire de leurs services. Le CRTC établit les règlements que doivent respecter les FST, notamment pour ce qui est de la mise en œuvre de mesures visant à aider les consommateurs à se protéger contre les tentatives de fraude. Certaines mesures sont appliquées dans tout le secteur, comme le blocage universel des appels manifestement illégitimes et le cadre de normes STIR/SHAKEN, qui sera mis en place prochainement. Les FST peuvent aussi proposer des mesures de protection à leurs propres clients. Ils ont la possibilité d'appliquer des mesures dans tout le secteur ou uniquement au sein de leur propre entreprise grâce à différentes techniques, tout en visant l'objectif général de protéger leur clientèle contre les appels frauduleux[47].

Cadre de normes STIR/SHAKEN

STIR/SHAKEN est un cadre de normes interreliées permettant aux FST d'authentifier l'identité d'un appelant lors d'appels vocaux sur protocole Internet (IP). Les normes STIR/SHAKEN ne permettent pas de filtrer ni de bloquer des appels, mais plutôt de lutter contre la mystification en fournissant des informations sur la légitimité d'un appel téléphonique et en aidant son destinataire à décider s'il veut ou non y répondre[48]. Le CRTC considère ces normes comme étant « les seules solutions viables en matière d'authentification et de vérification qui pourraient permettre d'accroître la confiance des consommateurs à l'égard de l'information sur l'identité de l'appelant[49] ». Le CRTC envisageait d'obliger les FST offrant des services de télécommunications vocales à appliquer les normes STIR/SHAKEN d'ici au 30 septembre 2020[50].

---

46 *Ibid*., 1100, 1120, 1140-1145 (CRTC, Scott, Garneau et Steven Harroun).

47 *Ibid*., 1245-1250 (Daniels); *Ibid*., 1250 (Slawner).

48 *Ibid*., 1105 (Scott); INDU, *Témoignages*, 12 mars 2020, 1105, 1125 (Gamble). Mais voir aussi INDU, *Témoignages*, 10 mars 2020, 1225 (Société TELUS Communications. [TELUS], Jérôme Birot); TELUS, *Mémoire présenté à INDU*, 9 mars 2020; COMsolve, *Mémoire présenté à INDU*, 29 avril 2020.

49 *Décision de Conformité et Enquêtes et de Télécom CRTC 2019-402*, parag. 22, 9 décembre 2019.

50 INDU, *Témoignages*, 10 mars 2020, 1105 (Scott). Voir aussi *Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2019-404*, 9 décembre 2019. Mais voir *Décision de Conformité et Enquêtes et de*

Selon COMsolve Inc., qui est un fournisseur de services technologiques, le déploiement éventuel des normes STIR/SHAKEN pourrait accroître les pressions en faveur de l'application de solutions de blocage des appels basées sur l'analytique. Bien que COMsolve considère que « [l]e cadre STIR/SHAKEN, mis en place conjointement avec le blocage des appels fondé sur l'analytique, est le meilleur moyen de traiter les appels mystifiés non désirés », les appelants devraient savoir comment les FST et leurs partenaires authentifient et traitent leurs appels, et être en mesure de prouver qu'ils utilisent des numéros autorisés[51].

De nombreux témoins se sont exprimés en faveur de la mise en œuvre des normes STIR/SHAKEN parmi les nombreux moyens de protéger les Canadiens contre les appels frauduleux, notamment Bell, Rogers et la Société TELUS Communications (TELUS). Ces FST ont donc fait des progrès significatifs dans la mise en œuvre de ces normes[52], mais ils ont averti également qu'ils ne seraient pas capables de les appliquer entièrement d'ici septembre 2020, malgré toute leur bonne volonté[53].

Certains témoins ont fait état des multiples problèmes que le CRTC et les FST doivent régler avant que l'on ne procède à la mise en œuvre des normes STIR/SHAKEN. Beaucoup sont d'ordre technique et concernent, par exemple, l'adaptation des réseaux et des appareils téléphoniques pour pouvoir appliquer correctement les normes STIR/SHAKEN. Selon les témoignages des FST, si l'on veut permettre aux consommateurs de tirer pleinement avantage des normes en question, il faut d'abord résoudre ces problèmes.

Pour fonctionner, les normes STIR/SHAKEN requièrent que tous les FST qui transmettent un appel s'interconnectent au moyen de la technologie IP. Il ne sera pas possible d'authentifier un appel si, à un certain point dans le réseau, il passe par une technologie non IP. Bien que la section canadienne de l'Internet Society ait fait observer que la plupart des petits FST se sont dotés de la technologie de téléphonie IP[54], certains des réseaux des grands FST comme Bell, Rogers et TELUS s'appuient encore sur des

---

Télécom CRTC 2019-402-2, parag. 17, 15 septembre 2020 (depuis son témoignage devant le Comité, le CRTC a repoussé la date limite au 30 juin 2021).

51 COMsolve, *Mémoire présenté à INDU*, 29 avril 2020.

52 INDU, *Témoignages*, 10 mars 2020, 1205 (Daniels); *Ibid.*, 1210 (Slawner); *Ibid.*, 1225 (Birot); TELUS, *Mémoire présenté à INDU*, 9 mars 2020. Voir aussi INDU, *Témoignages*, 12 mars 2020, 1115 (Lawford); *Ibid.*, 1125 (Gamble).

53 INDU, *Témoignages*, 10 mars 2020, 1210, 1245 (Slawner); *Ibid.*, 1245 (Birot). Mais voir *Décision de Conformité et Enquêtes et de Télécom CRTC 2019-402-2*, parag. 17, 15 septembre 2020 (depuis son témoignage devant le Comité, le CRTC a repoussé la date limite au 30 juin 2021).

54 INDU, *Témoignages*, 12 mars 2020, 1105 (Gamble).

équipements de commutation de circuits non IP. Ces FST doivent donc mettre leurs réseaux à niveau pour être en mesure d'appliquer pleinement les normes STIR/SHAKEN, un processus qui exigerait beaucoup de temps[55].

Les FST ont également souligné que la plupart des téléphones d'aujourd'hui, qu'ils soient fixes ou cellulaires, ne permettent pas de visualiser les informations que les normes STIR/SHAKEN permettraient d'obtenir. Les fabricants de téléphones, comme Apple et Samsung, doivent donc concevoir des appareils capables d'afficher efficacement ces informations. De toute évidence, les FST canadiens n'ont pas de contrôle sur la rapidité avec laquelle ces fabricants rendront ces dispositifs disponibles sur le marché[56]. D'autres témoins ont également fait remarquer que le CRTC et l'industrie n'ont pas encore élaboré de normes concernant l'affichage, c'est-à-dire quelles informations sur la légitimité d'un appel téléphonique seront communiquées aux consommateurs et de quelle façon[57].

C'est pourquoi certains témoins ont plaidé en faveur d'un report de la mise en œuvre des normes STIR/SHAKEN par le CRTC[58]. Selon Jonathan Daniels, vice-président chez Bell, juin 2022 serait une date limite plus réaliste pour l'application complète des normes sur les réseaux canadiens[59]. M. Gamble, de la section canadienne de l'Internet Society, a ajouté que le calendrier de mise en œuvre complète des normes STIR/SHAKEN ne sera pas connu tant que les clients ne seront pas désireux et capables d'adopter ces dernières[60]. Le CRTC avait assuré le Comité que même s'il s'attendait à ce que les FST soient en mesure de mettre en œuvre les normes STIR/SHAKEN d'ici septembre 2020, il accorderait plus de temps pour le faire à ceux qui le lui demanderont[61].

---

55 INDU, *Témoignages*, 10 mars 2020, 1210-1215 (Slawner); *Ibid*., 1225, 1235 (Birot); *Ibid*., 1245 (Daniels); TELUS, *Mémoire présenté à INDU*, 9 mars 2020. Voir aussi COMsolve, *Mémoire présenté à INDU*, 29 avril 2020. Mais voir aussi INDU, *Témoignages*, 12 mars 2020, 1105 (Gamble).

56 INDU, *Témoignages*, 10 mars 2020, 1205, 1230 (Daniels); *Ibid*., 1225, 1235 (Birot); TELUS, *Mémoire présenté à INDU*, 9 mars 2020.

57 INDU, *Témoignages*, 10 mars 2020, 1130 (Scott); *Ibid*., 1210 (Slawner); COMsolve, *Mémoire présenté à INDU*, 29 avril 2020.

58 INDU, *Témoignages*, 10 mars 2020, 1245 (Slawner); *Ibid*., 1245 (Daniels); *Ibid*., 1245 (TELUS, John Mackenzie).

59 *Ibid*., 1205 (Daniels).

60 INDU, *Témoignages*, 12 mars 2020, 1150 (Gamble).

61 INDU, *Témoignages*, 10 mars 2020, 1130 (Scott). Mais voir *Décision de Conformité et Enquêtes et de Télécom CRTC 2019-402-2*, parag. 17, 15 septembre 2020 (depuis son témoignage devant le Comité, le CRTC a repoussé la date limite au 30 juin 2021).

Au-delà des défis techniques, la section canadienne de l'Internet Society a attiré l'attention du Comité sur les questions de politique que suscite l'actuelle mise en œuvre des normes STIR/SHAKEN. Le CRTC propose d'obliger tous les FST offrant des services de communications vocales à appliquer les normes STIR/SHAKEN, même les petites entreprises de télécommunications. Rogers a prédit que ces dernières profiteront de l'expérience des grands FST dans la mise en œuvre des normes[62]. La section canadienne de l'Internet Society a fait valoir, toutefois, que des décisions prises au départ concernant les politiques et la conception profitent aux grands FST au détriment des petits[63].

Par exemple, selon les normes STIR/SHAKEN, seul le FST qui est propriétaire d'un numéro de téléphone peut l'authentifier. Les revendeurs de services de télécommunications qui ne sont pas propriétaires de leurs numéros de téléphone – plus de 1 200 FST – sont donc dans l'impossibilité de les authentifier. D'après la section canadienne de l'Internet Society, les normes STIR/SHAKEN actuelles font courir à ces petits fournisseurs le risque de perdre des clients au profit de plus gros FST capables d'authentifier leurs numéros de téléphone. Cela aurait pour effet de réduire la concurrence dans le secteur canadien des télécommunications[64].

Pour expliquer les préjudices que subiraient les petits FST, la section canadienne de l'Internet Society a indiqué que ces entreprises sont sous-représentées au sein du groupe de travail du CRTC chargé de la formulation des normes STIR/SHAKEN. D'ailleurs, rares sont les petites entreprises de télécommunications à disposer des ressources nécessaires pour participer à de telles tribunes[65]. M. Gamble a ajouté que l'Alliance for Telecommunications Industry Solutions (ATIS), qui a participé à l'élaboration des normes STIR/SHAKEN, étudie actuellement des propositions visant à mieux prendre en compte les petites entreprises de télécommunications, mais que l'échéance de septembre 2020 imposée par le CRTC arriverait avant que l'ATIS n'ait fait part de ses conclusions[66]. Interrogé sur la question, le CRTC a répondu que son processus de consultation s'étend aux petites entreprises qui offrent des services de communications vocales, et que

62 INDU, *Témoignages*, 10 mars 2020, 1240 (Slawner).

63 INDU, *Témoignages*, 12 mars 2020, 1105 (Gamble).

64 *Ibid.*, 1105, 1150.

65 *Ibid.*, 1125, 1135.

66 *Ibid.*, 1150. Mais voir *Décision de Conformité et Enquêtes et de Télécom CRTC 2019-402-2*, parag. 17, 15 septembre 2020 (depuis son témoignage devant le Comité, le CRTC a repoussé au 30 juin 2021 l'échéance pour la mise en œuvre des normes STIR/SHAKEN).

celles-ci pourraient réduire les coûts de mise en œuvre des normes STIR/SHAKEN en se regroupant entre elles ou en s'associant à des FST plus grands[67].

Enfin, les normes STIR/SHAKEN pourraient soulever des questions de protection de la vie privée. Quand les appels authentifiés passeront par leurs réseaux, les FST obtiendront des données sur leur origine et leur destination. Les FST pourront communiquer ces données à des tiers, au pays ou à l'étranger, par exemple pour effectuer des analyses afin de raffiner les techniques de filtrage antipourriel ou pour établir des profils de clients[68]. La section canadienne de l'Internet Society et le CDIP ont tous deux proposé que l'on demande au commissaire à la protection de la vie privée d'examiner les risques que posent les normes STIR/SHAKEN[69].

Autres mesures

La mise en œuvre des normes STIR/SHAKEN n'est qu'une des nombreuses initiatives qu'ont prises les FST pour réduire la fraude téléphonique, que ce soit de leur propre chef ou conformément aux décisions du CRTC. Depuis décembre 2019, le CRTC impose le blocage universel des appels manifestement illégitimes, comme les appels faits depuis l'étranger en utilisant des numéros locaux, ou les appels non standards, comme ceux dont les numéros de téléphone ne correspondent pas à une structure de 10 chiffres[70]. Bell affirme bloquer 220 millions d'appels par mois grâce au système de blocage universel[71]. Un groupe de travail du CRTC se penche également sur un processus de dépistage des appels pour mieux identifier la provenance des appels importuns[72].

Certains FST proposent également à leurs clients différents services pour réduire les appels importuns et les appels frauduleux. En plus des fonctions courantes, comme l'identification des appelants et les systèmes de filtrage des appels[73], TELUS offre à ses clients un service de « contrôle des appels » qui requiert (ou « met à l'épreuve ») un appelant inconnu de composer un numéro choisi au hasard pour pouvoir joindre le destinataire. TELUS tient une liste de tous les appels qui ont subi et réussi l'épreuve afin d'optimiser le contrôle des appels et de faire en sorte que les appelants légitimes ne

67 INDU, *Témoignages*, 10 mars 2020, 1135 (Scott).

68 INDU, *Témoignages*, 12 mars 2020, 1105, 1150 (Gamble).

69 *Ibid*., 1140; *Ibid*., 1140 (Lawford).

70 INDU, *Témoignages*, 10 mars 2020, 1105, 1150 (Scott); *Ibid*., 1220 (Birot); *Ibid*., 1210 (Slawner).

71 *Ibid*., 1205 (Daniels).

72 *Ibid*., 1150 (Scott).

73 *Ibid*., 1220 (Birot).

soient pas soumis à l'épreuve plusieurs fois. Le vice-président de TELUS, Jérôme Birot, a affirmé que ce type de contrôle empêche les appels automatisés d'aboutir. Grâce à ce système, TELUS bloque jusqu'à 40 % des appels entrants des clients qui ont activé la fonction[74].

M. Daniels a expliqué que Bell a développé une technologie algorithmique qui permet de détecter les appels frauduleux. Selon Bell, cette technologie devrait permettre de bloquer 120 millions d'appels illégitimes par mois. Comme le prévoit la *Loi sur les télécommunications*, Bell a demandé au CRTC l'autorisation de procéder à un essai de trois mois, dans le cadre duquel l'entreprise bloquera les appels illégitimes[75].

Howard Slawner, vice-président chez Rogers, a expliqué également que chaque acteur peut contribuer à sensibiliser davantage les gens aux appels frauduleux[76]. En plus de diffuser de l'information sur son site Web pour aider ses clients à se protéger, Rogers mène des campagnes de sensibilisation ciblées. Par exemple, lorsque l'entreprise remarque l'existence d'un stratagème qui vise une communauté en particulier, elle publie des annonces dans des journaux locaux dans la langue de la communauté ciblée[77]. Rogers a affirmé également travailler en collaboration avec d'autres grandes entreprises de télécommunications pour mettre au point des solutions de filtrage des appels pour l'industrie dans son ensemble[78].

Les FST ont fourni des réponses différentes à la question de savoir s'ils facturaient à leurs clients ces services de filtrage. Le Comité a appris qu'ils pouvaient faire payer à leurs clients au moins certaines fonctions permettant de réduire les appels importuns passant par leurs réseaux[79]. Les représentants de TELUS ont indiqué que l'entreprise offre gratuitement à la plupart de ses clients de téléphonie résidentielle le service de filtrage des appels, incluant la fonction de contrôle des appels[80]. Bell fait payer à ses clients le service d'identification de l'appelant, mais ne prévoit pas le faire pour sa nouvelle technologie de blocage des appels[81]. M. Slawner n'a pas été en mesure de confirmer si

74 *Ibid.*, 1225-1230. TELUS, *Mémoire présenté à INDU*, 9 mars 2020. Mais voir aussi INDU, *Témoignages*, 12 mars 2020, 1130 (Lawford).

75 INDU, *Témoignages*, 10 mars 2020, 1210, 1240, 1255 (Daniels).

76 *Ibid.*, 1210-1215 (Slawner). Voir aussi ACE, *Mémoire présenté à INDU*, 28 avril 2020.

77 INDU, *Témoignages*, 10 mars 2020, 1235 (Evans). Mais voir aussi INDU, *Témoignages*, 12 mars 2020, 1245 (Schroeder).

78 INDU, *Témoignages*, 10 mars 2020, 1210 (Slawner).

79 INDU, *Témoignages*, 12 mars 2020, 1140 (Gamble).

80 INDU, *Témoignages*, 10 mars 2020, 1220, 1240-1245 (Birot).

81 *Ibid.*, 1240, 1250 (Daniels).

Rogers facture à ses clients ses services d'identification des appelants ou de blocage des appels[82].

M. Lawford a dit craindre que les FST n'essaient de répercuter sur leurs clients le coût de la mise en œuvre des normes STIR/SHAKEN et d'autres nouvelles fonctions. Il a fait valoir que les clients devraient avoir accès gratuitement à ces fonctions, car il est dans l'intérêt du secteur des télécommunications dans son ensemble de réduire et de prévenir les appels importuns. M. Lawford considère que si les FST font payer leurs clients, le CRTC devrait réglementer et contrôler les tarifs appliqués[83].

PORTAGE NON AUTORISÉ

Des témoins ont attiré l'attention du Comité sur le portage non autorisé, aussi appelé « transfert non autorisé de cartes SIM ». Le « portage » consiste à transférer un numéro de téléphone entre fournisseurs de services[84]. On dit qu'il y a « portage non autorisé » lorsque le numéro de téléphone d'une personne est « échangé » ou transféré d'une carte SIM à une autre sans l'autorisation de cette personne. Le portage non autorisé empêche la personne d'avoir accès à tous les appels et messages textes qui sont envoyés à son téléphone, car ceux-ci sont redirigés vers l'appareil du fraudeur. La redirection des télécommunications permet au fraudeur de commettre d'autres méfaits, comme le vol, la prise de contrôle de compte et l'usurpation d'identité. Un fraudeur peut par exemple utiliser l'authentification par texte pour réinitialiser un mot de passe associé à un compte afin d'accéder aux informations que le compte contient. Le portage non autorisé peut donc avoir des conséquences désastreuses et durables pour la personne qui en est victime[85].

Selon Randall Baran-Chong, cofondateur de Canadian SIM-swap Victims United, les fraudeurs utilisent le stratagème du transfert de cartes SIM en exploitant les règles fédérales concernant la transférabilité des numéros sans fil (TNSF). Conçues pour favoriser la concurrence sur le marché des télécommunications, les règles de TNSF permettent aux clients de transférer facilement leur numéro de téléphone d'un FTS à un

82 *Ibid*., 1245 (Slawner).

83 INDU, *Témoignages*, 12 mars 2020, 1115, 1140, 1150 (Lawford).

84 INDU, *Témoignages*, 10 mars 2020, 1230 (Evans); INDU, *Témoignages*, 12 mars 2020, 1215 (Randall Baran-Chong, à titre personnel).

85 INDU, *Témoignages*, 12 mars 2020, 1220 (Baran-Chong); Randall Baran-Chong, *Mémoire présenté à INDU*, 12 mars 2020.

autre[86]. Un fraudeur peut procéder à l'échange non autorisé de cartes SIM en se faisant passer pour sa victime potentielle avec très peu d'informations – le numéro de téléphone de la victime ciblée et son numéro de compte, le numéro d'identification de son appareil ou un code PIN – et en contactant le service clientèle d'un FST pour faire transférer le numéro de téléphone d'une carte SIM à une autre. Le FST acceptera la demande et, conformément aux règles de TNSF, procédera au portage sans grande difficulté et en seulement deux heures et demie[87].

Selon M. Baran-Chong, une fois que le FST a effectué le portage, les victimes ont des moyens limités pour se protéger. Les fraudeurs peuvent surveiller leurs victimes potentielles sur les médias sociaux et attendre le moment propice durant lequel elles ont un accès restreint à leur téléphone pour mettre à exécution leur stratagème. Une fois qu'elles ont compris ce qui leur est arrivé, les victimes ne sont pas nécessairement en mesure de reprendre rapidement le contrôle de leur numéro de téléphone, étant donné que les FST n'offrent généralement pas de service à la clientèle 24 heures sur 24. Les fraudeurs peuvent donc commettre des méfaits préjudiciables en peu de temps. Les victimes de portage non autorisé ne reçoivent presque pas de dédommagement, voire aucun[88].

Même si le CRTC et les FST élaborent des mesures pour contrer le portage non autorisé[89], M. Baran-Chong a affirmé qu'il reste encore beaucoup à faire pour protéger les Canadiens. Il a demandé que l'on sensibilise davantage les gens à la fraude par transfert de cartes SIM et que l'on augmente la coordination entre les organismes chargés de l'application des lois. Il a plaidé aussi en faveur de l'adoption de règles plus sévères et uniformes requérant des notifications et des vérifications obligatoires avant le portage. Il a ajouté qu'au Canada, les gouvernements, les FST, les institutions financières et d'autres entreprises devraient délaisser les protocoles d'authentification à deux facteurs reposant sur les messages textes pour adopter des systèmes d'authentification plus sûrs. Il a suggéré que l'on s'inspire de ce qu'ont fait d'autres pays qui ont pris

86 Baran-Chong, *Mémoire présenté à INDU*, 12 mars 2020. Voir *Décision de télécom CRTC 2005-72*, 20 décembre 2005.

87 INDU, *Témoignages*, 12 mars 2020, 1215 (Baran-Chong); Baran-Chong, *Mémoire présenté à INDU*, 12 mars 2020. Voir aussi INDU, *Témoignages*, 12 mars 2020, 1230 (Evans); Association canadienne des télécommunications sans fil (ACTS), *Mémoire présenté à INDU*, 28 avril 2020.

88 INDU, *Témoignages*, 12 mars 2020, 1240, 1255 (Baran-Chong).

89 Voir, par exemple, INDU, *Témoignages*, 10 mars 2020, 1230 (Evans).

l'initiative de s'attaquer au portage non autorisé, comme l'Australie, l'Afrique du Sud et les États-Unis[90].

Le CDIP et la section canadienne de l'Internet Society étaient d'accord avec la proposition de M. Baran-Chong voulant que le CRTC lance une enquête publique sur le portage non autorisé[91]. MM. Lawford et Baran-Chong ont critiqué le CRTC et les FST pour n'avoir que des discussions limitées sur le sujet, et à huis clos, sans consulter davantage les victimes de transfert de carte SIM et le grand public. Même s'ils admettent qu'il faut cacher certaines informations aux fraudeurs, les discussions informelles ne permettraient pas l'élaboration, en toute transparence, de mesures efficaces pour contrer le portage non autorisé[92].

En ce qui concerne le portage non autorisé, l'Association canadienne des télécommunications sans fil (ACTS) a défendu les mesures prises par les FST. Les FST – comme Bell, Rogers et TELUS – font partie du conseil s'occupant des règles de TNSF, qui établit et tient à jour les processus et spécifications en matière de portage. L'ACTS a affirmé que le conseil élabore des mesures de protection au niveau de l'industrie contre le portage non autorisé. Le conseil a collaboré avec le CRTC dans ce dossier en lui fournissant l'information que celui-ci lui avait demandée. D'après l'ACTS, « une consultation publique n'ajoutera aucune valeur au travail en cours; elle détournera plutôt des ressources de la mise en œuvre des mesures de protection supplémentaires en cours d'élaboration[93] ». L'ACTS a aussi dit craindre qu'une enquête publique sur le portage non autorisé n'ait pour effet de renseigner les fraudeurs sur la teneur des mesures de protection qui seraient prises et de leur permettre de trouver les moyens de les contourner[94].

FRAUDE LIÉE À LA COVID-19

La fraude ciblant des Canadiens a augmenté pendant la pandémie de COVID-19. Entre janvier et avril 2020, la GRC a constaté que le nombre de signalements de fraude était en

90 INDU, *Témoignages*, 12 mars 2020, 1220-1225, 1235-1240, 1250 (Baran-Chong). Baran-Chong, *Mémoire présenté à INDU*, 12 mars 2020.

91 INDU, *Témoignages*, 12 mars 2020, 1130 (Gamble); *Ibid*., 1135 (Lawford).

92 *Ibid*., 1120, 1135 (Lawford); *Ibid*., 1235 (Baran-Chong); Baran-Chong, *Mémoire présenté à INDU*, 12 mars 2020.

93 ACTS, *Mémoire présenté à INDU*, 28 avril 2020.

94 *Ibid*.

hausse de 25 % par rapport à la même période l'an dernier[95]. Si les fraudeurs commettent leurs escroqueries par les voies habituelles, principalement par message texte et par courriel, mais aussi par téléphone et au moyen du Web, ils tirent parti de l'incertitude, de l'anxiété et de la désinformation entourant la pandémie pour berner leurs victimes :

> Depuis mars 2020, nous avons dénombré près de 1 000 plaintes de fraude relativement à la COVID-19. Dans la plupart des cas, il s'agit de tentatives d'hameçonnage dans le cadre desquelles des criminels cherchent à obtenir des renseignements personnels au moyen de courriels ou de messages textes prétendument liés à des demandes de Prestation canadienne d'urgence, ou de tentatives d'installation d'un logiciel malveillant sur les appareils des victimes. Toutefois, les plus importantes pertes pécuniaires découlent de la vente frauduleuse de biens liés à la pandémie de COVID-19, comme des masques, du matériel de dépistage ou des remèdes miracles[96].

Le commissaire adjoint Slinn a insisté sur le fait que certains groupes sont plus vulnérables que d'autres, mais que tous sont à risque. Le crime organisé emploie des moyens frauduleux pour détourner des fonds publics que les gouvernements canadiens destinent aux mesures d'aide[97].

D'autres témoins ont également constaté une recrudescence de la fraude ciblant des Canadiens pendant la pandémie. Jean-François Fortin, directeur général du contrôle des marchés à l'Autorité des marchés financiers (AMF), a fait état de fraudes financières consistant à inciter des victimes à investir dans de faux vaccins et thérapies, ainsi que d'un risque accru de délits d'initiés résultant de retards dans la publication d'états financiers[98]. Scott Jones, dirigeant principal du Centre canadien pour la cybersécurité (CCC), au Centre de la sécurité des télécommunications (CST), a également évoqué des fraudes liées à la COVID-19, telles que des campagnes d'hameçonnage et des fraudes commises au moyen de maliciels où des fraudeurs se font passer pour des porte-parole d'organisations sanitaires pour soutirer de l'argent et des renseignements personnels aux Canadiens[99]. Simon Marchand, chef des services de prévention de la fraude chez Nuance Communications, dit avoir constaté ces dernières semaines une hausse importante des cas d'hameçonnage rattachés à la COVID-19 qui pourraient exposer leurs victimes à l'usurpation d'identité pendant des mois, sinon des années. M. Marchand a

95 INDU, *Témoignages*, 43e législature, 1re session, 20 mai 2020, 1525, 1640 (Slinn et Larocque).

96 *Ibid.*, 1525 (Slinn). Voir aussi *ibid.*, 1635, 1650 (Larocque).

97 *Ibid.*, 1525, 1610 (Slinn).

98 *Ibid.*, 1500, 1610, 1615 (Autorité des marchés financiers, Jean-François Fortin)

99 *Ibid.*, 1515, 1605, (Centre de la sécurité des télécommunications, Scott Jones).

ajouté que le télétravail sans supervision pouvait offrir aux employés mal intentionnés plus d'occasions de détourner des renseignements personnels confidentiels[100].

Le CST a déclaré que la pandémie menace la cybersécurité au Canada. Selon M. Jones, les cyberattaques qui auraient récemment été lancées contre la propriété intellectuelle canadienne font craindre que les organismes de santé et de recherche mobilisés dans le cadre de la lutte nationale contre la pandémie ne deviennent des proies attrayantes aux yeux d'acteurs malveillants. Le CST collabore avec des organismes ayant signalé des activités suspectes liées à la recherche sur la COVID-19 en vue d'en déterminer la nature, l'origine et le succès qu'elles ont eu[101]. Comme la fraude, la plupart des cyberattaques semblent provenir d'outre-mer[102].

Devant la hausse des cas de fraude signalés, la GRC a réaffecté des ressources financières et a mis en place un programme de coordination des interventions. Le CAFC mène le travail de collecte et d'analyse des renseignements, ainsi que les efforts d'information du public, tandis que la GRC collabore avec les services de police locaux et ses partenaires nationaux et internationaux pour échanger des renseignements et coordonner la répression[103]. Le commissaire adjoint Slinn a assuré le Comité que, du point de vue de la GRC, des ressources accrues pour lutter contre la fraude sont toujours les bienvenues, mais que le CAFC, malgré le passage au télétravail, dispose d'effectifs suffisants pour s'acquitter de ses fonctions[104].

La répression a toutefois ses limites. Étant donné la multitude de signalements de fraude, il est impossible pour la GRC et les autres corps policiers d'enquêter sur tous les cas. Le fait que la plupart des fraudeurs sont basés à l'étranger rend la répression d'autant plus difficile et nécessite un recours accru à l'intervention de partenaires internationaux. La GRC encourage néanmoins les services de police locaux à enquêter sur les cas de fraude par l'entremise de l'Association canadienne des chefs de police, et transmet des renseignements par l'intermédiaire du CAFC et du Service canadien de renseignements criminels. Estimant qu'ils pourraient en faire encore davantage, les représentants de la GRC ont affirmé que les corps policiers pourraient accroître les ressources et les efforts consacrés à la lutte contre la fraude[105].

---

100 *Ibid.*, 1520 (Nuance Communications, Simon Marchand).

101 *Ibid.*, 1515, 1540, 1635-1640 (Jones).

102 *Ibid.*, 1505 (Autorité canadienne pour les enregistrements Internet [ACEI], Byron Holland).

103 *Ibid.*, 1525, 1635 (Slinn).

104 *Ibid.*, 1605.

105 *Ibid.*, 1610, 1630-1635, 1645-1650 (Slinn et Larocque).

Compte tenu des limites de la répression, la GRC et d'autres témoins ont souligné que la sensibilisation du public demeure le meilleur rempart contre la fraude[106]. L'AMF a riposté à la fraude liée à la COVID-19 en émettant des mises en garde, en offrant son aide aux associations de protection des consommateurs et des aînés, et en diffusant de l'information par l'entremise de ses partenaires. De plus, l'AMF a mené une campagne de sensibilisation du public à la télévision, sur le Web et dans les médias sociaux du 6 avril au 5 mai 2020, en axant plus particulièrement ses efforts sur les aînés et d'autres groupes vulnérables[107]. Quant à la GRC, elle a diffusé des bulletins d'information qu'elle a également publiés sur son site Web et dans les médias sociaux pour mettre en garde contre la fraude liée à la COVID-19[108].

L'Autorité canadienne pour les enregistrements Internet (ACEI), organisme qui gère le registre du domaine « .ca », mène également des activités de sensibilisation du public pour promouvoir la cybersécurité et réduire la vulnérabilité aux fraudes en ligne. L'ACEI offre une formation sur la sensibilisation envers la cybersécurité sur une plateforme qui aide les utilisateurs à repérer les tentatives de fraude, les fausses nouvelles, la désinformation et les arnaques. Elle propose aussi gratuitement un cours de cybersécurité conçu pour aider les télétravailleurs canadiens à se protéger eux-mêmes et leur organisation contre les cybermenaces[109].

En avril 2020, l'ACEI a lancé le « Bouclier canadien de l'ACEI » pour aider à prévenir la fraude en ligne et les cyberattaques. Il s'agit d'un service gratuit de coupe-feu qui empêche ses utilisateurs d'accéder à des sites Web jugés malveillants sur la foi de renseignements fournis par le CST. Byron Holland, président et chef de la direction de l'ACEI, a déclaré que 50 000 Canadiens utilisent le Bouclier canadien à l'heure actuelle. L'ACEI assure en outre des services de cybersécurité d'entreprise aux hôpitaux, écoles, universités et municipalités au Canada[110]. De façon plus générale, l'ACEI veille à ce que les particuliers et les entités n'utilisent pas le domaine .ca à des fins frauduleuses. Pour ce faire, elle a recours à ses processus d'enregistrement et de vérification. M. Holland a assuré le Comité que les sites Web .ca restent sûrs, malgré la hausse de la fraude liée à la COVID-19[111].

106 *Ibid*., 1525, 1610, 1645-1650; *Ibid*., 1610 (Fortin).

107 *Ibid*., 1500-1505 (Fortin).

108 *Ibid*., 1650 (Larocque).

109 *Ibid.*, 1530-1535 (Holland).

110 *Ibid*., 1505; *Ibid*., 1550 (Jones).

111 *Ibid.*, 1505, 1530, 1545 (ACEI, Holland et Albert Chang).

Le CCC du CST joue un rôle important pour préserver la cybersécurité au Canada. À ce titre, il fait de la sensibilisation aux cybermenaces, surtout auprès d'entités vulnérables telles que les organismes canadiens de santé et de recherche, et contribue à la suppression de sites Web frauduleux. Le CST veille aussi à la protection d'importants programmes fédéraux contre les cybermenaces, y compris les demandes en ligne pour la Prestation canadienne d'urgence. Il travaille de manière proactive pour aider les organismes publics et privés à se prémunir contre les cybermenaces, notamment en transmettant de l'information et des alertes rapides aux cibles potentielles et en offrant de l'aide aux victimes de cyberattaques[112].

M. Marchand a recommandé d'autres mesures pour mieux protéger les Canadiens contre la fraude et renforcer la cybersécurité. Il préconise l'abandon des moyens d'identification actuels, tels que le numéro d'assurance sociale, le permis de conduire et la carte d'assurance-santé, en faveur de méthodes plus avancées et sécurisées, plus précisément la biométrie[113]. Il recommande, par ailleurs, que le gouvernement fédéral oblige les entreprises des secteurs sous réglementation fédérale, telles que les banques et les entreprises de télécommunications, à prévenir la personne quand ses renseignements ont été utilisés pour tenter d'ouvrir un compte frauduleux. Une telle alerte rapide aiderait les victimes d'usurpation d'identité à mieux se protéger. D'autre part, M. Marchand a fait valoir que ces entreprises devraient rendre plus transparents leurs processus d'identification et d'authentification en divulguant, chaque année, le nombre de comptes qu'elles ont ouverts sur présentation de renseignements obtenus par la fraude[114]. Le commissaire adjoint Slinn est d'avis que les entreprises éviteront de rendre cette information publique dans l'intérêt de la confiance des consommateurs et de l'intégrité de leurs processus[115]. Pour sa part, M. Fortin croyait que la proposition de M. Marchand améliorerait la transparence et la sensibilisation du public[116].

Pour terminer, M. Marchand a recommandé de mettre en place le cadre STIR/SHAKEN dans les plus brefs délais. Tout en reconnaissant les limites des normes STIR/SHAKEN, la principale étant le fait qu'elles ne s'appliqueront qu'aux appels provenant du Canada et des États-Unis, il considère que le cadre aidera néanmoins les consommateurs et les entreprises à repérer les appels potentiellement frauduleux. M. Marchand a insisté sur l'importance d'agir rapidement pour appliquer les normes STIR/SHAKEN de manière à

112 *Ibid.*, 1520-1525, 1605, 1620 (Jones).

113 *Ibid.*, 1655 (Marchand).

114 *Ibid.*, 1550, 1600, 1625.

115 *Ibid.*, 1555, 1630 (Slinn).

116 *Ibid.*, 1555 (Fortin).

empêcher les fraudeurs d'intensifier leurs activités au Canada après la mise en œuvre du cadre aux États-Unis[117].

OBSERVATIONS ET RECOMMANDATIONS DU COMITÉ

En formulant ses recommandations, le Comité ne perd pas de vue le fait qu'en vertu du cadre législatif actuel, le gouvernement fédéral n'a qu'un pouvoir direct limité sur les activités et les décisions d'organismes indépendants comme la GRC et le CRTC. Il n'en demeure pas moins que le gouvernement fédéral peut encourager et soutenir ces organismes en plus de s'acquitter des responsabilités qui lui incombent.

Les autorités fédérales et provinciales ne peuvent pas protéger les Canadiens contre la fraude si elles ne disposent pas de données suffisantes pour éclairer les services de police et le processus d'élaboration des politiques. Pour aider les Canadiens à se protéger, il est essentiel de les sensibiliser à la fraude. Les autorités et les autres acteurs devraient adapter leurs documents d'information en fonction de leurs publics cibles et des circonstances, par exemple en diffusant les informations dans une autre langue que le français ou l'anglais, au besoin. Par conséquent, le Comité recommande :

Recommandation 1

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.

Recommandation 2

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.

Pour favoriser la transparence et la sensibilisation du public, les entreprises sous réglementation fédérale doivent rendre visibles au gouvernement fédéral et à la population canadienne leurs processus d'identification et d'authentification. Le Comité reconnaît que ces entreprises doivent aviser les victimes d'usurpation d'identité dans les plus brefs délais, mais estime que toute obligation juridique à cet égard doit tenir

117 *Ibid.*, 1615-1620, 1655 (Marchand).

compte du fait que les fraudeurs éviteront de donner à ces entreprises les moyens de contacter leurs victimes.

Recommandation 3

Que le gouvernement du Canada présente un projet de loi visant à obliger les entreprises des secteurs sous réglementation fédérale, telles que les banques et les entreprises de télécommunications, à rendre public chaque année le nombre de comptes qu'elles ont ouverts sur présentation de renseignements obtenus par la fraude et le nombre de personnes qu'elles ont avisées de l'utilisation de leurs renseignements à des fins frauduleuses.

Comme l'ont souligné les représentants de la GRC et du CRTC ainsi que d'autres témoins, la collaboration avec les partenaires nationaux et étrangers est essentielle pour déjouer efficacement les stratagèmes d'appels frauduleux ciblant des Canadiens. Le gouvernement fédéral devrait faciliter une telle collaboration, tant au pays qu'avec l'étranger. Par conséquent, le Comité recommande :

Recommandation 4

Que le gouvernement du Canada collabore davantage avec les gouvernements d'autres pays et les organisations internationales dans le but de fermer les centres d'appels frauduleux établis à l'étranger et de poursuivre les fraudeurs qui ciblent des Canadiens.

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.

Malgré les défis techniques qu'elles présentent, le Comité est favorable à la mise en œuvre des normes STIR/SHAKEN, et il reconnaît la détermination du CRTC à déployer ces normes dans les plus brefs délais et en étroite collaboration avec les FST. Le Comité invite le CRTC à reconsidérer la participation des petites entreprises de télécommunications pour maintenir la concurrence dans ce marché. Le gouvernement fédéral peut et doit soutenir ces petites entreprises. Le commissaire à la protection de la vie privée du Canada devrait aussi se pencher sur les questions de protection de la vie privée que soulèvent les normes STIR/SHAKEN. Par conséquent, le Comité recommande :

Recommandation 6

Que le gouvernement du Canada appuie la participation des petites entreprises de télécommunications à la mise en œuvre des normes STIR/SHAKEN afin de préserver la concurrence sur le marché des télécommunications.

Recommandation 7

Que le gouvernement du Canada demande au commissaire à la protection de la vie privée du Canada d'examiner les problèmes éventuels de protection de la vie privée soulevés par la mise en œuvre des normes STIR/SHAKEN.

Le gouvernement fédéral ou le CRTC pourraient exiger que les FST offrent à bas prix ou gratuitement aux Canadiens des fonctionnalités permettant de réduire ou de prévenir les appels frauduleux passant par leurs réseaux. Par ailleurs, le Comité a remarqué que l'industrie des télécommunications est en grande partie responsable du développement de ces fonctionnalités. Étant donné que, dans la lutte contre la fraude, il y a une « course aux armements », les FST doivent avoir des incitations pour investir dans le développement de contre-mesures. Le gouvernement fédéral et le CRTC doivent donc trouver un juste équilibre pour ce qui est de rendre ces fonctions disponibles au plus grand nombre tout en favorisant l'innovation. Par conséquent, le Comité recommande :

Recommandation 8

Que le gouvernement du Canada favorise le développement par l'industrie de solutions pour contrer les appels frauduleux à un coût raisonnable pour les consommateurs.

Recommandation 9

Que le gouvernement du Canada encourage le Conseil de la radiodiffusion et des télécommunications canadiennes à suivre de près le coût des solutions de l'industrie pour contrer les appels frauduleux et à en tenir compte dans les décisions ayant une incidence sur l'abordabilité des services de télécommunications.

Le gouvernement fédéral devrait examiner les dispositions actuelles en matière de droit pénal pour voir si elles permettent de protéger efficacement les Canadiens contre les appels frauduleux, y compris les appels automatisés. Même si cet examen pourrait déboucher sur le dépôt d'une mesure législative interdisant spécifiquement d'escroquer ou de tenter d'escroquer des personnes par le biais des communications vocales, le Comité n'appuie pas la proposition consistant à obliger le CRTC à appliquer la législation pénale. Au-delà des difficultés d'ordre pratique liées à la mise en place de moyens de

mener des enquêtes criminelles, cela pourrait détourner le CRTC de ce qui devrait être son principal objectif, soit permettre aux Canadiens d'utiliser leur téléphone en toute sécurité, en coordonnant le travail des FST, notamment au moyen de mesures réglementaires. Par conséquent, le Comité recommande :

Recommandation 10

Que le gouvernement du Canada revoie les mesures législatives concernant la fraude pour s'assurer qu'elles interdisent de manière adéquate et explicite les appels frauduleux, y compris ceux effectués à l'aide d'un composeur-messager automatique.

Recommandation 11

Que le gouvernement du Canada revoie les directives données au Conseil de la radiodiffusion et des télécommunications canadiennes pour s'assurer que la protection contre la fraude au moyen de télécommunications vocales est suffisamment intégrée dans la politique canadienne des télécommunications.

Tout comme M. Randall-Chong, la section canadienne de l'Internet Society et le CDIP, le Comité encourage le CRTC à mener une enquête publique officielle sur le portage non autorisé. Les autorités fédérales ainsi que les FST, les autorités financières et d'autres acteurs doivent s'attaquer à cette nouvelle menace et présenter rapidement des mesures pour l'éliminer. Les témoignages qu'a recueillis le Comité montrent qu'il est nécessaire de trouver un nouvel équilibre entre la concurrence et la sécurité en ce qui concerne le portage. Dans la mesure du possible, la réglementation et les contre-mesures doivent être élaborées de manière transparente et en sollicitant la participation du public, y compris des victimes de transferts non autorisés de cartes SIM.

Recommandation 12

Que le gouvernement du Canada appuie la réalisation d'une enquête publique sur le portage non autorisé par le Conseil de la radiodiffusion et des télécommunications canadiennes.

Recommandation 13

Que le gouvernement du Canada présente un projet de loi pour protéger les Canadiens contre le portage non autorisé si le Conseil de la radiodiffusion et des télécommunications canadiennes n'amorce pas d'enquête publique sur le portage non autorisé dans un délai de six mois.

La pandémie de COVID-19 menace les vies et les moyens de subsistance, et met en péril l'économie canadienne. Le gouvernement fédéral doit agir pour empêcher que les Canadiens subissent d'autres préjudices. Dans l'immédiat, la sensibilisation du public demeure le moyen le plus efficace de contrer la fraude liée à la COVID-19. Comme le temps presse, le gouvernement fédéral doit intervenir sans tarder.

Recommandation 14

Que le gouvernement du Canada lance une campagne de sensibilisation du public d'un mois dans les médias locaux et nationaux pour mettre les Canadiens en garde contre la fraude liée à la COVID-19.

Recommandation 15

Que le gouvernement du Canada s'emploie à devenir un chef de file de la prévention de la fraude sur la scène internationale en évaluant, dans un an, les progrès accomplis par rapport aux présentes recommandations, et que tous les ministres compétents présentent à la Chambre des communes un rapport en ce sens, qui sera ensuite renvoyé au comité pertinent.

ANNEXE A
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Bell Canada	2020/03/10	7
Jonathan Daniels, vice-président Droit réglementaire		
Conseil de la radiodiffusion et des télécommunications canadiennes	2020/03/10	7
Ian Scott, président et dirigeant principal		
Steven Harroun, chef de l'application de la conformité et enquêtes		
Alain Garneau, directeur Mise en application, Télécommunications, Secteur de la conformité et des enquêtes		
Gendarmerie royale du Canada	2020/03/10	7
Eric Slinn, commissaire adjoint Opérations criminelles de la Police fédérale		
Guy Paul Larocque, officier responsable intérimaire Centre antifraude du Canada		
Rogers Communications Inc.	2020/03/10	7
Howard Slawner, vice-président Affaires réglementaires, Télécommunications		
Deborah Evans, chef de la protection de la vie privée		
Société Telus Communications	2020/03/10	7
John MacKenzie, directeur Affaires réglementaires		
Jérôme Birot, vice-président Développement et exploitation, Voix et services		

Organismes et individus	Date	Réunion
À titre personnel	2020/03/12	8
Randall Baran-Chong, co-fondateur Canadian SIM-swap Victims United		
Centre pour la défense de l'intérêt public	2020/03/12	8
John Lawford, directeur exécutif et avocat général		
Internet Society Canada Chapter	2020/03/12	8
Matthew Gamble, directeur		
Réseau canadien pour la prévention du mauvais traitement des aînés	2020/03/12	8
Kate Schroeder, membre du conseil d'administration		
Autorité des marchés financiers	2020/05/20	16
Jean-François Fortin, directeur général, Contrôle des marchés		
Christian Desjardins, directeur de l'évaluation et du renseignement		
Autorité canadienne pour les enregistrements Internet	2020/05/20	16
Albert Chang, conseiller juridique		
Dave Chiswell, vice-président, Développement de produits		
Byron Holland, président et chef de la direction		
Centre de la sécurité des télécommunications	2020/05/20	16
Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité		
Nuance Communications	2020/05/20	16
Simon Marchand, examinateur de fraude certifié et administrateur agréé, Biométrie et sécurité		
Gendarmerie royale du Canada	2020/05/20	16
Guy Paul Larocque, officier responsable intérimaire, Centre antifraude du Canada		
Eric Slinn, commissaire adjoint, Opérations criminelles de la Police fédérale		

ANNEXE B
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Association canadienne de l'électricité

Association canadienne des télécommunications sans fil

Baran-Chong, Randall

COMsolve Inc.

Réseau canadien pour la prévention du mauvais traitement des aînés

Société TELUS Communications

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions n^{os} 7, 8, 16, 27 et 29) de la 43^{e} législature, première session, et (réunion n^{o} 2) de la 43^{e} législature, deuxième session est déposé.

Respectueusement soumis,

La présidente,
Sherry Romanado