CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

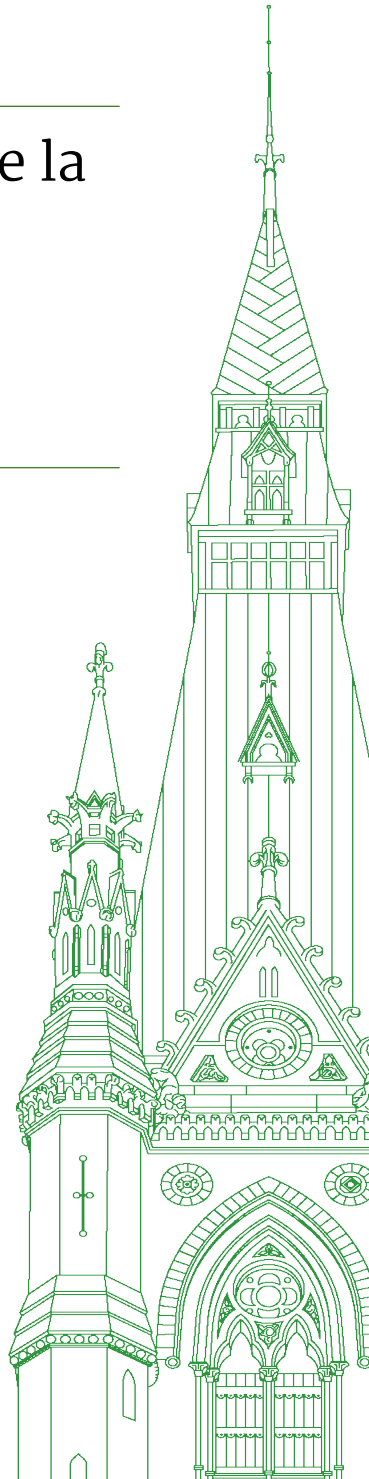
45e LÉGISLATURE, 1re SESSION

Comité permanent de l'industrie et de la technologie

TÉMOIGNAGES

NUMÉRO 042

Le jeudi 4 juin 2026



Président : Ben Carr

Comité permanent de l'industrie et de la technologie

Le jeudi 4 juin 2026

● (1105)

[*Traduction*]

Le président (Ben Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour à tous.

[*Français*]

Je vous souhaite la bienvenue.

J'espère que tout le monde a passé une bonne semaine jusqu'à maintenant.

[*Traduction*]

Nous allons entamer ce matin une nouvelle étude qui revêt une importance considérable pour les Canadiens partout au pays.

J'ai un petit rappel à faire aux témoins.

Si votre oreillette est branchée, veuillez la poser sur l'autocollant devant vous quand vous ne la portez pas sur votre oreille afin de protéger la santé et le bien-être de nos interprètes.

[*Français*]

Je peux confirmer que nous avons fait tous les tests nécessaires et que la vidéo et le son fonctionnent bien.

[*Traduction*]

Chers collègues, nous aurons une heure pour entendre les témoins qui comparaissent devant nous ce matin, puis nous siégerons à huis clos afin de mettre la dernière main, je l'espère, à la deuxième version du rapport de notre étude sur les fabricants de moules à laquelle nous avons travaillé.

Sur ce, j'aimerais souhaiter la bienvenue aux témoins qui sont parmi nous.

Nous accueillons M. Anthony Ostler, président et chef de la direction, ainsi que M. Hartland Elcock, avocat général adjoint et vice-président de l'Association des banquiers canadiens.

Messieurs, bienvenue.

Nous accueillons M. Eric Smith, vice-président principal de l'Association canadienne des télécommunications.

Bienvenue, monsieur.

Nous accueillons M. Carey Frey, chef de la sécurité chez Telus.

Bienvenue, monsieur Frey.

Messieurs les témoins, vous disposerez chacun d'au plus cinq minutes pour vos déclarations liminaires. Vous n'êtes pas tenus d'utiliser tout ce temps, mais vous y avez droit, bien sûr.

À l'issue des déclarations liminaires de nos trois témoins, nous donnerons la parole aux députés ici présents, issus des différents partis politiques reconnus, pour entamer la séance de questions et réponses.

Pour l'Association des banquiers canadiens, monsieur Ostler, je suppose que c'est vous qui prendrez la parole. Je vous en prie, monsieur.

[*Français*]

Anthony Ostler (président et chef de la direction, Association des banquiers canadiens): Merci beaucoup.

Bonjour.

Je remercie grandement le Comité de nous offrir cette occasion de participer à ses travaux sur la fraude financière et les arnaques au Canada.

Je m'appelle Anthony Ostler et je suis président et chef de la direction de l'Association des banquiers canadiens, ou ABC. Je suis accompagné aujourd'hui par Hartland Elcock, directeur juridique adjoint et vice-président à l'ABC.

L'ABC est la voix de plus de 60 banques canadiennes et étrangères actives au Canada. Elle appuie l'adoption de politiques publiques pour maintenir un système bancaire solide et dynamique capable d'aider les Canadiennes et les Canadiens à atteindre leurs objectifs financiers.

[*Traduction*]

La lutte contre les crimes financiers est une priorité absolue pour l'ABC. Comme membre du conseil d'administration de l'International Banking Federation, l'IBFed, j'ai pu constater de première main, lors de notre réunion de novembre 2022 à Sydney, comment l'Australie réagissait en misant de plus en plus sur une approche intersectorielle public-privé. Les cybercriminels exploitaient la connectivité numérique, à un rythme qui s'était accéléré pendant la pandémie, pour voler des particuliers et blanchir les produits de leurs activités, finançant ainsi souvent le crime organisé, des États malveillants et le terrorisme.

En 2023, le Canada continuait d'enregistrer une hausse des fraudes et des escroqueries, tandis que l'Australie commençait à les réduire grâce à son programme intersectoriel. Début 2024, il était clair que nous devions appliquer ces enseignements au Canada. Il y a deux ans, l'ABC a réuni une cinquantaine de partenaires des secteurs public et privé, notamment des organes de réglementation, des institutions financières, des fournisseurs de services de télécommunication, des corps policiers et des plateformes numériques afin de créer la Coalition canadienne antifraude. La Coalition coordonne les efforts d'éducation, de sensibilisation et de prévention, notamment l'élaboration d'une taxonomie nationale, un projet pilote de détection des fraudes et la campagne en cours « Ensemble contre la fraude ».

Je suis ici en ma qualité de chef de la direction de l'ABC, mais je préside toujours le comité directeur de la Coalition, désormais hébergée à l'Échange canadien de menaces cybernétiques.

L'ABC a également transmis des observations à Finances Canada en faveur d'une stratégie nationale antifraude. Nous souscrivons à une approche fédérale intersectorielle visant à renforcer la protection des consommateurs et à consolider la confiance dans l'économie numérique canadienne, en commençant par les secteurs des services financiers, des télécommunications et des plateformes numériques. Ces secteurs se recoupent tout au long du cycle de vie de la fraude, et le Centre antifraude du Canada a constaté que plus de 85 % des pertes financières dues à la fraude peuvent être attribuées aux canaux de télécommunications ou numériques. Une action coordonnée entre les secteurs, associée à un comportement responsable de la part des consommateurs, est essentielle pour réduire les préjudices liés à la fraude subis par les Canadiens.

En janvier 2025, je suis devenu président de l'IBFed et j'ai lancé un groupe de travail chargé de diffuser les pratiques exemplaires internationales en matière de fraude et d'escroquerie. En mars, j'ai conduit une délégation de l'IBFed au Sommet mondial sur la fraude organisé par les Nations unies et Interpol à Vienne. Parmi les principaux résultats, citons un appel à l'action adressé aux pays et un cadre mondial de partenariat public-privé destiné aux institutions. Trente-sept États membres, dont le Canada, ont entériné cet appel à l'action, tandis que l'ABC, l'IBFed, des gouvernements, des plateformes numériques, des ONG et d'autres organisations ont approuvé ce cadre. Ce travail international se poursuit sous la forme de projets pilotes visant à renforcer les mesures de protection contre la fraude.

Comme le montrent l'expérience de l'Australie et les récentes recherches sur l'avenir de l'échange de renseignements financiers, l'échange d'information entre les secteurs est essentiel. S'appuyant sur une gouvernance solide et des garde-fous protégeant la vie privée, cet échange d'information volontaire et conditionnel permettra au Canada de lutter contre la fraude tout au long de son cycle de vie.

La sensibilisation et l'éducation du public sont également essentielles à une stratégie nationale antifraude efficace. Elles favorisent une détection plus précoce, de meilleures décisions, la prévention et un signalement amélioré. Nous encourageons le gouvernement à soutenir davantage la campagne multisectorielle « Ensemble contre la fraude » de la coalition. Une stratégie pangouvernementale peut aider les organisations à mettre leur savoir-faire à contribution, mais les rôles et les mandats au sein de ce système doivent être clairement définis. Une meilleure coordination entre les forces de l'ordre canadiennes à tous les niveaux et avec les partenaires internationaux nécessitera un modèle opérationnel plus clair, fondé sur le renseignement.

Nous estimons également que le Centre antifraude du Canada devrait rester la principale plaque tournante du Canada pour le signalement des fraudes et la collecte de renseignements. Comme je l'ai souligné, l'environnement de la criminalité financière évolue rapidement, et le Régime canadien de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes doit suivre le rythme. C'est pourquoi nous voyons d'un bon oeil la création par le gouvernement de l'Agence contre les crimes financiers qui devrait aider le Canada à lutter contre la criminalité financière complexe. Au fil de la mise sur pied de l'Agence, l'ABC soutient l'idée qu'elle devienne le chef de file national des opérations de lutte contre les crimes financiers en jouant un rôle de coordination et de définition des priorités afin d'orienter l'évolution continue du régime de lutte contre le blanchiment d'argent vers un cadre davantage axé sur les risques et adapté à ses objectifs.

En conclusion, l'ABC est reconnaissante de l'occasion qui lui est offerte de contribuer à l'étude du Comité. Les banques canadiennes connaissent de première main le lourd fardeau financier et émotionnel que la fraude fait peser sur leurs clients. Elles investissent massivement dans la prévention de la fraude, la formation en cybersécurité et la sensibilisation des clients, mais aucune organisation ni aucun secteur ne peut à lui seul endiguer efficacement cette vague. Si nous travaillons ensemble, au sein du gouvernement et de tous les secteurs, de manière concertée pour faire face à cette menace, nous pourrons, ensemble, protéger les Canadiens, les entreprises canadiennes et l'économie.

● (1110)

Nous sommes impatients de répondre à vos questions.

Le président: Merci beaucoup, monsieur Ostler. Vous avez manifestement minuté votre intervention, car vous avez respecté le temps imparti à la seconde près.

Monsieur Smith, je vous cède la parole.

Eric Smith (vice-président principal, Association canadienne des télécommunications): Je vais essayer de faire cinq secondes de mieux.

Merci, monsieur le président, et mesdames et messieurs, de m'offrir l'occasion de comparaître devant vous au nom de l'Association canadienne des télécommunications.

Notre association s'engage à bâtir un avenir meilleur pour les Canadiens grâce à la connectivité. Nos membres comprennent des fournisseurs de services de télécommunication, des fabricants d'équipements et d'autres organisations qui investissent dans les réseaux de télécommunications de renommée mondiale du Canada, les construisent, les entretiennent et les exploitent.

La fraude est un problème grave. Elle cause un préjudice financier, mine la confiance dans les services numériques et touche les Canadiens dans toutes les régions du pays. Le secteur des télécommunications prend ce défi très au sérieux. Nos membres investissent des ressources considérables dans la prévention de la fraude et s'efforcent sans relâche de détecter les menaces émergentes, de renforcer la protection des réseaux, de soutenir les enquêtes des forces de l'ordre et de sensibiliser les Canadiens aux fraudes.

Parmi les mesures prises pour aider les Canadiens, citons le blocage de certains types d'appels; les outils de prévention de l'usurpation d'identité de l'appelant, comme les programmes de blocage de numéros sortants et la mise en œuvre de la norme STIR/SHAKEN; les capacités de traçage des appels pour aider à trouver l'origine des appels frauduleux; l'analyse au niveau du réseau pour détecter et signaler les communications suspectes; les systèmes de signalement des pourriels; les mesures de protection de l'identité et des comptes; ainsi qu'une collaboration continue avec les forces de l'ordre et les organismes gouvernementaux.

Parallèlement, il est important de reconnaître que la fraude est un défi à l'échelle de l'écosystème. Les réseaux de télécommunications sont souvent la voie par laquelle transitent les communications frauduleuses, mais ce n'est généralement pas là que les fraudes prennent leur source, que le contenu frauduleux est créé ou que les pertes financières se produisent en définitive. Aujourd'hui, les fraudeurs utilisent fréquemment des plateformes numériques pour concevoir, optimiser, amplifier et mettre en œuvre leurs stratagèmes, ou recourent à des applications de messagerie par contournement pour communiquer avec leurs victimes potentielles. Bien que les réseaux de télécommunications servent à acheminer ces communications, les fournisseurs de services de télécommunication n'ont généralement pas accès à leur contenu.

Pour reprendre une analogie courante, les fournisseurs de services de télécommunication acheminent l'enveloppe, mais ils ne lisent pas le courrier.

Ces fournisseurs sont également soumis à des obligations légales qui limitent leur capacité à interférer avec les communications. L'article 36 de la Loi sur les télécommunications leur interdit de bloquer de leur propre chef des communications sans autorisation expresse du Conseil de la radiodiffusion et des télécommunications canadiennes. Cette restriction est un élément fondamental du cadre canadien de neutralité du Net et vise à garantir que les mesures de lutte contre la fraude ne bloquent pas par inadvertance le trafic légal ni n'interfèrent avec les communications essentielles.

Certaines mesures déjà mentionnées, prises par notre secteur pour lutter contre la fraude, n'ont pu être mises en œuvre qu'après un examen minutieux par le CRTC, et ce, uniquement après que le Conseil eut été convaincu que ces mesures seraient efficaces, qu'elles serviraient l'intérêt public et qu'elles ne compromettraient pas le trafic légitime.

Alors que le gouvernement élabore sa Stratégie nationale antifraude, nous estimons qu'il devrait se concentrer sur les quatre priorités suivantes.

Premièrement, renforcer la coordination et l'échange d'information entre les différents secteurs. La prévention de la fraude est plus efficace lorsque les fournisseurs de services de télécommunication, les institutions financières, les plateformes numériques, les organismes gouvernementaux et les forces de l'ordre collaborent et s'échangent des renseignements.

Deuxièmement, renforcer la coopération internationale. De nombreuses opérations frauduleuses, voire la plupart, trouvent leur origine hors des frontières du Canada, ce qui rend la collaboration transfrontalière essentielle.

Troisièmement, sensibiliser et éduquer davantage le public. La plupart des fraudes reposent en fin de compte sur l'ingénierie sociale. Aider les Canadiens à reconnaître les fraudes reste l'un des outils les plus efficaces à notre disposition.

Quatrièmement, veiller à ce que toute nouvelle mesure de lutte contre la fraude envisagée vienne compléter les cadres réglementaires existants et évite les doublons inutiles. S'appuyer sur les pouvoirs existants, l'expertise et les initiatives menées par le secteur permettra de garantir que les ressources soient consacrées à la prévention de la fraude au lieu de gérer les obligations de conformité qui se chevauchent.

Pour conclure, le secteur des télécommunications s'engage à faire partie de la solution. Nos membres continueront d'investir dans la protection des réseaux, de collaborer avec des partenaires de tous les secteurs et de soutenir les efforts visant à protéger les Canadiens contre la fraude. Nous nous réjouissons de travailler avec le gouvernement, les organes de réglementation, les forces de l'ordre et les autres parties prenantes afin d'élaborer une Stratégie nationale antifraude qui soit pratique et efficace, et qui prend en compte le partage des responsabilités nécessaire pour faire face à cette menace en constante évolution.

Merci de votre attention. Je serai heureux de répondre à vos questions.

● (1115)

Le président: Merci beaucoup, monsieur Smith.

Monsieur Frey, je vous cède la parole pour cinq minutes maximum.

Carey Frey (chef de la sécurité, Telus): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de m'offrir l'occasion de comparaître devant vous.

Je m'appelle Carey Frey et j'occupe le poste de chef de la sécurité chez TELUS.

Avec plus de 21 millions de connexions de télécommunications, nous prenons très au sérieux notre responsabilité, non seulement de connecter les Canadiens, mais de les protéger.

Je tiens à faire d'abord un simple constat. La fraude est désormais un élément central de notre économie. Elle est hautement organisée, d'envergure internationale et connaît une croissance à un rythme qu'aucun secteur ni aucun gouvernement ne peut endiguer à lui seul.

Bien que TELUS lutte quotidiennement contre la fraude, je tiens à vous présenter un exemple illustrant le type de fraude auquel le Canada est confronté aujourd'hui et à vous dire que le seul modèle permettant de la combattre repose sur la collaboration entre le secteur privé, les forces de l'ordre et le gouvernement.

En novembre dernier, TELUS a reçu un signalement concernant un SMS suspect circulant sur des téléphones à Toronto. Ces messages contenaient des liens conçus pour usurper l'identité de sites Web de paiement légitimes. Nous avons lancé une enquête et n'avons rien trouvé. Il n'y avait aucune trace de ces messages dans les journaux de notre réseau. Cette absence était en soi un indice. Nous soupçonnions d'avoir affaire à un SMS Blaster, c'est-à-dire un dispositif de télécommunication complexe qui imite une tour cellulaire légitime et inonde de SMS frauduleux les appareils mobiles connectés à proximité. Il s'agit d'une cybermenace portable que des criminels utilisent pour semer le chaos et escroquer des victimes sans méfiance. Nous n'avions encore jamais vu de SMS Blaster déployé au Canada.

Finalement, il est devenu évident que quelqu'un se déplaçait avec ce dispositif dans les environs de Toronto, parcourant les quartiers et ciblant des milliers de téléphones à la fois. Le secteur a contacté la police de Toronto pour signaler ces SMS et a également signalé l'utilisation non autorisée des ondes au ministère de l'Innovation, des Sciences et du Développement économique. Ces signalements ont donné le coup d'envoi d'une enquête de cinq mois baptisée « Projet Lighthouse ».

Grâce aux efforts d'échange d'information entre le secteur et les forces de l'ordre, trois individus ont été arrêtés et sont inculpés de 44 chefs d'accusation. Au total, ces individus sont responsables de plus de 13 millions de perturbations du réseau.

Si l'objectif premier des criminels était de commettre des fraudes, leur technologie constitue également un nouveau type de cybermenace prépositionnée particulièrement destructrice. Ces dispositifs peuvent perturber les appels au 911, provoquer des pannes de réseau et servir à lancer des cyberattaques contre des infrastructures essentielles depuis l'intérieur des frontières canadiennes. Ils peuvent même servir à installer des logiciels malveillants sur des téléphones intelligents à proximité. Ces nouveaux outils de fraude internationale font peser sur les Canadiens des menaces qui vont bien au-delà des pertes financières. Nous devons localiser et neutraliser ces technologies au lieu de nous contenter de protéger nos citoyens contre leur utilisation criminelle.

Le projet Lighthouse a été couronné de succès non pas grâce à une nouvelle loi, mais grâce à une collaboration soutenue entre les principales institutions financières, les fournisseurs de services de télécommunication canadiens, trois corps policiers et plusieurs agences fédérales. Nous avons réussi parce que nous avons instauré la confiance, l'échange d'information et la volonté d'agir parmi tous les partenaires. C'est le modèle que le Canada devrait suivre.

Le Canada dispose déjà d'une grande partie de ce dont il a besoin pour lutter plus efficacement contre la fraude. Le Centre antifraude du Canada, les organes de réglementation sectoriels, les forces de l'ordre et les coalitions du secteur privé sont déjà en place. Ce qui manque, c'est une force de coordination centrale qui veille à ce que les meilleurs outils et renseignements parviennent à ceux qui en ont besoin. C'est un rôle que seul le gouvernement fédéral peut jouer, et il devrait s'y consacrer pleinement avant de réclamer de nouveaux pouvoirs.

Le projet Lighthouse nous a enseigné quatre leçons que le Parlement peut mettre en œuvre pour lutter contre la fraude.

Premièrement, nous devons renforcer la coopération entre les acteurs du secteur privé et les pouvoirs publics, ainsi qu'à l'échelle mondiale, afin de démanteler les réseaux frauduleux qui exploitent nos plateformes numériques. Tenter de bloquer chaque cas de fraude distinct revient à jouer à un jeu de la taupe sans fin et futile face à la criminalité internationale. La plupart des fraudes numériques visant les Canadiens sont perpétrées depuis l'étranger, ce qui rend indispensable une collaboration internationale solide pour y mettre un terme. Au Canada, le gouvernement fédéral est le mieux placé pour diriger les efforts de prévention, de démantèlement et de lutte contre la fraude dans les secteurs public et privé.

Deuxièmement, les fournisseurs de services de télécommunication pourraient bloquer davantage de trafic frauduleux sur nos réseaux, mais aujourd'hui, le risque de responsabilité limite nos possibilités d'action. Des dispositions d'exonération protégeant ceux qui prennent de bonne foi des mesures antifraude contribueraient à protéger les Canadiens sans coût supplémentaire pour les contribuables.

Troisièmement, il faut doter les forces de l'ordre d'un mandat explicite et des ressources nécessaires pour appréhender efficacement les auteurs de fraudes et démanteler leurs dispositifs techniques.

Quatrièmement et enfin, le Parlement devrait examiner les politiques en vigueur et la manière dont elles facilitent involontairement la fraude. Par exemple, les règlements du CRTC relatifs à la confidentialité des clients restreignent l'échange de renseignements entre les différents secteurs. Un autre exemple est celui des règles du CRTC concernant le déverrouillage de dispositifs, qui facilitent la tâche des criminels souhaitant escroquer les Canadiens de leurs téléphones intelligents, les laissant avec des dettes importantes et une cote de crédit détériorée.

● (1120)

Pour conclure, TELUS constate chaque jour des fraudes persistantes à l'encontre de nos clients et, pour être honnête, à l'encontre de tous les Canadiens. Ce phénomène prend de l'ampleur, mais il est possible de le combattre si nous agissons de manière coordonnée et dans l'urgence. TELUS est prête à s'associer à cet effort.

Je suis impatient de répondre à vos questions. Merci de votre attention.

Le président: Merci beaucoup, monsieur Frey.

Nous allons passer à la première série de questions.

Madame Dancho, la parole est à vous pendant six minutes.

Raquel Dancho (Kildonan—St. Paul, PCC): Merci, monsieur le président.

C'est un honneur de lancer cette importante étude. Je sais que tous les coins du pays ont été touchés par des fraudes et des escroqueries. Les députés se sont réunis au sein du Comité dans un esprit de collaboration afin de formuler des recommandations à l'intention du gouvernement, de manière à protéger les Canadiens, leurs finances et, comme on l'a souligné dans les témoignages, leur sécurité ainsi que leur accès au 911 et à d'autres ressources.

Merci aux témoins d'être ici. Vos témoignages sont très importants pour nous. J'ai plusieurs questions à poser à chacun d'entre vous, mais je tiens d'abord à expliquer en partie ce qui m'a incitée à mener cette étude.

Il y a environ un an, nous avons reçu un appel à mon bureau de circonscription. L'afficheur indiquait « Services bancaires en ligne de la RBC ». Mon assistante a répondu. L'appel semblait tout à fait légitime, mais quelque chose lui semblait louche. N'étant pas sûre de la situation, elle a raccroché et m'a appelée. Nous avons décidé d'appeler directement la RBC pour vérifier. Comme nous nous y attendions, il s'agissait bien d'une arnaque. Mon assistante est jeune et au fait de l'actualité. On dit souvent que si l'on ne possède pas ces qualités, on est plus vulnérable, mais elle a déclaré qu'il lui aurait été extrêmement facile de fournir les renseignements demandés. L'interlocuteur était très convaincant. Comment les gens sont-ils censés se défendre contre cela?

Je voudrais vous donner la parole, monsieur Frey. Pouvez-vous expliquer comment cela a pu se produire dans mon bureau et au domicile d'autres Canadiens? Le nom de la banque figurait sur l'afficheur, mais de manière manifestement frauduleuse. Comment cela se produit-il, et comment peut-on l'empêcher?

Carey Frey: La triste réalité est qu'il est possible d'usurper l'identité de l'expéditeur d'appels téléphoniques et de SMS. C'est dû aux limites de la sécurité de l'infrastructure de télécommunications, mise en place il y a plusieurs décennies et sur laquelle nous continuons de nous appuyer, à ses niveaux les plus fondamentaux, partout dans le monde.

Notre secteur a mis au point de nombreux nouveaux protocoles sécurisés pour contrer l'usurpation d'identité. Cependant, les pays doivent tous les adopter. Les pays qui ne les adoptent pas offrent un refuge aux criminels, qui acheminent des appels et des SMS depuis ces territoires, que nous devons ensuite traiter sur les réseaux canadiens. Nous bloquons la grande majorité de ces communications — probablement plus de 99 % des appels téléphoniques et SMS frauduleux et d'usurpation d'identité —, mais certains parviennent tout de même à passer en nombre suffisamment important pour alimenter toute une industrie de l'escroquerie.

Raquel Dancho: Merci beaucoup. Vous dites qu'une partie du problème ne relève pas nécessairement de votre contrôle chez TELUS. Vous n'êtes pas limités par la loi. Vous avez fait allusion à certaines contraintes législatives, mais, pour ce problème précis, il n'y a pas de modification législative ni de mesure qu'on puisse prendre à l'échelle nationale pour y mettre fin. Vous faites beaucoup d'efforts, mais vous dites que, comme ces appels proviennent de l'étranger et transitent par votre réseau, cela pose certains problèmes. Est-ce exact?

Carey Frey: Oui. C'est exact.

Raquel Dancho: D'accord.

Avez-vous une recommandation à nous faire qui vous aiderait à empêcher cela?

Carey Frey: Je ne vois pas de recommandation pour l'empêcher. C'est une réalité de l'infrastructure des télécommunications à l'échelle mondiale. Les options que nous pourrions envisager consistent à communiquer par d'autres moyens ou, comme je l'ai dit dans mon témoignage, à réexaminer la possibilité d'une collaboration internationale renforcée dans ce domaine et à chercher à moderniser les réseaux dans d'autres pays afin qu'ils délaissent les anciennes versions de leur infrastructure de télécommunications, qui constituent la vulnérabilité permettant une grande partie de cette activité.

Raquel Dancho: Pensez-vous que l'intelligence artificielle puisse jouer un rôle, tant dans l'aggravation de la menace que dans la lutte contre celle-ci? Cela serait-il utile dans ce scénario ou dans d'autres situations similaires?

Carey Frey: Oui, ce serait utile. Ma préoccupation générale est que l'exemple que vous avez cité, que je connais bien, ne représente qu'une infime minorité des sources de fraude à grande échelle si l'on considère le montant total des pertes financières subies au Canada. Bien qu'il s'agisse d'un aspect important sur lequel il faut continuer à se concentrer, on trouve de nombreux autres exemples d'abus de nos plateformes numériques: non seulement les infrastructures de télécommunications, mais les grandes plateformes infonuagiques et les applications sur nos téléphones portables que les fraudeurs utilisent également pour commettre ces fraudes.

C'est un fait: même si nous supprimions les parties vulnérables de notre infrastructure mondiale de télécommunications, ils réorienteraient tout simplement leurs activités à 100 % vers les plateformes numériques. Nous devons veiller à adopter une approche globale dans notre stratégie.

● (1125)

Raquel Dancho: Au crédit des plateformes de télécommunications, j'ai remarqué, comme d'autres l'ont peut-être fait aussi, que depuis un an, lors d'un appel entrant, un message indique « Appel bloqué: fraude probable », ou un message du genre. Je n'avais jamais vu ça, mais c'est désormais assez fréquent. C'est très apprécié, mais comme vous l'avez dit, il semble que certains appels parviennent encore à se faufiler.

Monsieur Smith, aviez-vous quelque chose à ajouter à cette discussion concernant la prévention, une modification législative ou toute autre mesure que vous estimez utile?

Eric Smith: Non, je pense que je vais simplement compléter ce que M. Frey a dit. Certains outils adoptés par les fournisseurs de services de télécommunication au Canada et ailleurs dans le monde visent précisément ce genre de problèmes. En effet, en collaboration avec le CRTC, ils ont mis en œuvre la norme STIR/SHAKEN qui permet de vérifier l'identité de l'appelant, mais pas l'objet de l'appel. Cependant, comme on l'a dit, si cette technologie n'est pas adoptée dans le pays d'où provient l'appel, par exemple, elle ne remplit pas cette fonction.

Les fournisseurs mettent aussi en place d'autres programmes, notamment les programmes de blocage de numéros sortants. Par exemple, si une banque dispose de numéros commençant par 1-800 qu'elle n'utilise pas pour ses appels sortants — ces numéros servent uniquement aux clients à communiquer avec le service à la clientèle —, elle peut les enregistrer auprès des fournisseurs de services de télécommunication, de sorte que si un appel semble provenir de ce numéro, il soit automatiquement bloqué.

Les entreprises prennent différentes mesures, mais comme on l'a dit, dès que l'on comble une faille, les fraudeurs trouvent d'autres moyens. On observe de plus en plus de cas sur les réseaux sociaux, les plateformes numériques et ce genre de supports.

Raquel Dancho: Merci beaucoup.

Le président: Madame O'Rourke, la parole est à vous pour six minutes.

Dominique O'Rourke (Guelph, Lib.): Merci beaucoup, monsieur le président. Je vous en suis reconnaissante.

En 2024, l'Association des banquiers canadiens, les grandes banques, les fournisseurs de services de télécommunication, les entreprises technologiques, les forces de l'ordre et le gouvernement du Canada ont formé la Coalition canadienne antifraude afin de faciliter une réponse coordonnée face aux fraudes.

Monsieur Ostler, je me demande quels résultats concrets la Coalition a obtenus à ce jour. Comment ces résultats sont-ils mesurés? Comment la Coalition va-t-elle collaborer avec la nouvelle Agence contre les crimes financiers annoncée par le gouvernement?

Anthony Ostler: Les progrès de la Coalition portent sur plusieurs éléments. Il est essentiel de noter que la Coalition repose sur le volontariat. L'une de nos plus grandes réalisations a sans doute été le lancement, à l'automne 2025, de notre campagne de sensibilisation intitulée « Ensemble contre la fraude ». Le slogan de cette campagne est « Arrêtez. Vérifiez. Parlez-en. »

L'objectif est d'aider les Canadiens à acquérir davantage de compétences pour mieux se protéger. En réalité, si l'on se concentre sur un seul type de vecteur ou de mode d'escroquerie, les malfaiteurs, comme ces experts ont dit, changeront de méthode. Voilà pourquoi nous tentons d'aider les Canadiens à acquérir de meilleures compétences.

De plus, nous avons conçu une taxonomie du partage d'informations afin de cerner les besoins des entreprises de télécommunications, des banques, des plateformes numériques et des forces de l'ordre. Ainsi, nous disposerons d'une version unique de la vérité lorsque nous mettrons en place, le cas échéant, un système formel d'échange d'informations.

Enfin, nous avons établi un excellent partenariat avec le secteur des télécommunications dans le cadre d'un projet pilote. Une des grandes entreprises de télécommunications et deux ou trois de mes membres mènent actuellement un projet pilote sur le partage d'informations. Au fil de leurs travaux, ils ont repéré des méta-informations concernant les auteurs d'escroqueries. Ce qui est intéressant dans ce projet, c'est qu'ils peuvent, par exemple, repérer un numéro de téléphone ayant fait l'objet d'une utilisation frauduleuse chez une entreprise de télécommunications, puis découvrir qu'il a été utilisé avec une fausse identité auprès d'une banque. Ils ont alors pu en déduire que cette personne devait s'en servir comme compte mule. Nous pouvons alors bloquer le compte, et ce genre de chose.

Ce projet pilote s'est révélé vraiment très intéressant. Nous tirons parti de l'infrastructure de l'industrie des télécommunications pour faciliter le partage sécurisé de ces informations. Ce n'est pas une solution durable. Elle n'est pas automatisée. Cependant, lorsque les participants au projet pilote comparent les informations, l'effet de réseau généré par la présence de plusieurs parties prenantes est considérable. Nous espérons prendre appui sur cela maintenant que nous avons de la taxonomie, et faire progresser l'échange d'informations de manière plus formelle.

Je pense qu'un élément essentiel consistera également à intégrer les plateformes numériques dans une perspective d'échange d'informations. Les plateformes numériques font partie de la coalition depuis le début et ont joué un rôle clé dans la sensibilisation, notamment au moyen de programmes comme celui que Meta mène actuellement dans le contexte de la Coupe du monde pour tenter d'empêcher les gens d'être victimes d'escroqueries. C'est un volet particulier de notre campagne.

Nous avons vraiment salué cet investissement de tous les secteurs dans la campagne de sensibilisation, mais je dirais qu'il reste encore beaucoup à faire. C'est pourquoi nous nous réjouissons de notre présence à ce comité et de notre participation à cette étude.

L'Australie a réduit les escroqueries de 30 % au cours des trois dernières années. Le nombre d'escroqueries signalées chez nous a augmenté de 32 %. Depuis 2022, nous avons une hausse de 32 %; eux, une baisse de 30 %. C'est le seul pays qui, au cours des trois dernières années, a réussi à réduire le nombre d'escroqueries. Ils y sont parvenus grâce à un programme intersectoriel piloté par le gouvernement. Cela a permis non seulement de rassembler les différents secteurs, mais aussi les forces de l'ordre et la justice, par l'intermédiaire des procureurs de la Couronne et d'autres instances semblables. Il s'agit d'une approche globale, coordonnée et intégrée, qui a permis de protéger remarquablement les citoyens australiens. Nous aimerions faire de même au Canada.

● (1130)

Dominique O'Rourke: C'est fantastique.

Je garde un œil sur l'heure. J'ai deux questions concernant votre point de vue de la nouvelle agence contre les crimes financiers, annoncée par le ministre des Finances.

Dans l'énoncé économique du printemps, le gouvernement a dit qu'il allait interdire les distributeurs automatiques de cryptomonnaies, car ils sont fréquemment utilisés dans le cadre d'escroqueries. Nous devrions dire aux gens: « Ne faites pas de cadeaux aux escrocs. N'allez pas à un distributeur de cryptomonnaies. Le gouvernement ne vous demandera pas ce genre de chose. Votre banque ne vous demandera pas ce genre de chose. »

Je me demande si vous soutenez l'interdiction des distributeurs de cryptomonnaies que l'on trouve dans de nombreux petits commerces de quartier.

Anthony Ostler: Tout à fait. Si l'on considère la criminalité financière, les escroqueries et les fraudes en constituent un sous-ensemble. La criminalité financière est liée à la cybercriminalité. Elle est liée au blanchiment d'argent. Parmi les personnes qui commettent ces escroqueries et ces fraudes, 60 à 70 % se trouvent à l'étranger. Elles ont besoin de faire sortir l'argent. Elles blanchissent cet argent. Un des moyens les plus simples d'y parvenir est d'utiliser les canaux de cryptomonnaie.

La plupart des cas d'utilisation des cryptomonnaies sont liés à une forme ou une autre de criminalité financière. C'est pourquoi nous avons besoin d'une agence contre les crimes financiers. D'autres grands pays en ont, comme l'Italie, les États-Unis et le Royaume-Uni. Nous avons besoin d'une agence capable de coordonner son action avec ces organismes, compte tenu des risques en jeu. Cela nous permettrait de mieux contrer ces malfaiteurs. Nous ne pourrons peut-être pas mettre en prison ceux qui se trouvent à l'étranger, mais si nous parvenons à coordonner nos efforts entre les pays et à les empêcher de s'en prendre à nos citoyens et à nos entreprises, nous serons alors mieux à même de les protéger.

Dominique O'Rourke: Merci.

Monsieur le président, puis-je disposer d'une minute? Mme Begum souhaiterait intervenir.

Le président: Je vous l'accorderai à la fin.

Madame Begum, vous pourrez intervenir après M. Ntumba pendant quelques secondes lorsque nous passerons à la prochaine série de questions.

[*Français*]

Monsieur Ste-Marie, vous avez la parole pour six minutes.

Gabriel Ste-Marie (Joliette—Manawan, BQ): Merci, monsieur le président. C'est un plaisir de vous revoir au Comité. Je peux vous dire que Mme Dancho a fait un travail de présidence hors pair. Je tiens également à la remercier d'avoir proposé cette importante étude.

Je remercie également les quatre témoins de leur présence. Ils nous ont transmis beaucoup d'informations dans leurs réponses ainsi que dans leur allocution d'ouverture, évidemment.

Je vais d'abord m'adresser à MM. Ostler et Elcock, de l'Association des banquiers canadiens. Je veux toutefois remercier M. Smith de ses recommandations, notamment la quatrième, qui est en lien avec le projet de loi C-29, sur lequel le débat devrait commencer sous peu à la Chambre des communes et se poursuivre en comité par la suite. Je le remercie donc de ses recommandations.

Monsieur Ostler, je voudrais discuter avec vous de deux types de fraudes qui ont beaucoup fait les manchettes et qu'on voit à l'international, mais qui ont des effets dévastateurs au Canada.

Juste avant, j'aimerais inviter les représentants de l'Association des banquiers canadiens à transmettre au Comité, si possible, plus d'informations sur le projet pilote auquel ils ont fait allusion, car c'est très intéressant, ainsi que sur ce qu'a fait l'Australie et dont ils nous ont donné les grandes lignes. Nous pourrions nous en inspirer et peut-être réussir à produire un meilleur rapport de comité.

Je vous donne un exemple du premier type de fraude qu'on a vu dans les émissions d'affaires publiques. Un jeune retraité qui a son fonds de pension va sur les réseaux sociaux et tombe sur un hypertrucage dans lequel on voit le premier ministre ou Elon Musk dire des faussetés et inciter les gens à investir dans les cryptomonnaies en présentant un lien sur lequel cliquer. Le jeune retraité le fait et investit 20 $. On lui dit ensuite que son investissement lui a rapporté, qu'il a triplé, alors il récupère son argent: 60 $. Comme il se dit que ça fonctionne, il recommence et investit cette fois 1 000 $ et récupère ensuite 3 000 $. Il finit par investir tout son fonds de pension, par exemple 500 000 $ ou 1 million de dollars, et pouf, tout son argent part à l'étranger et il ne le revoit jamais.

J'ai hâte que des représentants des réseaux sociaux comparaissent devant le Comité pour les questionner à ce sujet. Ça n'a pas de bon sens qu'il soit permis de diffuser des fausses vidéos comme ça.

Que peuvent faire les banques et les institutions financières quand l'argent a quitté le pays? Nous avons parlé de coordination, mais il semble que ce soit fini. Y a-t-il moyen, en s'appuyant sur les lois et les règles en place actuellement, d'en faire plus lorsqu'on voit qu'un montant de 500 000 $ s'en va à l'étranger et qu'on soupçonne une situation problématique, voire une fraude?

En ce qui concerne le CANAFE, soit le Centre d'analyse des opérations et déclarations financières du Canada, il ne semble pas avoir de pouvoir. Il reçoit l'information, il produit des rapports et il est submergé.

Donc, qu'est-ce qui peut être fait en fonction des règles et des lois actuelles? Qu'est-ce que vous, les banquiers, pouvez faire pour arrêter ce phénomène et empêcher les criminels de voler les économies de toute une vie?

● (1135)

Anthony Ostler: Merci beaucoup.

[*Traduction*]

Bien sûr, nous vous fournirons les renseignements sur le projet pilote et sur l'Australie. Nous avons déjà fourni certains documents concernant l'Australie au Comité, et nous avons encouragé l'association des banquiers australiens ainsi que les experts qui participent à leur échange d'informations à témoigner. Nous espérons que cela pourra être organisé pour le Comité, mais nous contribuerons à faciliter ce suivi.

En ce qui concerne les hypertrucages, la situation est très complexe. Nos membres surveillent en permanence le Web, les réseaux sociaux ou autres, à la recherche d'hypertrucages pouvant mettre en relief leurs représentants, qu'il s'agisse du PDG ou d'experts financiers de renom. Lorsqu'ils en repèrent un, ils en informent la plateforme concernée afin qu'ils soient retirés, car ils ne veulent pas que cela alimente les bruits ou confère de la crédibilité à de fausses offres d'investissement.

Et cela ne concerne pas uniquement les faux investissements dans les cryptomonnaies, même si ceux-ci sont malheureusement courants.

Ce qui est intéressant, c'est que les escrocs jouent sur les émotions. Ils exploitent la peur, la cupidité, la convoitise et la solitude. Malheureusement pour les consommateurs, lorsque quelqu'un joue sur vos émotions, l'esprit critique est souvent écarté. Si c'est la peur, la personne s'inquiète peut-être pour un petit-enfant ou autre chose. Si c'est la solitude, cela concerne peut-être un ami. Il peut s'agir de cupidité, et la victime éventuelle a besoin de plus d'argent. Ces facteurs poussent alors les gens à céder.

Nos membres ont de nombreux programmes de vigilance. Si quelqu'un tente d'envoyer une somme importante à l'étranger, ils lui demandent quel en est le but. Dans le cas d'un retrait d'argent, il s'agit souvent d'une arnaque locale, impliquant des personnes de la région plutôt que des acteurs internationaux. Cette arnaque consiste à convaincre les gens de retirer de l'argent de leur compte bancaire et de le leur remettre en espèces sous prétexte d'un risque de sécurité ou autre. Dans ces cas-là, si la personne n'a pas l'habitude de retirer de grosses sommes en espèces, les guichetiers ont été formés pour lui demander ce qui se passe.

En ce qui concerne les mesures supplémentaires que nous pouvons prendre, un élément clé réside évidemment dans le renforcement de notre capacité à partager des informations et à repérer les schémas récurrents. Si un incident se produit à Trois-Rivières ou à Thunder Bay, et que nous pouvons établir des liens — que ce soit avec nos partenaires des télécommunications ou des plateformes numériques —, nous collaborons avec les forces de l'ordre pour mettre fin à ces agissements.

En ce qui concerne le CANAFE, nos membres dépensent chaque année des milliards pour assurer la conformité et lutter contre la criminalité financière. Notre système n'est pas efficace, car nous nous concentrons plus sur la conformité que sur le risque. Il y a donc là une réelle occasion de réformer notre régime de lutte contre le blanchiment d'argent. Si vous souhaitez plus de détails, M. Elcock, qui est ici avec moi, est notre expert en matière de criminalité financière.

Hartland Elcock (avocat général adjoint et vice-président, Association des banquiers canadiens): C'est une excellente question. Je vous en remercie.

Tout d'abord, il faut replacer le rôle du CANAFE dans son contexte. C'est un organisme de renseignement et non un organisme d'application de la loi. Nos membres sont ceux qui signalent le plus grand nombre d'opérations suspectes au CANAFE: lorsqu'une organisation constate une activité douteuse donnant lieu à des motifs raisonnables de soupçonner le blanchiment d'argent, elle transmet cette information au CANAFE.

Encore une fois, il s'agit de blanchiment d'argent, de financement du terrorisme et de contournement des sanctions. Il ne s'agit pas des infractions principales de fraude, mais du traitement de l'argent après l'incident initial, et le rôle du CANAFE consiste à lier ces informations pour les transmettre aux autorités.

Je pense que l'Agence contre les crimes financiers, ou ACF, joue ici un rôle essentiel. On peut recevoir de nombreuses déclarations, comme c'est le cas actuellement. En fait, je crois que la Commission Cullen a noté que nous avons un nombre de déclarations bien supérieur à celui d'autres États, mais nous ne voyons pas les résultats escomptés en enquêtes et en poursuites.

Ce que l'ACF peut faire, c'est offrir ce que tous mes collègues ont mentionné, à savoir des enquêtes coordonnées et intégrées sur des crimes financiers complexes, afin de produire des résultats pour les Canadiens, de les protéger et de transformer ces informations en résultats concrets.

Cela ne signifie pas pour autant que le régime de lutte contre le blanchiment d'argent ne nécessite pas lui-même les améliorations que vous évoquez. Comme l'a mentionné M. Ostler, notre président, il est crucial de se concentrer sur le risque. Nous recevons de nombreuses déclarations au CANAFE, ce qui produit beaucoup de bruit dans le système.

Ce qui nous semble essentiel, c'est de voir une réforme globale du régime de lutte contre le blanchiment d'argent. Nous devons moderniser nos lois en matière de lutte contre le blanchiment d'argent pour que nous puissions examiner le genre de déclarations faites au CANAFE et veiller à ce qu'il cible les risques, en particulier les risques prioritaires cernés par le gouvernement. Ainsi, les forces de l'ordre recevront exactement les informations dont elles ont besoin. Il n'y aura pas de déluge d'informations. Le système sera véritablement ciblé sur les malfaiteurs.

Nous pouvons y parvenir en modifiant le projet de loi. Nous pouvons y parvenir en modifiant les pouvoirs de partage d'informations. Actuellement, le partage d'informations s'effectue entre entités privées. Ce système est en cours de mise en place. Nous envisageons d'autres modifications concernant le partage d'informations entre le secteur public et le secteur privé, afin que les forces de l'ordre puissent partager avec les banques des indicateurs clés de préproduction, ce qui permettra d'orienter les efforts de détection du blanchiment d'argent, puis de lutte contre celui-ci.

Enfin, nous devons aussi nous pencher sur la façon dont nous appliquons le régime. Faut-il envisager un règlement propre à certains secteurs? Le CANAFE compte 39 000 entités déclarantes. C'est une tâche colossale, et je pense qu'il est important que les bons régulateurs se concentrent sur les secteurs concernés.

Nous avons mentionné d'autres secteurs, comme les entreprises de services monétaires. Il est important que, dans les domaines à haut risque, les ressources de surveillance soient consacrées à ces domaines précis afin d'assurer la conformité. Nos membres respectent scrupuleusement la réglementation. Ils sont également soumis à une supervision prudentielle, ce qui offre plusieurs lignes de défense. Il est important, toutefois, que nous disposions d'une réglementation exhaustive à tous les niveaux.

Je terminerai en évoquant à nouveau l'Agence contre les crimes financiers elle-même. Je pense que tout ce qui est déposé est très prometteur, tant sur le plan de la structure que sur celui du mandat et des pouvoirs. Nous espérons aussi qu'elle évoluera graduellement pour devenir une agence de coordination, capable de définir des priorités nationales. Il est difficile de se concentrer sur les risques s'il n'y a pas de priorités, et nous espérons que l'Agence contre les crimes financiers pourra jouer ce rôle.

● (1140)

[*Français*]

Gabriel Ste-Marie: Merci beaucoup.

Merci, monsieur le président.

[*Traduction*]

Le président: Merci.

Monsieur Falk, la parole est à vous, monsieur.

Ted Falk (Provencher, PCC): Merci beaucoup, monsieur le président.

Merci à nos témoins pour leurs témoignages ce matin.

Monsieur Ostler, j'aimerais commencer par vous.

Je voudrais approfondir un peu la question de la conformité au CANAFE et celle de la réglementation qui s'applique à vous, en tant que banques au Canada. Exige-t-elle le bon type de conformité?

Je sais que le fardeau est considérable. Je le comprends parfaitement et j'en ai moi-même fait l'expérience.

Ce qu'ils vous demandent de faire est-il efficace?

Anthony Ostler: C'est une excellente question. Merci.

Comprenez-vous le concept du rendement décroissant?

Ted Falk: Oui.

Anthony Ostler: La Déclaration d'opérations douteuses du CANAFE comporte 400 champs. Le formulaire équivalent en Australie — dont nous avons constaté l'efficacité dans la lutte contre la criminalité financière — en compte entre 30 et 50. Au-delà de 30 champs, le rendement devient décroissant.

Si nous voulons agir rapidement et nous concentrer sur les risques, je pense qu'il y a là une excellente occasion, par exemple, de réformer le processus de déclaration et de mettre davantage l'accent sur l'action.

Ted Falk: Pensez-vous que l'ensemble de la réglementation du CANAFE et des questions de conformité devraient faire l'objet d'une réforme en profondeur?

Anthony Ostler: Certainement.

Ted Falk: Je ne m'oppose pas à ce que vous dites. C'est une bonne chose.

Vous avez indiqué aussi que, dans de nombreux autres pays, les escroqueries et la criminalité ont baissé d'environ 30 %, mais ici, au Canada…

Anthony Ostler: En Australie.

Ted Falk: C'est en Australie en particulier.

Anthony Ostler: C'est en Australie, et la baisse est de 30 % au cours des trois dernières années.

Ted Falk: Chez nous, c'est une hausse de 32 % depuis 2022.

Anthony Ostler: C'est exact.

Ted Falk: Pourquoi?

Anthony Ostler: Les chiffres ont augmenté partout ailleurs qu'en Australie au cours de ces trois années.

Ce qui s'est passé, c'est que ces malfaiteurs sont de plus en plus perfectionnés. Leur intelligence artificielle est plus puissante; leurs outils sont plus puissants. Ils ont mis en place des équipes internationales, des équipes spéciales et des équipes virtuelles, qui collaborent toutes. Ils disposent d'experts capables d'explorer le Web clandestin et d'autres spécialisés dans le profilage psychologique. Ils élaborent, par exemple, une stratégie qui pourrait fonctionner en Australie. Si l'Australie la contrecarre, ils la mettent alors en œuvre au Canada. C'est ce genre de chose.

Ces malfaiteurs...

Ted Falk: C'est un peu comme l'électricité. On va là où il y a le moins de résistance.

Anthony Ostler: Exactement. On va là où il y a le moins de résistance.

Ted Falk: Je m'interroge également sur ce qui suit. Une fois que ces malfaiteurs sont identifiés et que vous parvenez à faire toute la lumière sur un incident ou une escroquerie dans son ensemble, les poursuites judiciaires sont-elles efficaces, d'après vous?

Anthony Ostler: J'étais au Sommet mondial sur la fraude, organisé par les Nations unies. On y a mentionné que 60 à 70 % des sources d'escroqueries et de fraudes sont internationales.

Cela dépend du pays d'origine. C'est ce que constatent également nos homologues du secteur des télécommunications. Si certains pays ne modernisent pas leurs systèmes de télécommunications ou ne disposent pas d'une solide primauté du droit, ils peuvent devenir la porte dérobée ou la canalisation de nombreux problèmes.

Ted Falk: Lorsque certaines de vos organisations membres, certaines des banques que vous représentez, ont été victimes de fraudes et ont arrêté les malfaiteurs, vous signalent-elles que les sanctions sont lourdes ou appropriées?

● (1145)

Anthony Ostler: En ce qui concerne les malfaiteurs, nous n'avons tout simplement pas constaté… Par exemple, en ce qui concerne la lutte contre le blanchiment d'argent, nous n'avons pas constaté beaucoup de condamnations. Pour les escroqueries, les statistiques que j'ai consultées indiquent que seules 5 à 10 % des victimes signalent les escroqueries dont elles sont victimes. Parmi celles-ci, une infime partie, je pense que c'est 0,1 ou 0,2 %… C'est une erreur d'arrondi par rapport au nombre réel de condamnations.

Quant aux escroqueries elles-mêmes et aux signalements de blanchiment d'argent… Il n'y a pas, au Canada, un nombre élevé de condamnations pour crime financier.

Ted Falk: Le ratio risque-rémunération est en fait à leur avantage.

Anthony Ostler: Oui, tout à fait.

Je pense que c'est en partie pour cette raison que nous voulons agir en amont et mettre en place ce partenariat intersectoriel public et privé. Si nous parvenons à ériger une barrière plus élevée autour du Canada et à empêcher ces malfaiteurs d'entrer par de multiples canaux, nous pourrons mieux protéger nos habitants et réduire le risque qu'ils soient dupés par ces personnes.

Ted Falk: J'ai encore une question à vous poser avant de passer à M. Frey.

Quel devrait être le niveau de responsabilité ou d'obligation des banques dans ce genre de situation où des escroqueries sont commises?

Anthony Ostler: Nous sommes soumis à une réglementation très stricte, potentiellement. Nous avons un code de conduite.

Si le consommateur est véritablement une victime, dans la mesure où il n'a communiqué aucune information ni envoyé quoi que ce soit et où il a été escroqué, alors nos membres s'occupent évidemment de lui. Malheureusement, bien des gens envoient volontairement l'argent. Les banques leur demandent, au moment de l'envoi: « Êtes-vous sûr? Que faites-vous? »

Ted Falk: Je suis très heureux de recevoir ces textos qui demandent: « C'est bien vous qui achetez cela? »

Anthony Ostler: Exactement. Nous faisons beaucoup pour essayer d'aider nos clients. Ce que nous avons compris, c'est qu'il faut agir en amont pour essayer de les empêcher d'être trompés.

Ted Falk: Monsieur Frey, je n'ai plus de temps. Je suis désolé.

Le président: Chers collègues, si tout se passe comme prévu, la sonnerie d'appel retentira à midi pour les votes. J'ai besoin d'un consentement unanime pour poursuivre les travaux malgré la sonnerie d'appel. J'aimerais d'abord m'en assurer. Si je ne l'obtiens pas, nous devrons nous interrompre. Si je l'obtiens et que tout le monde est disposé à voter en ligne, alors nous pourrons continuer.

Tout le monde peut-il indiquer très clairement s'il est d'accord ou pas?

Allez-y, monsieur Ma.

Michael Ma (Markham—Unionville, Lib.): Je suis d'accord, mais nous devons faire une pause de quelques minutes pour procéder au vote.

Le président: Oui, c'est pour voter, mais j'ai besoin du consentement unanime pour continuer à siéger malgré la sonnerie d'appel. Le vote n'aura pas lieu avant environ 12 h 30, donc ça ne poserait pas de problème.

Ai-je le consentement unanime pour continuer malgré la sonnerie?

Oui. Très bien. Dans le cas présent, je vais me montrer un peu plus indulgent. Nous avons largement dépassé le temps imparti avec M. Ste-Marie. Cela semble devenir une habitude. J'ai moi-même quelques questions, et, comme c'est notre première réunion, je serai peut-être un peu plus indulgent.

Ted Falk: L'autre présidente était intransigeante.

Le président: En effet, elle était intransigeante, monsieur Falk.

Soyez très bref avec M. Frey, puis je poserai moi-même quelques questions. Nous allons simplement continuer, et lorsque nous entendrons les sonneries d'appel à midi, cela ne signifie pas que le vote commence. Cela signifie simplement que c'est une période d'avertissement.

Monsieur Falk, vous avez environ 45 secondes.

Ted Falk: Ce sera parfait. Merci beaucoup, monsieur le président.

Monsieur Frey, vous avez indiqué que trois des fraudeurs à l'origine des dispositifs SMS Blaster avaient été inculpés de 44 chefs d'accusation différents. Quel niveau de…? Quelle a été la peine? Êtes-vous satisfait de ce que la Couronne demande?

Carey Frey: Oui, mais il est certain qu'ils ont accumulé un certain nombre de chefs d'accusation dans le cas présent, dans de nombreuses catégories différentes. On pourrait déduire que les infractions individuelles en elles-mêmes étaient probablement mineures, mais 44 infractions en tout peuvent entraîner une peine beaucoup plus longue.

L'affaire est devant les tribunaux, nous devrons donc attendre de voir quelle en sera l'issue.

Ted Falk: Merci.

Le président: Je vous remercie, monsieur Falk.

[*Français*]

Monsieur Ntumba, vous avez la parole pour cinq minutes, mais, comme je l'ai dit, je vais accorder quelques secondes à Mme Begum pour poser une question. J'accorde un peu plus de temps à tout le monde ici.

Alors, je donne la parole pour cinq minutes à vous, monsieur Ntumba, et ensuite pour 45 secondes à Mme Begum.

Bienvenu-Olivier Ntumba (Mont-Saint-Bruno—L'Acadie, Lib.): Merci, monsieur le président. Il n'y a pas de souci pour ça.

Permettez-moi de m'adresser à M. Ostler ou à M. Frey; il faudra voir qui veut répondre.

L'intelligence artificielle permet aujourd'hui aux fraudeurs de créer des arnaques de plus en plus convaincantes. Le Canada est-il suffisamment préparé à cette nouvelle génération de fraudeurs? Quelles mesures devraient être prioritaires au cours des trois prochaines années?

[*Traduction*]

Anthony Ostler: Malheureusement, comme le montrent les statistiques, le Canada n'est pas tout à fait prêt. Notre coalition volontaire de lutte contre l'escroquerie étant en place depuis quelques années, nous avons probablement une longueur d'avance sur de nombreux pays, voire la plupart d'entre eux, pour ce qui est de comprendre les risques, mais, comme tous les pays à l'exception de l'Australie, nous n'avons aucune initiative intersectorielle public et privé exhaustive en place.

Je pense que nous pourrions y parvenir assez rapidement. Le gouvernement a créé la Stratégie nationale antifraude. Il met sur pied l'Agence contre les crimes financiers. Il a l'occasion de réformer le régime de lutte contre le blanchiment d'argent. Je pense que nous pourrions réellement inverser la tendance et réduire le nombre d'escroqueries et de fraudes d'ici quelques années.

Une fois que l'Australie a compris comment s'y prendre, elle a obtenu des résultats très rapidement. Nous sommes sur le point d'y parvenir, mais un élément clé consiste à trouver comment harmoniser des définitions claires avec un cadre intersectoriel, afin que les différents acteurs connaissent tous leur rôle et que des contrôles soient en place pour les divers secteurs.

Comme nos collègues l'ont mentionné ici, chaque secteur a ses propres régulateurs, mais il doit y avoir une entité globale garantissant la coordination. Pour que ce système soit efficace, nous devons améliorer l'échange des données sur la fraude, la surveillance de cet échange et la sensibilisation du public.

Nous avons beaucoup avancé sur le plan de la sensibilisation du public...

● (1150)

[*Français*]

Bienvenu-Olivier Ntumba: En fait, votre commentaire sur l'échange des données relatives à la fraude répond quasiment à ma prochaine question. J'allais vous demander si les banques disposent des outils nécessaires pour transmettre rapidement les renseignements sur les fraudeurs à leurs partenaires financiers ainsi qu'à d'autres organisations en matière de sécurité, aux gouvernements et aux services de police.

Veuillez répondre rapidement afin de permettre à M. Frey de répondre également.

[*Traduction*]

Anthony Ostler: C'est une excellente question.

Nous avons le cadre juridique nécessaire pour échanger l'information. Nous avons l'information, mais nous n'avons pas un outil qui permettrait de les échanger rapidement. Nous menons actuellement un projet pilote entre deux de nos membres du secteur des télécommunications. Cela fonctionne, et rapidement, vers l'entité qui conserve l'information en toute sécurité, mais l'analyse proprement dite est lente, car elle n'est pas automatisée.

Nous n'en sommes pas encore là, mais, maintenant que nous avons une taxonomie conçue pour fonctionner dans tous les secteurs, la prochaine étape consisterait à mettre en place un système d'échange d'information. Cette taxonomie a d'ailleurs été conçue pour répondre aux besoins du gouvernement.

[*Français*]

Bienvenu-Olivier Ntumba: Monsieur Frey, si vous deviez recommander au gouvernement fédéral une seule mesure pour réduire le plus possible les fraudes ou les tentatives de fraude au Canada, quelle serait-elle? Pourquoi serait-elle importante?

[*Traduction*]

Carey Frey: Comme je l'ai mentionné dans mon témoignage, nous avons besoin d'un pouvoir de coordination, pas d'un comité — il n'est pas question de lutter contre la fraude de manière globale avec un comité. Il doit y avoir un lieu unique, une organisation qui peut assumer la responsabilité de comprendre comment la fraude se produit et diriger les stratégies et les campagnes auxquelles nous pouvons tous participer pour trouver la solution qui nous permettra de nous débarrasser de l'arnaque ou du réseau frauduleux en question qui commet ces crimes contre les Canadiens.

[*Français*]

Bienvenu-Olivier Ntumba: Pensez-vous que les citoyennes et citoyens sont assez outillés ou équipés pour faire face à des types de fraudes qui s'appuient sur la nouvelle technologie?

Bien que nous ayons tous accès à l'information, il y a trois types de personnes: les jeunes, les moins jeunes et les personnes âgées. Que pensez-vous de la diversité des perceptions de l'information selon les différentes tranches d'âge?

[*Traduction*]

Carey Frey: Je pense que nous devons sensibiliser davantage les Canadiens aux nouveaux types de fraude et d'escroquerie qui se produisent et leur accorder une attention particulière. J'avais l'impression, autrefois, de pouvoir suivre le rythme. Je suis un professionnel de la sécurité depuis trois décennies, et j'en suis arrivé au point où je ne peux plus suivre l'évolution de la situation, ne serait-ce que pour moi-même.

Si l'on extrapole cela à l'ensemble de notre société, non, je ne pense pas que nous soyons prêts, et nous devons accorder beaucoup plus d'attention et d'importance à cela. Comme l'a souligné mon collègue, la sensibilisation à ces escroqueries et aux mesures que nous pouvons prendre pour ne pas en être victimes est primordiale.

[*Français*]

Le président: Merci, monsieur Ntumba.

Mme Begum a indiqué ne pas avoir besoin de temps de parole, alors la parole est à vous, monsieur Ste-Marie.

Gabriel Ste-Marie: Dans ce cas, je remercie Mme Begum de me laisser le temps de parole qui lui était imparti; mais non, c'est une blague.

Je vais encore poser une question aux représentants de l'Association des banquiers canadiens. Cela dit, comme je risque de manquer de temps pour entendre vos réponses si vous en avez, messieurs Smith et Frey, n'hésitez pas à nous les transmettre par écrit.

J'aimerais parler de la question des fuites de données dans toutes sortes d'entreprises, que ce soit des entreprises financières ou autres. Même les géants des télécommunications au Canada ont eu de tels cas. Ces fuites mènent à des vols d'identité; les fraudeurs prennent des hypothèques ou font des emprunts au nom des gens dont ils ont volé l'identité.

Que pourrait-on faire pour que ça arrête? Les données de tout le monde circulent partout, par exemple sur le Web clandestin. Les données des Canadiens sont là. Qu'est-ce qui peut être fait pour que ça n'arrive plus?

Par ailleurs, devrait-il y avoir un délai quand l'entreprise sait qu'il y a eu un vol de données? Devrait-elle déclarer tout de suite qu'une fuite de données a eu lieu? Ce n'est pas dans tous les cas que ces informations sont dévoilées.

● (1155)

[*Traduction*]

Hartland Elcock: C'est une excellente question. Merci beaucoup.

Je me référerais à la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE, et au signalement obligatoire des atteintes à la sécurité des données au titre de cette loi. Cette obligation est déjà en vigueur et exige, lorsqu'une fuite se produit, que les particuliers concernés soient informés. La Loi précise aussi diverses autres mesures à prendre, ainsi que les mesures d'amélioration à mettre en œuvre pour remédier aux préjudices qui pourraient en découler.

Comme M. Ostler l'a souligné tout à l'heure, il est également essentiel de tenir compte de ces engagements en ligne en cas de violation. Il ne s'agit pas d'une fraude autorisée ni d'aucune autre forme de violation technique, ce qui serait très rare. Il y a également l'engagement à indemniser pleinement les clients.

Je pense que le cadre juridique prévu par la législation sur la protection des renseignements personnels est déjà suffisamment large pour traiter le type de situation que vous décrivez. Il n'exige pas un délai particulier, mais il exige un délai défini.

[*Français*]

Gabriel Ste-Marie: Merci.

Il me reste 30 secondes. Monsieur Smith ou monsieur Frey, voulez-vous ajouter quelque chose?

[*Traduction*]

Carey Frey: Si je peux me permettre, j'ajouterais que nos normes en matière d'authentification d'identité ne sont pas uniformes partout au pays. C'est sur une base volontaire que les organisations choisissent, par exemple, d'informer leurs clients qu'ils doivent changer leur mot de passe. La solution consiste à faire appliquer des normes de manière uniforme dans ce domaine par une personne ayant les connaissances nécessaires pour déterminer ce que celles-ci devraient être, et le pouvoir de les mettre en vigueur partout au pays, afin qu'il n'y ait plus à l'avenir de différenciation concurrentielle sur cette question.

[*Français*]

Gabriel Ste-Marie: Merci.

Monsieur Smith, vous pourrez transmettre vos commentaires par écrit au Comité, car mon temps de parole est écoulé.

Je vous remercie.

Le président: Merci, monsieur Ste-Marie.

[*Traduction*]

Madame Dancho, la parole est à vous pour cinq minutes.

Raquel Dancho: Monsieur Ostler, j'aimerais revenir sur quelques-unes des questions posées par les collègues qui m'ont précédée.

Vous l'avez souligné, tout comme d'autres. L'Australie est le seul pays au monde à avoir enregistré une baisse de ces fraudes et escroqueries. Je crois que les données montrent une baisse d'un peu moins de 30 % depuis 2022, comme vous et d'autres l'avez souligné aujourd'hui. Partout ailleurs, il y a eu une augmentation. Cela représente en réalité près de 1 milliard de dollars d'économies. Les pertes s'élevaient à un peu plus de 3 milliards de dollars en 2022, et elles sont tombées à 2,18 milliards de dollars en 2025. Ce sont là des économies importantes pour les Australiens.

Nous avons entendu, de votre part et d'autres personnes, que le problème principal est d'ordre international. Y remédier est un véritable défi. Oui, il faut davantage de collaboration internationale… mais l'Australie a trouvé un moyen d'y faire face. Pouvez-vous nous expliquer un peu plus ce qu'elle a fait exactement que nous ne parvenons pas à faire?

Anthony Ostler: L'une des mesures clés que l'Australie a adoptées a consisté à mettre en place des codes de conduite pour les différents secteurs concernés — plateformes numériques, télécommunications et banques — et à définir clairement ce qu'elle attendait d'eux. Par exemple, pour les plateformes numériques, si elles repéraient une publicité frauduleuse ou un site Web malhonnête, elles étaient tenues de les retirer ou de les bloquer.

Lorsqu'une banque ou un conseiller en investissement diffuse une publicité sur les réseaux sociaux en Australie, il doit vérifier que l'annonceur de services financiers est bien une personne physique enregistrée ou une entité réglementée autorisée à faire de la publicité. Il existe une obligation de vérifier, ou la nécessité de « connaître son annonceur ». Cela a un impact considérable quand on pense aux fausses publicités produites par l'intelligence artificielle. Nous avons déjà entendu le cas de personnes encouragées à investir dans les cryptomonnaies par un fonctionnaire ou une personnalité publique dont l'image est exploitée par l'intelligence artificielle. Les publicités de ce genre seraient supprimées plus rapidement, et leur diffusion ne serait pas autorisée.

Ces éléments — « connaître son annonceur », vérification, retrait des contenus et blocage des sites — sont essentiels. Pour faire échec aux manœuvres qui sont à l'origine des escroqueries ou des arnaques, il faut supprimer ces contenus plus rapidement. C'est là un des principaux facteurs qui ont contribué à la réduction du nombre d'escroqueries et de fraudes.

Comme l'ont indiqué mes collègues du secteur des télécommunications présents ici, il existe des portes dérobées donnant accès au système. Une institution financière qui appelle un client a des moyens de s'assurer que son logo peut s'afficher. Il n'est pas possible de passer par un système de SMS. Il s'agirait d'un processus officiel. C'est un exemple montrant comment les consommateurs pourraient savoir que, si le logo de leur banque n'apparaît pas, ce n'est sans doute pas un appel authentique de cette banque. Ce sont là des exemples.

● (1200)

Raquel Dancho: Je vous en suis très reconnaissante.

Je ne souhaite pointer du doigt aucun pays abritant des acteurs malveillants. Nous ne connaissons pas les ressources de ce pays ni les défis auxquels il est confronté, mais je pense qu'il est important d'inclure ces données dans l'étude du Comité. Pourriez-vous simplement mentionner quelques pays qui sont à l'origine de certains de ces problèmes?

Anthony Ostler: Le Myanmar est au cœur même de ces problèmes. Il y a aussi des États-nations, comme l'Iran, qui contribuent aux escroqueries et à la fraude. Ce sont là des exemples de pays faisant problème.

Raquel Dancho: Merci pour votre témoignage.

Monsieur le président, une question pertinente et préoccupante s'est posée au Canada. Le Comité de l'industrie en a longuement débattu par le passé. Je voudrais donner avis de la motion suivante:

> Que le comité fasse rapport à la Chambre de sa condamnation du recours au travail forcé dans les chaînes d'approvisionnement, particulièrement en Chine; qu'il rejette les tarifs américains injustifiés qui menacent les travailleurs et les industries du Canada; et qu'il demande au gouvernement libéral de renforcer l'interdiction canadienne actuelle visant les importations issues du travail forcé et de prendre des mesures plus efficaces pour empêcher l'entrée au Canada de biens fabriqués au moyen du travail forcé.

Monsieur le président, nous en avons longuement débattu. Je pense qu'il serait pertinent maintenant d'obtenir le consentement unanime pour l'adoption de cette motion aujourd'hui. C'est ce que je demande.

Merci.

Le président: D'accord. Juste pour être clair, madame Dancho, présentez-vous cette motion, ou en donnez-vous avis?

Raquel Dancho: J'en donne avis, mais étant donné que nous en avons déjà longuement débattu, je demande aussi le consentement unanime pour que nous l'adoptions aujourd'hui.

[*Français*]

Gabriel Ste-Marie: J'invoque le Règlement, monsieur le président.

Le président: Monsieur Ste-Marie, vous avez la parole.

Gabriel Ste-Marie: J'aimerais que nous puissions avoir la motion par écrit avant de nous prononcer.

Raquel Dancho: Oui, bien sûr.

Le président: C'est exactement ce que j'allais dire.

[*Traduction*]

Voilà pourquoi, madame Dancho, ce n'est pas aussi simple que de demander le consentement unanime. Je dois savoir si vous présentez cette motion ou non.

Si vous la présentez, vous nous demandez d'en débattre, mais je dois d'abord en prendre connaissance. D'après ce que j'ai compris du texte que vous avez lu, je ne suis pas certain qu'elle soit pertinente au regard des travaux qui nous occupent. Je doute donc de sa recevabilité à ce stade-ci.

Si vous souhaitez que je l'analyse et que je me prononce à ce sujet, je peux le faire. Si vous n'insistez pas pour la présenter en ce moment, vous êtes bien sûr autorisée à en donner avis, et nous pourrons alors procéder en conséquence.

Raquel Dancho: Comme nous en avons longuement débattu au cours des séances précédentes du Comité, je pense que tout le monde est parfaitement au courant de cette question. Vu que le débat à son sujet figure dans le compte rendu, je demande le consentement unanime pour l'adopter.

Le président: La question, madame Dancho, n'est pas de savoir si nous en avons déjà débattu. C'est qu'elle n'est pas pertinente par rapport au sujet à l'étude. Vous n'avez pas donné le préavis requis. Par conséquent, elle n'est pas recevable.

Raquel Dancho: Je ne la présente pas encore, mais je demande le consentement unanime, ce que je suis en droit de faire.

Le président: C'est vrai, mais pour que nous puissions entamer un processus décisionnel à ce sujet, il faudrait que la question soit elle-même recevable.

Raquel Dancho: Pas pour demander le consentement unanime, non.

Le président: Permettez-moi tout d'abord d'y jeter un coup d'œil.

Raquel Dancho: Bien sûr. Merci.

Le président: Pour que je puisse le faire, j'en aurai besoin dans les deux langues officielles.

Raquel Dancho: Nous l'avons.

Le président: Compte tenu du degré de collaboration important qui a permis de mener à bien cette étude sur la fraude, à votre demande et avec la collaboration des députés présents autour de cette table, il me semble plutôt utile de poursuivre le débat sur la fraude avant de traiter cette question.

Par conséquent, comme nous l'avons déjà fait par le passé lorsque des motions nous ont été présentées inopinément, je recommande que nous contournions un peu le règlement ici, avec votre permission, chers collègues, afin d'utiliser les dernières minutes dont nous disposons pour entendre les témoignages, puis je pourrai revenir, madame Dancho, sur cette question. Je ne vois pas l'intérêt de faire attendre les témoins pour que nous la réglions tout de suite.

Raquel Dancho: Bien sûr. Cela me convient. Merci.

Le président: Chers collègues, y a-t-il d'autres observations à ce sujet avant que nous ne concluions cette partie et que j'examine la question?

Monsieur Ntumba, vous avez la parole.

● (1205)

[*Français*]

Bienvenu-Olivier Ntumba: Je pense que vous avez tout dit. Nous avons des témoins. De plus, l'avis de motion n'a pas été déposé au préalable. Donc, je suis d'accord sur ce que vous avez dit.

Le président: Nous allons d'abord terminer les témoignages, puis nous pourrons continuer cette discussion.

[*Traduction*]

Madame Dancho, je vais demander à votre équipe de travailler rapidement, s'il vous plaît, afin que ce document soit distribué aux députés dans les deux langues officielles. J'y jetterai un coup d'œil, une fois que nous aurons entendu tous les témoins ici.

Monsieur Bains, la parole est à vous, si vous souhaitez encore poser quelques questions. Ensuite, je prendrai quelques minutes pour poser moi-même une ou deux questions, puis nous reviendrons à celle que madame Dancho vient de soulever.

Monsieur Bains, à vous la parole.

Parm Bains (Richmond-Est—Steveston, Lib.): Merci, monsieur le président.

Je remercie nos témoins de s'être joints à nous aujourd'hui dans le cadre de cette étude très importante.

Nous avons reçu beaucoup d'information, et je vous remercie d'en avoir partagé une grande partie et d'avoir mis l'accent sur les risques, tout en formulant d'autres recommandations. En fin de compte, la raison d'être du Comité est de produire des recommandations solides que nous pourrons ensuite mettre en œuvre.

J'aimerais vous demander votre point de vue sur le projet de loi C-22, qui est actuellement examiné et débattu à la Chambre, et sur la question de l'accès légal. D'après mes entretiens avec de nombreux services de police locaux ici, en Colombie-Britannique, et même avec le Service canadien du renseignement de sécurité, le SCRS, ceux-ci veulent un accès accru aux informations et la possibilité de participer à la question de l'accès légal et de l'Agence contre les crimes financiers. Ils veulent savoir comment ils peuvent prendre part à ces processus pour s'assurer qu'ils pourront s'attaquer à certains de ces problèmes.

La mention de l'Australie m'intéresse énormément. Dans l'ensemble, il semble s'agir d'un changement tout à fait réalisable en ce qui concerne le code de conduite des banques et des plateformes et les dispositifs de vérification. Pourriez-vous nous faire part de vos réflexions sur l'accès légal et formuler des recommandations, le cas échéant?

Anthony Ostler: Cette question s'adresse-t-elle d'abord à l'Association des banquiers canadiens?

Parm Bains: Oui, à l'ABC.

Anthony Ostler: Merci beaucoup, monsieur Bains. Je suis ravi de vous voir.

À une échelle plus générale, il ne s'agit pas seulement des mesures que devrait comprendre le projet de loi C-22 pour nous aider à lutter contre les escroqueries et la fraude. Ce qui compte surtout, c'est d'assurer un bon soutien, la supervision de l'échange d'information et la coordination avec les forces de l'ordre, surtout si nous concluons que des malfaiteurs étrangers participent aux escroqueries ou à la fraude. C'est un volet plus vaste.

Je m'en remettrai à mes collègues du secteur des télécommunications pour savoir s'ils estiment que des éléments particuliers du projet de loi C-22 concernant les fraudes et les escroqueries leur paraîtraient utiles.

Parm Bains: Pourrions-nous entendre M. Frey, de Telus, s'il vous plaît?

Carey Frey: En ce qui concerne le projet Lighthouse, dont j'ai parlé tout à l'heure, nous avons bien reçu de la part de la police des ordonnances judiciaires nous permettant de lui fournir les données dont elle avait besoin pour mener cette enquête. À mon avis, tout a très bien fonctionné sur ce plan, sauf peut-être en ce qui concerne la rapidité d'exécution. Je dirai seulement que nous devons trouver des moyens, dans le cadre de notre système d'accès légal, de transmettre rapidement les données aux enquêteurs, car ils en ont besoin pour mener à bien leur travail.

Parm Bains: Pour en venir à l'arme cybernétique, avez-vous découvert…?

Les auteurs de l'attaque par SMS Blaster ont été arrêtés, mais vous avez longuement expliqué comment les fraudeurs trouvent toujours le moyen de passer à autre chose et de se tourner vers d'autres domaines. Avez-vous constaté que les fraudeurs utilisent de nouvelles méthodes ou d'autres technologies? À quels éventuels investissements ou initiatives le gouvernement pourrait-il recourir pour les combattre sur le plan de la cybersécurité?

Carey Frey: Nous avons détecté au Canada de nombreuses autres formes d'appareils destructeurs prépositionnés. L'arrestation de ce groupe à Toronto n'a pas mis fin complètement à l'utilisation de dispositifs SMS Blasters. Nous savons qu'il en existe d'autres et qu'ils sont actifs dans d'autres régions, villes ou provinces du pays.

Pour revenir à mon témoignage de ce matin, je tiens à réaffirmer que les forces de l'ordre ont besoin d'un mandat direct et de ressources supplémentaires afin de procéder au démantèlement et à l'arrestation des réseaux qui opèrent au Canada et déploient cette technologie pour commettre des fraudes à grande échelle.

● (1210)

Parm Bains: Je vais rester sur ce sujet avec vous.

Vous avez évoqué la réforme du régime de lutte contre le blanchiment d'argent. Pouvez-vous nous en dire davantage là-dessus? En tant que gouvernement, en avons-nous suffisamment parlé, ou s'agit-il d'une question que vous soulevez maintenant?

Hartland Elcock: Je pense que le régime de lutte contre le blanchiment d'argent nécessite des réformes importantes.

La dernière modernisation approfondie de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, la LRPCFAT, remonte à environ 26 ans. Il n'y a pas eu d'examen parlementaire depuis un bon moment. Je pense que nous sommes un peu en retard sur ce point.

Nous aimerions voir des réformes dans divers domaines, mais commençons par moderniser la loi. Il faut examiner la gestion du régime axé sur la LRPCFAT et les outils législatifs dont il dispose. Ensuite, il faut aussi que nous nous penchions sur l'échange d'information. Ce qui a été abordé aujourd'hui est essentiel, mais il y a une quantité considérable de renseignements transmis au CANAFE qui ne mènent pas nécessairement à des résultats.

Le nombre de rapports est considérable. Comme l'a mentionné mon collègue, au Canada, la Déclaration d'opération douteuse, la DOD, comporte 400 champs, contre 35 en Australie. Il existe bien des façons de réduire ce nombre de champs et celui des déclarations, tout en obtenant des résultats concrets, voire meilleurs. Ainsi, le « bruit » dans le système serait atténué, et nous pourrions mieux utiliser l'information obtenue pour accroître les moyens d'action des forces de l'ordre. Nous souhaitons voir ce genre de supervision axée sur chaque secteur, car, grâce à elle, les domaines à risque feront l'objet d'une surveillance appropriée, et les intervenants y travaillant pourront ensuite échanger l'information.

Je constate que vous avez mentionné le projet de loi C-22. Le projet de loi C-2, qui est toujours en cours d'examen, comporte certaines modifications que nous aimerions voir adopter du point de vue de la lutte contre le blanchiment d'argent. Elles concernent les dispositions d'exonération pour les secteurs public et privé et celles qui permettent aux organisations régies par le gouvernement fédéral d'utiliser, sans risque de responsabilité, les renseignements que les forces de l'ordre leur fournissent, à savoir les renseignements préalables à la communication qui permettent aux organisations assujetties à la LRPCFAT de concentrer correctement leurs efforts sur les risques.

D'abord et avant tout, je pense qu'un examen approfondi de la loi s'impose, mais nous avons de nombreuses idées, comme je viens de le montrer, sur l'orientation à suivre pour favoriser réellement l'amélioration des résultats.

Parm Bains: Merci beaucoup.

Je cède le reste de mon temps de parole au président.

Le président: Très bien, monsieur Bains.

Messieurs les témoins, j'ai ici quelques questions très brèves.

Peut-être, monsieur Ostler, êtes-vous le mieux placé pour y répondre. Madame Dancho a effectivement soulevé ce point à propos des Australiens.

Vous parliez de retraits rapides. Dans le contexte canadien, les plateformes de réseaux sociaux se montrent-elles coopératives lorsque vous les contactez, après avoir cerné un problème quelconque, et que vous sollicitez leur coopération pour retirer un hypertrucage, une fausse publicité, ou tout autre contenu de ce genre? Répondent-elles à vos demandes? Sont-elles disposées à travailler avec vous? Sinon, pourquoi?

Anthony Ostler: C'est une excellente question, monsieur le président.

Lorsque nous avons lancé la Coalition canadienne antifraude, nous avions mis en place, dès la première année, un volet de travail consacré précisément à cette question, car les plateformes numériques font partie de cette coalition. Nous avons cherché la meilleure façon de leur fournir l'information dont elles ont besoin pour supprimer de tels contenus. Cela a amélioré la coopération, mais leur processus de vérification avant suppression est long. Les contenus ne sont pas supprimés aussi rapidement qu'ils le seraient en Australie.

Il est difficile de savoir ce qui explique cela. Peut-être que c'est un problème de ressources ou de priorités. Nous avons notamment eu d'excellents entretiens, mais le fait est que des améliorations sont possibles.

Le président: À votre avis, monsieur Ostler, reconnaissent-elles l'ampleur du problème?

Anthony Ostler: Il est intéressant de noter que, lors du Sommet mondial sur la fraude, organisé par les Nations unies, les représentants de toutes les grandes plateformes numériques ont signé l'entente-cadre dont j'ai parlé. Celle-ci traite de la responsabilité partagée de tous les acteurs tout au long du cycle de la fraude; ils ont donc convenu de l'ampleur du problème.

À l'occasion du forum, Meta a dit vouloir améliorer son processus de vérification. À ce moment-là, son taux de vérification était de 70 %. Si une banque n'authentifiait que 70 % de ses clients, je pense qu'elle ferait faillite. L'objectif de Meta est de passer à 90 %.

Je pense que ce sont là des progrès, mais que des améliorations sont possibles.

Le président: Je vous pose ma question d'une façon plus précise: lorsque vous avez des entretiens avec les représentants des plateformes de réseaux sociaux sur la gravité du problème, estimez-vous qu'ils acceptent la responsabilité du rôle que ces plateformes jouent en tant que vecteurs favorisant cette fraude?

● (1215)

Anthony Ostler: Oui.

L'International Banking Federation, l'IBFed, s'est entretenue avec le responsable mondial de la lutte contre la fraude et de la sécurité chez Meta, lors du Sommet mondial sur la fraude. Ils ont convenu qu'il s'agissait d'un problème et ont souhaité collaborer avec nous à l'échelle internationale. Nous avons des entretiens fructueux sur les moyens de mettre en place des projets pilotes et d'améliorer ce que nous pouvons.

Je dirais que l'année 2026 a produit les progrès les plus marquants que nous ayons réalisés, mais il reste encore beaucoup à faire.

Le président: Merci.

J'ai une deuxième question.

On a fait allusion tout à l'heure au fait qu'une fraude ou une escroquerie affaiblit la cote de crédit de la victime. Je sais que ce n'est pas nécessairement votre domaine d'expertise, mais pourriez-vous donner au Comité votre avis sur les moyens qu'une Canadienne ou un Canadien peut prendre s'il est victime d'une fraude et constate ensuite des répercussions négatives sur sa cote de crédit? Comment peut-il remédier à cette baisse de sa cote causée par la fraude?

Anthony Ostler: Le cas évoqué concernait l'usurpation d'identité numérique. Quelqu'un contracte un emprunt avec une fausse pièce d'identité, et la personne dont l'identité a été compromise est alors désignée comme étant l'emprunteuse, ce qui n'est pas le cas. En pareilles situations, une fois cela prouvé, la banque concernée ou l'établissement financier visé collabore avec l'agence d'évaluation du crédit pour mettre à jour la cote de crédit de la personne, car celle-ci a été victime d'un vol d'identité.

Évidemment, la difficulté pour les victimes tient au fait qu'elles doivent collaborer avec les institutions financières et d'autres organismes pour prouver qu'elles ont fait l'objet d'un vol d'identité. C'est un processus qui risque de prendre beaucoup de temps.

Une partie du problème tient au fait que les fraudeurs peuvent tirer parti de cette faille; c'est pourquoi des contrôles sont en place. En réalité, si vous êtes vraiment victime d'un vol d'identité et que quelqu'un a contracté un emprunt en votre nom, cette information sera effacée de votre dossier.

Le président: Disposez-vous de données provenant des grandes banques canadiennes qui vous permettraient d'établir quel pourcentage des victimes d'escroquerie ou de fraude sont des personnes âgées, c'est-à-dire des personnes qui ont au moins 65 ans?

Anthony Ostler: Je ne dispose pas de ces données, mais je dirais que tous les Canadiens sont victimes d'escroqueries. Ce qui tend toutefois à se produire, c'est que les sommes d'argent varient.

Souvent, les personnes de plus de 65 ans ont épargné toute leur vie pour pouvoir prendre leur retraite; par conséquent, le montant des pertes est logiquement plus élevé, d'après ce que nous avons constaté.

Le président: Cependant, diriez-vous que les personnes âgées représentent un pourcentage global disproportionné des victimes de fraude ou des personnes visées par la fraude, que celle-ci se soit concrétisée ou non? Ne disposez-vous pas de données sur lesquelles vous pourriez vous appuyer pour étayer cette affirmation en ce moment?

Anthony Ostler: Tous les Canadiens sont des cibles, au point qu'un adolescent de 15 ans pourrait l'être lui aussi...

Le président: Je comprends que tous les Canadiens sont à risque, mais ce n'est pas là ma question. Ma question est la suivante: les personnes âgées sont-elles victimes de la fraude d'une manière disproportionnée au Canada?

Anthony Ostler: C'est le cas pour ce qui est du montant en dollars.

Je pense que vous pourriez peut-être avoir un entretien avec Chris Lynam, le directeur du Centre antifraude du Canada. M. Lynam est un expert en la matière. Cet établissement recueille toutes les statistiques et dispose de données démographiques, donc...

Le président: Monsieur Ostler, ce sera mon dernier point. Ce que je veux dire, c'est ceci: vous représentez les banques.

Anthony Ostler: Oui.

Le président: D'accord. Si je suis client d'une banque et que 100 personnes ont été victimes d'une arnaque ou d'une fraude impliquant cette banque au Canada, je veux savoir si, parmi elles, il y en a au moins 50 qui ont plus de 65 ans. C'est en gros ce que j'essaie de cerner.

Anthony Ostler: Je n'ai pas...

Le président: Je comprends votre argument selon lequel tous les Canadiens sont visés par la fraude, et il est logique de conclure que, plus un Canadien est âgé, plus son compte bancaire contient une somme importante. Cependant, j'essaie ici de comprendre si l'ampleur du problème qui se pose à nous nécessite que nous l'abordions plus directement. Par exemple, vous avez beaucoup parlé de la sensibilisation du public et de la collaboration avec celui-ci. Eh bien, si nous partons de l'hypothèse que les personnes âgées sont victimisées d'une manière disproportionnée, cela oblige le gouvernement à réorienter sa réflexion pour comprendre qui sont les personnes les plus vulnérables et lesquelles il aide.

Je comprends que vous ne disposez peut-être pas de ces éléments. J'aimerais vraiment que vous puissiez transmettre au Comité, par l'intermédiaire de la greffière, à titre de suivi, les données qui sont effectivement accessibles au public. Cela pourrait nous aider à mieux cerner, d'un point de vue démographique et en fonction de l'âge, les groupes les plus ciblés dans le pays.

● (1220)

Anthony Ostler: Oui, nous le ferons.

J'aimerais ajouter que l'Agence de la consommation en matière financière du Canada prescrit un code de conduite pour les aînés que les banques respectent. De nombreux contrôles et processus existent pour soutenir les aînés.

Outre la sensibilisation aux escroqueries et à la fraude et l'information diffusée à ces égards, il y a, par exemple, les cas de maltraitance ou d'exploitation financière des aînés; c'est pourquoi notre site Web comporte des programmes et des outils pour renseigner les aînés et les aider à éviter diverses situations, non seulement les escroqueries ou la fraude, mais aussi les cas où des fraudeurs cherchent à les déposséder de leur argent. De nombreuses initiatives sont lancées, mais le code pour les aînés joue un rôle essentiel dans la protection des aînés.

Le président: Merci. Je vous en suis reconnaissant.

Messieurs les témoins, merci beaucoup de nous avoir consacré votre temps et d'avoir comparu devant nous aujourd'hui. Vos connaissances nous sont précieuses et utiles; nous pouvons maintenant entamer cette importante étude d'une façon constructive.

Chers collègues, comme les votes auront lieu à 12 h 34, je crois, je vais suspendre la séance jusqu'à ce que la période de vote de 10 minutes soit terminée, ou que vous m'ayez tous indiqué que vous avez fini de voter, ce qui nous amènera à 12 h 44 environ. Nous reprendrons alors cette conversation. Pour l'instant, la séance est suspendue.

● (1220)

(Pause)

● (1250)

Le président: Nous reprenons nos travaux là où nous nous sommes arrêtés, conformément à l'engagement que nous avons pris.

Madame Dancho, vous avez présenté une motion. Afin d'éviter de vous prêter des propos que vous n'avez pas tenus, je vais vous demander d'expliquer brièvement l'objet de votre motion pour nous rafraîchir la mémoire. Ensuite, je poursuivrai en conséquence.

Merci.

Raquel Dancho: Merci, monsieur le président.

Je demande le consentement unanime pour adopter la motion suivante:

> Que le Comité fasse rapport à la Chambre de sa condamnation du recours au travail forcé dans les chaînes d'approvisionnement, particulièrement en Chine; qu'il rejette les tarifs américains injustifiés qui menacent les travailleurs et les industries du Canada; et qu'il demande au gouvernement libéral de renforcer l'interdiction canadienne actuelle visant les importations issues du travail forcé et de prendre des mesures plus efficaces pour empêcher l'entrée au Canada de biens fabriqués au moyen du travail forcé.

Cela fait suite à de nombreux débats tenus par le Comité. Je pense que nous avons formulé la motion en des termes qui exposent clairement la question de façon équitable, en nous appuyant sur nos conversations antérieures. Les conservateurs en soutiennent l'adoption, tout comme le Bloc québécois, qui en préconise aussi la transmission à la Chambre; c'est pourquoi nous demandons aux députés libéraux de nous accorder leur consentement unanime pour ce faire.

Merci, monsieur le président.

Le président: Merci, madame Dancho.

Pour plus de clarté, vous me demandez de solliciter le consentement unanime pour que cette motion soit adoptée.

Je rappelle aux députés que la motion a été présentée par madame Dancho avant la suspension de la séance un peu plus tôt. Nous ne votons pas sur la tenue d'un débat sur la motion, qui fait maintenant l'objet d'un avis officiel. Nous votons pour établir si nous adoptons la motion par consentement unanime, ce qui est nécessaire, car la motion n'a pas déjà fait l'objet d'un avis.

Sur ce, je sollicite le consentement unanime. Autant que je puisse voir, il n'y a pas de consentement unanime. Par conséquent, madame Dancho, nous ne pourrons pas aller de l'avant.

Ted Falk: Y aura-t-il un vote par appel nominal?

Le président: Monsieur Falk, comme il ne s'agit pas d'un vote à proprement parler, nous ne pouvons pas tenir un vote. Comme nous avons besoin d'un consentement unanime, ne serait-ce que pour autoriser un vote, le compte rendu ne fera aucune mention d'un tel vote.

Chers collègues, nous devions poursuivre notre discussion à huis clos sur l'étude relative aux fabricants de moules, mais, compte tenu de l'heure qu'il est, je ne pense pas que nous puissions aborder ce sujet en profondeur à ce stade-ci. Je propose donc de lever la séance; nous réviserons l'horaire afin de trouver une occasion d'apporter la dernière main à la deuxième version.

Sur ce, la séance est levée.