



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

45^e LÉGISLATURE, 1^{re} SESSION

Comité permanent de l'industrie et de la technologie

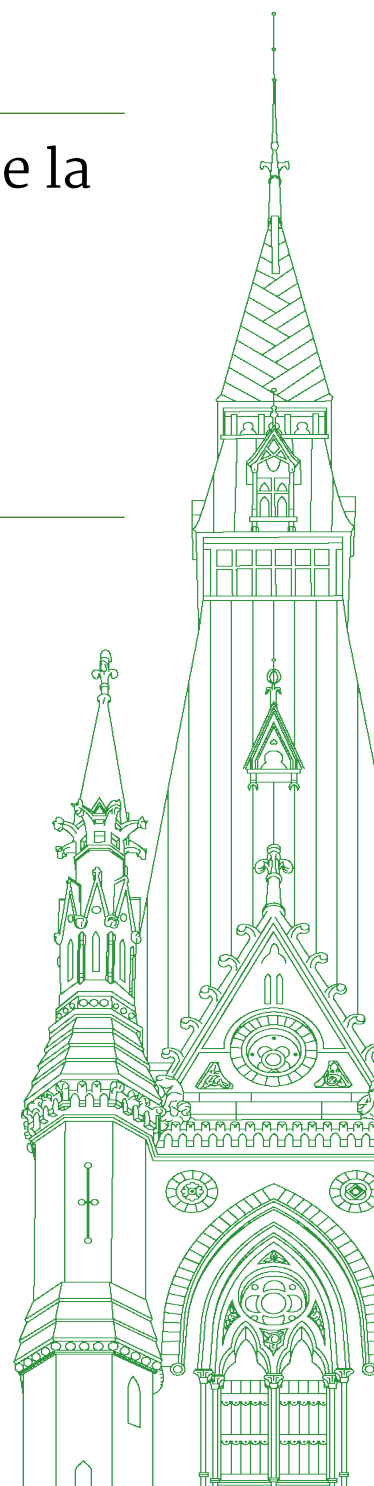
TÉMOIGNAGES

NUMÉRO 043

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le lundi 8 juin 2026

Président : Ben Carr



Comité permanent de l'industrie et de la technologie

Le lundi 8 juin 2026

• (1630)

[Français]

Le président (Ben Carr (Winnipeg-Centre-Sud, Lib.)): Bon après-midi, tout le monde.

Malheureusement, à cause de la tenue des votes, nous sommes un peu en retard cet après-midi, mais nous allons y remédier au cours des prochaines heures.

[Traduction]

J'espère que vous passez une bonne journée jusqu'à présent, malgré les interruptions pour le vote.

Je m'excuse aux témoins de les faire attendre. C'est simplement ainsi que les choses fonctionnent au Parlement; je vois que l'horloge indique 16 h 29, nous commençons donc en fait pile à l'heure. Je suis ravi que nous puissions commencer nos travaux.

Chers collègues, il s'agit de notre deuxième réunion pour notre étude sur la fraude et les escroqueries au Canada.

[Français]

Chers collègues, je peux vous confirmer que tous les tests audio-visuels ont été effectués et que tout est correct.

[Traduction]

Je tiens à rappeler aux témoins que, si vous utilisez une oreillette et qu'elle est branchée, mais pas sur votre oreille, vous devez la placer sur l'autocollant, devant vous. On veut protéger la santé et le bien-être de nos interprètes.

Sur ce, aujourd'hui, nous accueillons quatre témoins en personne. Nous accueillons M. David Shipley, directeur général, de Beauceron Security; Mme Jennifer Quaid, directrice exécutive, de l'Échange canadien de menaces cybernétiques; et M. Jon Camfield, responsable de la défense, Politique sur la sécurité; et Mme Rachel Curran, directrice, Politique publique, tous deux de Meta Canada.

Bienvenue.

Les témoins auront chacun cinq minutes pour faire leurs déclarations préliminaires. Je crois que M. Camfield parlera au nom de Meta.

Sur ce, monsieur Shipley, allez-y.

David Shipley (directeur général, Beauceron Security): Merci, monsieur le président. Merci de me donner l'occasion de comparaître de nouveau devant le Comité.

Beauceron Security a aidé plus d'un million de personnes à détecter et à contrer les cyberattaques et les escroqueries en ligne. J'ai passé plus d'une décennie à étudier la manière dont les cybercriminels exploitent la confiance des internautes. C'est une activité en

plein essor. Erin West, fondatrice d'Operation Shamrock, une organisation internationale de lutte contre la fraude, a dit qu'il s'agissait d'une véritable pandémie d'escroqueries.

La fraude a encore connu une recrudescence au Canada, en 2025; les pertes déclarées s'élèvent à plus de 700 millions de dollars, mais le montant réel des pertes se situerait probablement entre 7 et 14 milliards de dollars, puisque seulement 5 à 10 % des fraudes sont signalées. Au Canada, les pertes liées à la fraude ont augmenté de 326 % depuis 2020. Nous sommes perdants, et nous perdons bien plus que de l'argent. La fraude détruit des familles canadiennes et plonge les aînés dans la misère.

Je vais être franc; je vais vous dire sur quel front nous perdons. Imaginez l'économie de l'escroquerie comme un entonnoir, où chaque groupe se trouve à un niveau différent; les plateformes en ligne qui vendent des espaces publicitaires aux escrocs et qui empochent les profits se trouvent tout en haut de l'entonnoir. Les produits d'une entreprise en particulier se démarquent de tous les autres. Récemment, *l'Independent* a rapporté que, selon Lloyds, au Royaume-Uni, deux tiers des fraudes dont sont victimes leurs clients commencent sur les plateformes de Meta. C'est vraiment ironique de voir que Facebook bloque du contenu médiatique canadien authentique, tout en autorisant gaiement des vidéos frauduleuses générées par l'intelligence artificielle, montrant des hypertrucages de politiciens faisant la promotion d'escroqueries à l'investissement, et en versant de l'argent dans de faux comptes qui encouragent la séparation de l'Alberta.

Selon ce qu'a rapporté Reuters en novembre dernier, les propres projections internes de Meta montrent que l'entreprise devrait gagner 16 milliards de dollars à l'échelle mondiale en un an grâce aux publicités frauduleuses et aux publicités pour des biens interdits. Cela représente environ 10 % de son chiffre d'affaires mondial. J'aimerais connaître les estimations concernant la valeur et le nombre des publicités frauduleuses ciblant les Canadiens. Meta a ces chiffres.

Le comté de Santa Clara, dans la Silicon Valley, et une coalition américaine ont engagé des poursuites contre Meta, l'accusant d'avoir sciemment tiré profit de publicités frauduleuses. La corruption commence tout en haut. Tout le monde écope, tandis que Meta gagne des milliards de dollars.

J'aimerais parler des points suivants au Comité et lui demander d'en tenir compte dans ses études.

Premièrement, les plateformes en ligne doivent être responsables des publicités frauduleuses dont elles tirent profit. Si elles ne parviennent pas à surveiller correctement leurs plateformes, c'est elles qui en paieront le prix, et non les banques ou les Canadiens. Nous devons les obliger à rendre compte à des organismes fédéraux des fraudes signalées et des mesures qu'elles prennent pour les combattre.

Deuxièmement, il faut établir, par voie législative, un délai d'attente de 24 heures pour les transactions importantes et inhabituelles qu'un établissement financier signale comme suspectes. Les clients peuvent décider de ne pas y participer, mais le cas échéant, ils ne pourront pas être remboursés. Cette mesure suffirait à elle seule à protéger les personnes contre les arnaques sentimentales et les arnaques à l'investissement, les deux catégories les plus coûteuses. Cela aiderait à dissiper l'illusion amoureuse des victimes, qui peut se développer pendant ce genre d'arnaque sophistiquée.

Troisièmement, il ne faut pas bâtir un modèle de responsabilité qui repose uniquement sur les banques. Nous l'avons appris à nos dépens, dans le domaine de la cybersécurité, avec les rançongiciels. Dès que les assureurs ont commencé à verser des indemnités, les attaques se sont multipliées. Si les banques sont les seules responsables, les coûts liés à la fraude ne feront qu'augmenter pour les Canadiens ordinaires. Au bout du compte, les banques n'assument jamais ces coûts. Les coûts seront répercutés sur vos électeurs sous forme de frais de services et d'intérêts.

Il doit y avoir une responsabilité partagée entre les plateformes en ligne, les banques et les clients des banques. Les banques devraient proposer à leurs clients des formations sur la fraude et assurer un suivi. Sans rétroaction, les programmes de sensibilisation à la fraude sont peu efficaces. D'une part — et nous l'avons montré dans notre travail d'éducation des employés —, cela incite les gens à adopter des comportements moins risqués. Si un client ne prend pas 10 minutes pour apprendre, cela devrait être pris en compte dans le calcul de son remboursement. C'est cela, la responsabilité partagée.

Voici ce que montrent nos données. D'après notre travail auprès d'employés, ceux qui estiment ne pas jouer un rôle dans leur propre protection ou celle de leur entreprise cliquent 37 % plus souvent sur des courriers frauduleux que ceux qui estiment avoir un rôle à jouer à cet égard. Les gens renseignés et motivés à se protéger sont moins souvent victimes de fraudes et signalent davantage les activités suspectes.

Quatrièmement, il faut doter le Centre antifraude du Canada de ressources suffisantes. Il n'arrive pas à traiter le volume d'appels qu'il reçoit, et son travail ne se limite pas à simplement consigner les détails. Ce centre est une véritable bouée de sauvetage pour les victimes de fraude en détresse qui envisagent se faire du mal. Soyez transparents en ce qui concerne le financement du centre, pour que les Canadiens comprennent comment nous investissons pour lutter contre la fraude. Les amendes infligées aux géants de la technologie, qui tirent profit de la fraude dont sont victimes les Canadiens, pourraient servir à financer le centre.

J'ai une dernière demande. J'implore le Comité d'utiliser tous les pouvoirs dont il dispose pour établir si Meta a tiré sciemment profit des fraudes, comme le prétend l'article de *Reuters*. Les Canadiens méritent de connaître la vérité.

Merci; je suis prêt à répondre à vos questions.

Le président: Merci beaucoup, monsieur Shipley.

Madame Quaid, allez-y, s'il vous plaît; vous avez cinq minutes.

Jennifer Quaid (directrice exécutive, Échange canadien de menaces cybernétiques): Merci, monsieur le président.

Merci à tous les députés présents de me donner l'occasion de comparaître devant vous aujourd'hui au nom de l'Échange canadien de menaces cybernétiques et de la Coalition canadienne antifraude.

La Coalition canadienne antifraude est la plus grande coalition au Canada de lutte contre les escroqueries; elle rassemble des chefs de file des secteurs des services financiers, des télécommunications et des technologies, ainsi que des représentants des gouvernements, des organismes de réglementation et des organismes d'application de la loi. Nous faisons ce travail parce que la fraude n'est plus qu'un simple désagrément. C'est le plus important crime financier de notre époque. Chaque année, il touche des millions de Canadiens, coûte des milliards de dollars et mine la confiance du public dans nos systèmes. Ce n'est pas une simple tendance. C'est une menace persistante et croissante.

J'aimerais parler de trois mesures que le Canada peut prendre pour infléchir la tendance.

Premièrement, nous avons besoin d'une approche faisant véritablement intervenir toute la société. Les institutions financières, les entreprises de télécommunications, les plateformes numériques, les organismes de réglementation, les organismes d'application de la loi et le gouvernement doivent collaborer activement, se fixer des objectifs communs, coordonner leurs politiques et mettre l'accent sur la prévention en amont. Les escrocs font fi des frontières organisationnelles. Ils mènent chaque jour leurs activités en utilisant les réseaux de télécommunications, les systèmes bancaires et les plateformes de médias sociaux pour atteindre les téléphones cellulaires des Canadiens. Aucune organisation ne peut à elle seule les arrêter.

D'autres pays l'ont reconnu. Le Royaume-Uni a créé Stop Scams UK, l'Australie a mis sur pied le National Anti-Scam Centre et Singapour a réuni les banques et les entreprises de télécommunications dans un même cadre opérationnel. Le Canada a la volonté et le talent nécessaires pour faire de même. Ce qui nous manque, c'est l'architecture.

Deuxièmement, il faut comprendre que la fraude fait partie de l'écosystème plus vaste de la cybercriminalité et du blanchiment d'argent. L'infrastructure utilisée pour voler des informations de connexion est aussi utilisée pour commettre des fraudes. Les réseaux utilisés pour blanchir les produits du narcotrafic servent aussi à transférer des fonds volés à l'étranger. Nous avons besoin d'une approche coordonnée qui lie le Centre d'analyse des opérations et des déclarations financières du Canada, le Centre antifraude du Canada, les fonctions de cyberdéfense et le secteur privé, et nous devons comprendre que la fraude est un fil conducteur qui les lie tous.

Troisièmement, et c'est peut-être le point le plus urgent, la lutte contre la fraude nécessite un échange rapide de l'information. Aujourd'hui, une banque, un fournisseur de services de télécommunications et une plateforme numérique peuvent chacun identifier la même activité frauduleuse, mais il n'existe aucun mécanisme efficace leur permettant de partager cette information en temps réel. C'est pourquoi chaque organisation ne voit qu'une partie du tableau, alors que les escrocs partagent des informations instantanément et exploitent les lacunes créées par le cloisonnement des systèmes et la désuétude de la réglementation.

La Coalition canadienne antifraude a été créée entre autres pour s'attaquer à ce problème, mais nous avons besoin de cadres législatifs et réglementaires pour permettre un partage d'information responsable. D'autres pays ont franchi ce pas. Le Canada peut en faire autant, et nous avons l'occasion d'agir en tant que chef de file.

La menace à laquelle nous faisons face ne vient pas d'amateurs opportunistes. Il s'agit de réseaux de criminels organisés, qui utilisent des technologies sophistiquées et qui suivent des modèles opérationnels professionnels. Si nos interventions restent fragmentées, les escrocs continueront à nous déjouer.

La prévention doit être notre objectif principal. Cela suppose une intervention en temps réel sur les transactions, la perturbation du réseau des infrastructures utilisées pour les escroqueries et une campagne d'éducation publique significative qui s'adresse aux Canadiens vulnérables là où ils se trouvent et d'une manière qu'ils peuvent comprendre.

Le Canada a l'occasion de développer une intervention de calibre mondial. Le secteur privé veut s'impliquer. Nos organismes d'application de la loi comprennent la menace et veulent en faire plus. Aujourd'hui, nous avons besoin de cadres qui brisent les cloisonnements, favorisent une véritable collaboration, allouent des ressources significatives là où elles sont nécessaires et accordent la priorité à la prévention. La Coalition canadienne antifraude et l'Échange canadien de menaces cybernétiques sont prêts à bâtir cette infrastructure.

• (1635)

Le président: Merci beaucoup, madame Quaid.

Monsieur Camfield, allez-y, vous avez cinq minutes.

Jon Camfield (responsable de la défense, Politique sur la sécurité, Meta Platforms Inc.): Merci, monsieur le président.

Bonjour. Merci à vous tous de me donner l'occasion de paraître devant le Comité aujourd'hui. Je m'appelle Jon Camfield. Je dirige nos travaux sur les politiques en matière de confiance et de sécurité mondiales touchant la fraude et les escroqueries. Ma collègue, Mme Rachel Curran, directrice de la Politique publique, de Meta Canada, est ici avec moi.

Meta prend très au sérieux la menace que représentent la fraude et les escroqueries. Les criminels motivés par l'argent sont l'une des menaces les plus tenaces et les plus agiles auxquelles nous faisons face aujourd'hui sur Internet. Ces réseaux opèrent sur plusieurs plateformes, exploitent divers secteurs et agissent souvent en toute impunité depuis des pays où l'État de droit est limité.

En 2025 seulement, nous avons pris des mesures à l'encontre de plus de 10 millions de comptes liés à des centres de fraude criminelle, qui sont des organisations criminelles structurées menant des activités frauduleuses à grande échelle grâce à la traite et à l'exploitation de personnes. Des centaines de milliers de victimes sont derrière ces escroqueries. Nous faisons des investissements importants pour détecter et supprimer les acteurs et les contenus frauduleux, et nous entretenons des partenariats actifs avec les organismes d'application de la loi, les organismes de réglementation et le secteur, au Canada, pour lutter contre la fraude.

Notre approche est multidimensionnelle et axée sur les résultats.

Nous avons des politiques spécifiques concernant la fraude, les escroqueries et les pratiques trompeuses pour l'ensemble de nos plateformes — Facebook, Instagram, Threads, Messenger et What-

sApp — et aussi pour les publicités qui circulent sur toutes nos plateformes. En 2025, nous avons retiré plus de 159 millions de publicités, à l'échelle mondiale, qui contrevenaient à ces politiques. Nous en avons supprimé 92 % de manière proactive, avant même qu'elles ne nous soient signalées. Globalement, nous avons réduit de plus de 50 % le signalement d'annonces frauduleuses sur l'ensemble de nos plateformes au cours de la même période.

En plus de veiller au respect de nos politiques, nous redoublons sans cesse d'efforts sur nos plateformes pour dissuader les escrocs. Voici quelques exemples. Premièrement, nous renforçons la vérification des annonceurs; notre objectif, c'est que 90 % de nos revenus publicitaires viennent d'annonceurs confirmés d'ici la fin de 2026, comparativement à 70 % à la fin de 2025. Deuxièmement, nous déployons des outils d'IA avancés pour empêcher les escrocs d'utiliser des personnalités publiques dans leurs publicités frauduleuses et trompeuses. Troisièmement, sur Messenger, nous déployons également une intelligence artificielle intégrée à l'appareil pour détecter les comportements suspects dans les conversations et avertir les utilisateurs en temps réel, même dans les discussions chiffrées de bout en bout.

Alors que le gouvernement élabore la toute première stratégie canadienne de lutte contre la fraude, nous devons nous rappeler que la collaboration intersectorielle est essentielle. Aucune entreprise ni aucun secteur ne peut, à lui seul, avoir le portrait complet de la chaîne des attaques frauduleuses. Un escroc peut d'abord contacter un consommateur par message texte ou sur les réseaux sociaux, peut l'inciter à appeler ou à consulter un site d'investissement frauduleux, pour lui soutirer de l'argent grâce à une transaction en cryptomonnaie ou un virement bancaire. Chaque secteur a une vision limitée, et aucune entreprise ni plateforme n'a une vue d'ensemble complète. Pour lutter efficacement, nous devons partager des informations au-delà de ces frontières.

C'est pourquoi Meta investit énormément dans le partage intersectoriel d'information. Grâce à notre Fraud Intelligence Reciprocal Exchange, le FIRE, nous échangeons des informations de manière bidirectionnelle avec les institutions financières, ce qui nous permet d'agir plus rapidement. Grâce à Global Signal Exchange, nous partageons des indicateurs d'escroquerie structurés — adresses URL de sites malveillants, numéros de téléphone et comptes publicitaires — avec les gouvernements et le secteur à l'échelle du globe. Les entités gouvernementales peuvent participer gratuitement au GSE.

Ici, au Canada, Meta soutient la campagne Ensemble contre la fraude, avec l'Association des banquiers canadiens. Nous avons des canaux de signalement dédiés avec le Centre antifraude du Canada, la Gendarmerie royale du Canada, le groupe d'intervention sur la fraude en matière d'investissements des Autorités canadiennes en valeurs mobilières et le Bureau de la concurrence.

Nous avons participé à l'Opération Érable avec des organismes d'application de la loi, des organismes de réglementation des valeurs mobilières et des institutions financières du Canada. De plus, Meta a aussi soutenu le Cadre mondial de partenariat public-privé contre la fraude de l'Office des Nations Unies contre la drogue et le crime. Nous sommes aussi l'un des signataires fondateurs de l'Industry Accord Against Scams and Fraud, l'accord sectoriel de lutte contre les escroqueries et la fraude en ligne, avec Google, Amazon, Microsoft, OpenAI, et bien d'autres entreprises.

Alors que le Parlement cherche les meilleurs moyens de protéger les Canadiens contre la fraude, nous recommandons trois mesures. La première, c'est une approche globale de l'écosystème, qui réunit dès le départ tous les secteurs touchés par la chaîne des attaques frauduleuses: les plateformes numériques, les services de télécommunications, les institutions financières, les entreprises de technologies financières et les organismes d'application de la loi. La deuxième, c'est des cadres de partage d'information solides, avec des dispositions législatives d'exonération, pour que les entreprises puissent collaborer de bonne foi, sans craindre d'être tenues responsables au titre des lois sur la protection de la vie privée ou du droit à la concurrence. La troisième, c'est un cadre axé sur les résultats, qui mesure les résultats plutôt que d'imposer des méthodes spécifiques, ce qui permet à tous de rester le plus flexible possible face à l'évolution rapide des stratégies de fraude.

Merci de m'avoir écouté. Nous sommes disposés à répondre à vos questions.

• (1640)

Le président: Merci beaucoup, monsieur Camfield.

Chers collègues, nous allons maintenant passer à la première série de questions.

Madame Borrelli, vous avez la parole pour six minutes.

Kathy Borrelli (Windsor—Tecumseh—Lakeshore, PCC): Merci, monsieur le président.

Ma première question s'adresse à M. Shipley.

Monsieur Shipley, on dit souvent aux personnes âgées de porter une attention particulière aux signaux d'alerte, mais ceux-ci sont de plus en plus difficiles à détecter, puisque l'on parle maintenant de faux numéros de téléphone, de voix générées par l'intelligence artificielle, de fausses publicités d'investissement et d'arnaques avec usurpation d'identité. Compte tenu de votre expérience de l'éducation en matière de cybersécurité, quel genre de prévention fonctionne réellement pour les Canadiens âgés? Plus précisément, qu'est-ce que le Canada pourrait faire différemment pour protéger les personnes âgées, puisque les arnaques sont de plus en plus complexes et qu'il n'est plus seulement question de détecter des signaux d'alarme?

David Shipley: La première chose que nous avons constatée dans nos recherches — et oui, vous avez raison —, c'est que les indicateurs techniques qui nous permettent de dire s'il s'agit d'un courriel d'hameçonnage ou d'une arnaque sont très difficiles à déceler, maintenant, en partie à cause des entreprises d'intelligence artificielle qui conçoivent des outils qui donnent aux choses un air plus réel, plus rapidement que jamais.

Nos recherches et celles de l'Université métropolitaine de Toronto ont montré qu'il était utile d'enseigner aux gens ce qu'est l'intelligence émotionnelle, de leur montrer à écouter leur instinct et à se demander pourquoi quelqu'un essaie de leur faire ressentir certaines choses, qu'il s'agisse de déclencher une poussée d'adrénaline ou de leur présenter quelque chose qui les emballe. Ces arnaqueurs profitent souvent de la solitude qui mine notre pays.

Ce qui peut aider le plus nos personnes âgées à l'heure actuelle, c'est la retenue de 24 heures. J'ai discuté avec beaucoup de banques, et leurs équipes savent que c'est une arnaque, mais la personne est tombée amoureuse. Elle pense qu'un être cher est en danger et qu'elle doit agir. Si cette mesure de sécurité est en place — et il est important de comprendre que cette mesure de sécurité est en place

pour tout le monde, d'emblée; il y a par contre une option de non-participation — nous arrêterions énormément de ces fraudes les plus dispendieuses qui ciblent nos personnes âgées.

• (1645)

Kathy Borrelli: Vous avez déjà répondu en partie à ma question de suivi, qui est la suivante: quelles seraient les trois choses les plus importantes à inclure dans un programme de prévention de la fraude qui aideraient nos aînés?

David Shipley: Dans ma déclaration préliminaire, j'ai mis des notes en bas de page pour toutes les histoires que j'ai mentionnées. Darren Taylor a écrit une histoire déchirante pour *Orillia Matters*, le 5 juin, et je vous encourage tous à la lire; elle est intitulée « *Senior Lost almost \$1M in 'increasingly common' deepfake scam* », et c'est l'histoire d'une personne âgée qui a perdu près de 1 million de dollars dans une arnaque hypertruquée « de plus en plus courante ». Ces arnaques sont de plus en plus courantes sur les plateformes, sur Meta, mais sur d'autres plateformes aussi. Elles mettent en scène notre premier ministre et d'autres personnes. Le premier ministre Doug Ford a aussi été la vedette de l'une de ces arnaques et une personne âgée de la région du Grand Toronto a perdu 100 000 \$.

Nous devrions exiger que les plateformes surveillent cela. Si elles ne peuvent pas offrir de la publicité de façon responsable, elles devraient s'arrêter là.

Kathy Borrelli: Devrions-nous imposer des règles plus strictes concernant les premiers transferts, les achats de cryptomonnaie, les virements ou les paiements internationaux effectués sur un logiciel d'accès à distance?

David Shipley: Oui, et il y a beaucoup à faire de ce côté-là, mais rappelez-vous que, une fois que l'arnaqueur a tissé une relation à long terme avec sa victime, il l'incitera à faire des choses en la contrôlant par divers moyens. Comme l'a dit ma collègue, Mme Quaid, d'Échange canadien de menaces cybernétiques, c'est toute la société qui doit fournir des efforts pour lutter contre cela, mais tout cela aidera.

Kathy Borrelli: Madame Quaid, j'aimerais savoir ce qui se passe après qu'une personne âgée a été arnaquée. Dans de nombreux cas, la victime signale la fraude, mais l'argent est déjà passé dans le système, par des portefeuilles de cryptomonnaie, des comptes mules ou des canaux étrangers. La victime peut avoir l'impression que le système consigne sa perte, mais qu'il n'agit pas suffisamment rapidement pour récupérer l'argent.

Que doit faire le Canada pour retracer, geler et récupérer plus rapidement les fonds volés après qu'une personne âgée a signalé une arnaque?

Jennifer Quaid: Malheureusement, les preuves montrent que les aînés ont tendance à ne pas signaler qu'elles ont été victimes d'une arnaque; elles le font beaucoup moins que les autres tranches d'âge de la société. La plupart des personnes âgées qui le signalent sont celles qui ont perdu beaucoup moins d'argent ou qui ont détecté une arnaque sans en avoir été la victime. C'est un problème en soi.

Que peut faire le système? Il peut se concentrer sur la prévention. Peu importe ce que nous faisons, ce ne sera jamais assez rapide. Ce ne sera jamais suffisant. L'intelligence artificielle et les frontières de l'intelligence artificielle font en sorte qu'il est très difficile pour quiconque de détecter les arnaques, et pas juste pour les aînés. Si nous ne nous concentrons pas sur la prévention, nous continuons tout simplement de jouer au jeu de la taupe.

Kathy Borrelli: Merci beaucoup.

J'ai terminé.

Le président: Merci beaucoup, madame Borrelli.

Monsieur Bains, c'est à vous. Si je comprends bien, vous allez partager votre temps avec M. Ntumba. Je vais vous laisser départager cela entre vous.

Vous avez la parole, monsieur.

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

Merci beaucoup à nos témoins de s'être joints à nous aujourd'hui pour cette étude très importante.

Je n'ai pas pu m'empêcher de constater que Meta et Mme Quaid ont fait des recommandations très similaires.

Monsieur Shipley, vous avez parlé du rapport de Reuters. Je vais revenir un peu là-dessus, puis je vais poser des questions aux représentants de Meta.

Meta avait prévu qu'environ 10 % de ses revenus en 2024 proviendraient de publicités liées à des arnaques, à des biens interdits ou à du contenu trompeur.

Monsieur Camfield, vous avez dit avoir retiré plus de 159 millions de publicités trompeuses l'année dernière seulement. Ces mêmes documents indiquent que les utilisateurs de Meta auraient visionné chaque jour 15 milliards de publicités trompeuses à risque élevé, et que vous les laissez souvent passer, sauf si vous êtes certain à 95 % qu'il s'agit d'une fraude.

Voici ma question: quand il s'agit d'infractions incertaines, Meta choisit plutôt de demander des tarifs publicitaires plus élevés pour dissuader les délinquants, qui profitent toujours dans les faits des fraudes possibles. Pourquoi Meta a-t-il établi un seuil si élevé pour établir s'il s'agit d'une arnaque ou non? Pourquoi parle-t-on de 95 %?

• (1650)

Jon Camfield: Laissez-moi parler un peu des chiffres précis. Le 10 % était fondé sur une recherche interne visant à identifier le nombre maximal d'infractions possibles. Ce chiffre incluait du contenu en règle qui se retrouve souvent dans nos systèmes. Cela incluait aussi du contenu qui n'est pas réellement une fraude ou une arnaque. C'est un chiffre plus élevé que ce qu'il est en réalité.

Il est aussi indiqué, dans le document qui a fait l'objet d'une fuite dont parlait l'article de Reuters, en 2024, que le chiffre réel se situe sans doute entre 3 et 4 %. Encore une fois, c'était en 2024. Nous avons diminué cela de moitié en 2025, et nous travaillons toujours là-dessus aujourd'hui.

Pour ce qui est de demander un tarif plus élevé, le système de vente aux enchères de publicités est très complexe. Il diminue la valeur des enchères si nous soupçonnons, sans pouvoir le prouver, qu'une publicité est une arnaque.

Voilà où nous en sommes sur la chaîne des attaques frauduleuses. Ce que nous voyons, c'est le tout début d'une arnaque qui prend souvent la forme d'une publicité comme les autres, d'un engagement comme les autres ou du début d'une nouvelle amitié. C'est difficile...

Parm Bains: Je vais vous interrompre compte tenu du temps qu'il me reste.

Dans ce cas, comment vérifiez-vous la légitimité? Avez-vous un processus inverse, ou quelque chose du genre?

Jon Camfield: Nous avons deux ou trois processus. L'un d'eux est le partage d'information. L'un de nos signaux les plus importants, c'est quand les banques nous disent « attention, ce sont des comptes frauduleux qui se servent de ces URL, de ces domaines et de ces identifiants. Pourriez-vous regarder dans vos systèmes? » Nous prenons ces informations, les entrons dans nos systèmes, faisons une distribution et recherchons d'autres signaux semblables. Nous sommes souvent capables de générer jusqu'à 600 fois plus d'information dans nos systèmes à partir de n'importe quelle information unique reçue des banques. C'est l'information la plus importante.

Parm Bains: Enfin, avant de céder le reste de mon temps à M. Ntumba, j'aimerais souligner que le groupe de défense des consommateurs Consumer Federation of America a déposé une plainte similaire, alléguant que Meta n'a pas bloqué les publicités frauduleuses, mais a demandé plus d'argent aux annonceurs tout en réduisant ses efforts de lutte contre les arnaques. Que répondez-vous à cela?

Ensuite, monsieur Ntumba, vous avez la parole.

Jon Camfield: Je répondrais que nous n'imposons pas de tarifs plus élevés aux annonceurs. Nous diminuons la valeur des publicités frauduleuses possibles — les publicités douteuses ou possiblement incertaines — dans notre système d'enchères. Cela veut dire que, puisque nous pénalisons cette publicité, à long terme, celle-ci nous rapporte moins d'argent, car nous laissons une autre annonce remporter l'enchère. Cela ne veut pas dire que nous leur imposons un tarif plus élevé, et ils ne peuvent pas nous donner plus d'argent pour obtenir un meilleur placement publicitaire. C'est seulement une question de réduire la valeur de leur enchère.

Parm Bains: Merci.

[Français]

Bienvenu-Olivier Ntumba (Mont-Saint-Bruno—L'Acadie, Lib.): Merci.

Monsieur Camfield, vous savez, Meta, c'est quasiment comme une ville, une nation, une concession ou un centre commercial, dans lesquels il y a plusieurs maisons et plusieurs commerces, et où les gens circulent. Chaque personne est responsable de mettre l'alarme à la porte de sa maison. Vous assurez la sécurité de l'ensemble, la porte d'entrée principale. Je comprends que les banques ont pour approche de dire aux clients que, s'ils ont une carte bancaire, ils en sont responsables. À ma maison, je mets l'alarme et je tourne la clé. Je la sécurise.

Quand les gens vont envahir mon pays, je ne dis pas que c'est la faute du voisin. C'est la faute du gouvernement qui n'a pas sécurisé le pays. Ça revient un peu à Meta.

Comment se fait-il que la fraude continue à grandir au sein de Meta? Je vous pose la question puisque vous êtes responsables de la sécurité de Meta.

[Traduction]

Jon Camfield: C'est un défi. Les arnaqueurs d'aujourd'hui, comme je l'ai dit, sont les adversaires les plus redoutables auxquels nous faisons face en ligne, et cela comprend des acteurs étatiques, des acteurs se livrant à l'espionnage et des logiciels espions. Ils sont industrialisés et à une échelle qu'il est difficile de décrire.

Il est important de penser aux pays d'où ils viennent, habituellement. Nous parlons de centaines de milliers de victimes de la traite de personnes, qui sont passées à tabac si elles ne font pas les arnaques exigées et si elles ne respectent pas leurs quotas. Le PIB des pays où se font ces activités vient à 40 % d'activités frauduleuses, pas seulement sur nos propres plateformes, mais sur toutes les plateformes du monde. Ces personnes sont fortement encouragées à mener ces activités et elles n'ont presque aucune responsabilité.

L'enjeu est de savoir comment lutter contre un adversaire d'une si grande envergure, si déterminé et encouragé par l'aspect financier. Nous devons composer avec des perturbations. Nous devons modifier notre produit pour qu'il soit plus hostile pour les arnaqueurs sans toutefois créer d'obstacles aux utilisateurs ordinaires ou aux entreprises légitimes. Il est difficile de trouver un équilibre, mais nous y travaillons très fort. Nous prenons la menace au sérieux.

• (1655)

[Français]

Le président: Monsieur Ntumba, malheureusement, votre temps de parole est écoulé. Merci.

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

Gabriel Ste-Marie (Joliette—Manawan, BQ): Merci, monsieur le président.

Je salue tous les collègues. Je suis désolé d'être avec vous de façon virtuelle.

Je remercie les quatre témoins d'être des nôtres. Je leur en suis très reconnaissant.

Monsieur Shipley, vous avez terminé votre présentation en suggérant une question qui pourrait être posée à Meta.

Pouvez-vous nous la répéter?

[Traduction]

David Shipley: J'aimerais beaucoup savoir si Meta sait à combien environ s'élève la valeur des publicités frauduleuses qui ciblent les Canadiens. Combien y en a-t-il?

[Français]

Gabriel Ste-Marie: Est-ce que les représentants de Meta peuvent répondre à ça?

[Traduction]

Jon Camfield: Je regrette de vous dire que je n'ai pas ces chiffres, mais je peux les chercher et vous revenir.

[Français]

Gabriel Ste-Marie: D'accord.

Le Comité serait heureux que vous lui fassiez parvenir les données. Merci beaucoup.

Dans *Le Journal de Montréal*, le 11 mai dernier, le Bureau d'enquête a publié un dossier concernant l'hypertrucage, un stratagème qui fait perdre une fortune à des Québécois sur Facebook. Il y a de fausses vidéos de Mark Carney, de François Legault, de Doug Ford et d'influenceurs sur les réseaux sociaux. Il y a même de fausses vidéos de Keanu Reeves, et ainsi de suite. Quatre personnes ont témoigné de leur expérience au *Journal de Montréal*. Deux d'entre elles ont perdu plus de 100 000 \$. Je ne sais pas si vous avez eu connaissance de cet article ou de cette enquête. Les journalistes

disent avoir contacté Meta, qui n'a pas voulu répondre au *Journal de Montréal*.

Qu'avez-vous à dire aux personnes qui se sont fait flouer à cause des hypertrucages sur vos plateformes? Souvent, ce sont les épargnes d'une vie, les épargnes en vue de la retraite.

[Traduction]

Jon Camfield: C'est horrible. Ces crimes sont terribles, et c'est très troublant de voir ce genre de perte, peu importe la situation, mais surtout quand cela concerne des fonds d'épargne-retraite, puisque les gens ont hâte de terminer leur vie active et de prendre leur retraite. C'est horrible. Nous ne voulons pas voir ce genre d'actions sur nos sites.

Nous faisons notre possible pour détecter les hypertrucages et les arnaques qui mettent en scène des célébrités dans les publicités qui circulent sur nos plateformes. Nous avons déployé de nombreuses couches de technologie d'intelligence artificielle qui vérifient non seulement la vue d'ensemble, mais aussi le contexte des publicités hypertruquées.

Quand nous avons déployé cela, nous avons constaté que nos adversaires se sont adaptés immédiatement. Nous avons commencé par cibler les plus grandes célébrités mondiales, et nous avons immédiatement vu l'apparition de célébrités nationales, de célébrités gouvernementales et de politiciens. Au fur et à mesure que nous nous attaquons à la chaîne, les arnaqueurs se déplacent à l'échelon local. C'est utile, parce que cela demande beaucoup d'efforts de leur part. Nous aussi, nous devons en déployer, mais nous sommes contents de le faire.

Il faut s'attendre à cette adaptation et à cette contre-attaque des arnaqueurs, et ce n'est qu'en nous attaquant à toute l'économie qui touche les arnaques que nous pourrions modifier cela.

[Français]

Gabriel Ste-Marie: Je comprends que vous trouviez ça terrible, avec raison. Cependant, ça se passe sur vos plateformes. Je comprends qu'il y a des efforts qui sont déployés, mais les arnaques continuent à se faire sur vos plateformes.

Quelle est votre part de responsabilité par rapport à ces vols?

[Traduction]

Jon Camfield: Je dirais qu'il est très important de discuter les uns avec les autres et de travailler ensemble sur toute la chaîne d'attaques frauduleuses. Les choses qui commencent par un message texte ou sur les médias sociaux prennent de l'ampleur et se déplacent. Elles se retrouvent sur des sites Web — de faux sites d'investissements frauduleux —, mais, même quand on les bloque, elles restent tout de même sur l'Internet ouvert jusqu'à trois ans, ce qui veut dire que l'on s'en sert aussi dans d'autres campagnes, avec d'autres outils et avec d'autres pratiques, sur différentes plateformes.

Pour régler la situation, on a vraiment besoin d'une réponse à l'échelle de toute la société et que l'on peut partager.

• (1700)

Rachel Curran (directrice, Politique publique, Meta Canada, Meta Platforms Inc.): Si vous me le permettez, j'aimerais ajouter quelque chose, monsieur Camfield.

Nous avons réduit de 50 % le nombre d'arnaques signalées, donc nos efforts ont vraiment permis de diminuer le nombre d'arnaques signalées et le nombre d'arnaques qui apparaissent sur nos plateformes. Les efforts que nous déployons avec M. Camfield et son équipe donnent vraiment des résultats. Les avons-nous supprimées complètement? Pas encore, mais nous sommes sur la bonne voie.

[Français]

Gabriel Ste-Marie: Je vous remercie de votre réponse.

Évidemment, il faut continuer à en faire davantage. Je suis inquiet, car il y a beaucoup de fraudes et, même s'il y en a sur les sites Web, il semble que ça se passe en grande partie, sinon majoritairement, sur vos plateformes. Vous avez les moyens de corriger ça.

J'aimerais souligner un autre point. Depuis plusieurs années, sur Facebook, on ne peut plus avoir les nouvelles, les articles journalistiques, les partages d'articles ou de vidéos.

Cependant, on a les hypertrucages avec de faux reportages de Radio-Canada, de TVA ou d'autres médias.

Est-ce que Meta compte réintroduire le partage des articles journalistiques sous peu, ou est-ce que votre modèle est vraiment basé sur la désinformation du public?

[Traduction]

Rachel Curran: Oui, nous aimerions beaucoup avoir de nouveau du contenu de nouvelles canadien sur nos plateformes, et je dis cela en tant que Canadienne, non pas en tant que représentante officielle de Meta. Nous l'avons déjà dit.

Pour ce qui est des endroits où se produisent les arnaques, écoutez, nous sommes ici pour parler des efforts que nous faisons pour en réduire le nombre. Si j'ai bien compris, certains de nos collègues, des représentants d'autres plateformes technologiques, ont refusé l'invitation à comparaître devant le Comité pour parler du travail qu'ils font pour réduire les arnaques. Nous pensons que c'est un sujet important, et c'est pour cette raison que nous voulons parler des efforts que nous déployons.

[Français]

Gabriel Ste-Marie: J'aimerais poser une dernière question.

Pourquoi est-ce que Meta est plus efficace à supprimer le partage d'articles journalistiques que les vidéos hypertruquées qui mènent à de la fraude auprès du public?

Pourquoi êtes-vous plus efficaces à supprimer les articles de nouvelles que les vidéos de fraude?

[Traduction]

Rachel Curran: Je crois que vous avez tort. La Loi sur les nouvelles en ligne dit que nous devons soit rémunérer les éditeurs de presse pour le contenu qu'ils affichent volontairement sur nos plateformes, soit retirer complètement le contenu de nouvelles de nos plateformes. Nous avons choisi de nous conformer à la Loi sur les nouvelles en ligne en retirant le contenu de nouvelles de nos plateformes. Malheureusement, c'est la situation dans laquelle nous sommes aujourd'hui.

Nous avons parlé au ministre du Patrimoine pour savoir s'il était possible de ramener d'une façon ou d'une autre les nouvelles sur nos plateformes. J'espère que nous pourrions y arriver à un moment ou à un autre, mais nous n'y sommes pas encore.

[Français]

Gabriel Ste-Marie: Merci.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Monsieur Falk, vous avez la parole, monsieur, pour cinq minutes.

Ted Falk (Provencher, PCC): Merci.

Monsieur Shipley, j'aimerais pour commencer m'adresser à vous.

Vous avez dit que les deux tiers des arnaques — les arnaques et les fraudes en ligne — se produisent sur la plateforme Meta. Quelles sont les autres plateformes dont se servent les fraudeurs?

David Shipley: Cette information précise vient de la Lloyds Banking Group du Royaume-Uni. En fin de semaine, *The Independent* a dit que les deux tiers des cas de fraude visant leurs consommateurs ont commencé sur des plateformes détenues par Meta. Nous voyons aussi, dans la littérature, d'autres plateformes de médias sociaux, et, en aval, on parle de télécommunications, de messages textes, de faux appels téléphoniques, etc.

Il n'y a pas eu de changement. En 2023, Lloyds rapportait que plus de 54 % des fraudes par paiement initié par le payeur autorisé se passaient sur des plateformes détenues par Meta. Meta contrôle le marché, compte tenu de sa taille, donc, c'est sûr que les arnaqueurs veulent passer par ces plateformes.

Ted Falk: Pourriez-vous proposer des solutions?

David Shipley: Eh bien, voici ce que je dirais. Si vous...

Ted Falk: Donnez-moi une solution facile, qui pourrait donner des résultats.

David Shipley: Rendez Meta responsable des centaines de milliers de dollars qu'ont perdus les aînés canadiens en raison d'une fraude — un membre du Comité a mentionné des gens à Québec — jusqu'à ce qu'il n'y ait plus de publicités frauduleuses. S'il y a des incitatifs financiers suffisants, Meta pourra encaisser des millions de dollars en publicité, mais sans victimiser les Canadiens.

Ted Falk: Monsieur Camfield, j'aimerais vous poser quelques questions à vous aussi.

Il a clairement été établi que Meta est une plateforme où se font beaucoup d'arnaques en ligne. D'après l'article de *Reuters*, il semble que Meta sait très bien que les arnaqueurs se servent de ses plateformes. Selon vous, quelle devrait être la part de responsabilité de Meta à cet égard, et qu'en est-il en réalité?

Jon Camfield: Nous savons que nous avons un rôle essentiel à jouer dans la lutte contre les arnaques. Nous sommes en haut de l'entonnoir, comme on l'a décrit, ou de la chaîne d'attaques frauduleuses, où beaucoup de fraudeurs chercheront des victimes potentielles. Nous avons la chance et l'inconvénient d'être l'une des plus grandes plateformes de médias sociaux, donc nous sommes une cible intéressante, comme nous l'avons dit.

Cette taille entraîne des responsabilités et de nombreux enjeux. Nous devons en même temps respecter la liberté d'expression et tenir compte des intérêts des petites entreprises, tout en luttant de notre mieux contre les arnaqueurs. Nous devons trouver des moyens de détecter les acteurs ayant de mauvaises intentions et les fraudeurs, qui feront de leur mieux pour contrecarrer nos mesures de défense, tout en nous assurant que les utilisateurs ordinaires puissent accéder à la plateforme et l'utiliser sans problème.

• (1705)

Ted Falk: Laissez-vous entendre que vous laissez volontairement des arnaqueurs accéder à votre site et que vous effectuez une analyse de rentabilité ou une analyse avantages-risques pour savoir si vous leur laissez l'accès?

Jon Camfield: Je ne discuterais pas...

Rachel Curran: Je suis tout à fait en désaccord avec cela. C'est n'importe quoi.

Monsieur Camfield, vous pouvez en parler.

Près de 90 % de nos revenus proviendront d'annonceurs confirmés d'ici 2026. Actuellement, le pourcentage se situe entre 70 et 80 %.

Est-ce bien cela, monsieur Camfield? Vous pouvez nous en dire plus, mais notre objectif, c'est que 90 % de nos revenus proviennent d'annonceurs confirmés. Il y a une raison pour laquelle nous ne visons pas le 100 %, et M. Camfield peut vous en parler, mais nous ne voulons absolument pas tirer des revenus d'annonceurs qui sont des arnaqueurs ou des fraudeurs. Cela crée une expérience déplaisante sur nos plateformes, qui nuit à nos utilisateurs, et nous voulons empêcher dans la mesure du possible.

Ted Falk: D'accord. Je comprends ce que vous venez de dire.

Souvent, quand les banques ont affaire à des clients ou à des consommateurs qui viennent de se faire escroquer, elles offrent une indemnisation; pas tout le temps, mais souvent. Que peut faire Meta pour les consommateurs qui ont été victimes d'une fraude sur votre site? Que pouvez-vous faire? Quels recours s'offrent aux gens qui s'adressent à Meta?

Jon Camfield: C'est difficile parce que nous n'avons aucun contrôle sur les actes frauduleux ou les transferts monétaires. Nous ne touchons à rien. Nous ne voyons rien. Cela concerne les institutions financières.

Ted Falk: Je comprends, mais que faites-vous pour les gens qui ont été victimes d'une fraude en raison d'une annonce circulant sur votre plateforme?

Jon Camfield: Pour être clair, si nous savons qu'une annonce est frauduleuse, nous la retirons. Cela va à l'encontre de nos politiques, et nous la retirons.

Ted Falk: Que faites-vous pour les gens qui se font escroquer?

Jon Camfield: Nous ne pouvons pas savoir...

Ted Falk: Donc, vous ne vous souciez pas de vos utilisateurs.

Jon Camfield: Nous nous soucions d'eux.

Ted Falk: Non, c'est faux.

Jon Camfield: Je ne suis pas d'accord. Vraiment...

Ted Falk: J'ai posé toutes mes questions. Merci.

Jon Camfield: Les utilisateurs, c'est ce que Meta a de plus précieux.

Le président: Merci beaucoup, monsieur Falk.

C'est maintenant au tour de M. Ma et de M. Bardeesy de poser leurs questions.

Monsieur Bardeesy, vous avez la parole en premier.

Karim Bardeesy (Taiaiko'n—Parkdale—High Park, Lib.): Merci, monsieur le président.

J'aimerais poser deux ou trois questions à Meta, et j'aimerais commencer par vous, madame Curran.

Je pense que les Canadiens nous regardent et nous écoutent avec beaucoup d'intérêt compte tenu de la gravité de la question, et je pense qu'ils sont choqués par les propos non parlementaires qu'ils viennent d'entendre.

J'aimerais seulement revenir sur ce qu'a dit M. Ste-Marie à propos de la Loi sur les nouvelles en ligne. Un article très solide a été publié dans le *Globe and Mail* en fin de semaine — dans lequel Mme Quaid est citée — concernant le genre de fraude qui se fait en ligne, les mesures de protection auxquelles les Canadiens devraient s'attendre et le genre de mesures qui s'offrent à eux dans le cadre d'une approche pangouvernementale qui touche toute la société. Un de mes collègues vient de tenter de publier cet article sur la plateforme Facebook, et il a reçu la réponse suivante: « En réponse à la législation du gouvernement canadien, les contenus d'actualité ne peuvent pas être affichés au Canada. »

C'est un article qui pourrait aider des millions de Canadiens — s'ils avaient accès à cet article sur vos plateformes — à réagir à ce que nous étudions, précisément, en ce moment. Aujourd'hui, pourriez-vous vous engager à ne pas bloquer, sur Instagram et Facebook, la diffusion de cet article publié dans le *Globe and Mail* samedi, dans lequel Mme Quaid est citée?

Rachel Curran: J'aimerais vraiment pouvoir le faire, monsieur Bardeesy. Nous ne pouvons pas le faire en raison de la Loi sur les nouvelles en ligne, qui nous interdit de partager du contenu de nouvelles canadien sur Facebook et Instagram, sauf si nous acceptons le cadre de rémunération établi par le gouvernement dans ladite loi.

J'espère pouvoir régler cela avec le gouvernement et pouvoir de nouveau partager du contenu de nouvelles canadien sur nos plateformes. Nous cherchons à trouver une solution.

• (1710)

Karim Bardeesy: Madame Curran, je parle d'un article qui donne aux Canadiens de l'information exploitable pour les aider à lutter contre la fraude.

Rachel Curran: Justement, c'est cela, le problème. La Loi sur les nouvelles en ligne ne nous permet pas d'afficher ne serait-ce qu'un article sur Facebook ou Instagram, à moins de nous conformer à l'ensemble du cadre établi dans ladite loi. C'est ainsi que la loi a été rédigée.

Karim Bardeesy: C'est une loi qui a été dûment adoptée par le Parlement.

Je vais céder le reste de mon temps à M. Ma.

Michael Ma (Markham—Unionville, Lib.): Merci.

Tous les témoins semblent s'entendre pour dire que la collaboration est essentielle pour prévenir la fraude.

Je vais pour commencer poser une question au groupe Meta. Avec qui collaborez-vous, déjà?

Jon Camfield: Comme je l'ai mentionné brièvement dans ma déclaration, nous avons lancé, en 2024, un programme d'échange de renseignements sur la fraude — le programme FIRE —, et il a pris de l'ampleur au cours des deux ou trois dernières années. Il s'agit d'un échange bidirectionnel avec les banques. Il y a des représentants du Financial Services Information Sharing and Analysis Centre, un centre d'analyse et de partage d'informations sur les services financiers, qui compte également de nombreux membres canadiens, et d'autres banques dans le monde. À l'heure actuelle, plus de 50 banques échangent activement des signaux avec nous pour lutter contre la fraude.

Nous sommes aussi membres de Global Signal Exchange, un organisme international à but non lucratif qui travaille avec le secteur, les gouvernements et les organismes de réglementation. Il fournit gratuitement ses services aux organismes de réglementation, mais le secteur paie pour en faire partie. Nous nous servons de ces services pour communiquer avec d'autres gouvernements et avec les entreprises du secteur, en plus d'échanger de l'information sur de nombreuses activités.

Michael Ma: Vous dites collaborer à l'élaboration et à la mise en œuvre d'un certain nombre de mesures; or, nous voyons toujours les mêmes arnaques se répéter, encore et toujours.

J'aimerais savoir ce qu'en pensent M. Shipley et Mme Quaid.

David Shipley: On pourrait presque admirer l'ingéniosité des criminels.

En réalité, nous pourrions en faire beaucoup plus. Le problème, c'est qu'il manque de mesures incitatives financières pour nous forcer à agir de concert dans ce dossier. Si, soudainement, tout cela commence à coûter des milliards de dollars de revenus, je pense qu'ils travailleront plus fort pour mettre un terme aux publicités frauduleuses d'investissements mettant en vedette Mark Carney qui circulent sur leurs plateformes.

Jennifer Quaid: Laissez-moi ajouter quelque chose.

Ce n'est pas seulement parce qu'il n'y a pas de mesures incitatives financières que nous ne travaillons pas de concert. Les règles et règlements en vigueur nous empêchent de communiquer rapidement l'information importante. Si nous ne donnons pas le droit aux banques, aux entreprises de télécommunications et aux plateformes de médias sociaux de communiquer de l'information afin de prévenir les arnaques, nous allons tout simplement continuer à payer plus d'argent.

C'est ce dont nous avons besoin, dans la stratégie proposée.

Michael Ma: Quelles mesures semblent freiner les arnaques? Quelles lois précises les préviennent?

Jennifer Quaid: C'est en partie parce que de nombreuses organisations craignent les représailles. M. Camfield l'a mentionné dans sa déclaration liminaire. Nous avons besoin d'une loi de protection qui permettra aux organisations d'échanger de l'information les uns avec les autres sans craindre de représailles.

C'est en partie à cause des règles sur la communication d'informations; par exemple, le destinataire, le moyen, le moment, la raison et le temps que cela prend pour communiquer l'information. Nous devons attendre des jours, voire des semaines, pour communiquer de l'information, et l'arnaqueur est passé à autre chose. Ces choses sont immédiates. C'est ce que nous devons permettre.

Michael Ma: Je crois que vous avez tous mentionné la rapidité. À l'heure actuelle, croyez-vous que c'est assez rapide? Puisque l'IA

est là, en arrière-plan, nous devrions être en mesure de le détecter immédiatement.

Monsieur Shipley, je ne sais pas si vous...

David Shipley: J'aimerais ajouter ceci au sujet de la rapidité. Alors que nous passons à des systèmes de paiement en temps réel qui vont au-delà des modes de réconciliation traditionnels, on ne peut pas récupérer l'argent. Cela se fait instantanément.

Ce qu'a dit ma collègue au sujet de la prévention est tout à fait essentiel. Nous ne pouvons pas revenir en arrière une fois que la fraude a eu lieu.

Jennifer Quaid: En ce qui concerne l'échange d'information, si cela se fait rapidement et utilement, nous commencerons à voir les schémas d'activité très rapidement. C'est à ce moment-là qu'il faut faire de la prévention. Nous pouvons empêcher qu'il y ait une prochaine victime.

Michael Ma: Merci.

Le président: Merci beaucoup, monsieur Ma.

[Français]

Monsieur Ste-Marie, vous avez la parole.

Gabriel Ste-Marie: Merci, monsieur le président.

Mes questions s'adressent encore aux représentants de Meta.

Vos bénéfices sont mirobolants, tant à l'échelle mondiale qu'au Canada. Meta fait partie des grandes entreprises. Elle ne paie pas d'impôt au Canada, grâce à tout le montage financier et aux paradis fiscaux, entre autres choses. Les géants du Web et vous [*difficultés techniques*] le gouvernement canadien pour qu'il suspende la taxe sur les services numériques, qui est une compensation de l'impôt que vous ne payez pas ici. Vous refusez de partager les articles journalistiques, parce qu'il faudrait qu'il y ait des redevances aux médias. Ces derniers sont en crise, parce que toute la publicité va vers les plateformes comme les vôtres. Aujourd'hui, nous discutons de la fraude. Vous faites des efforts pour limiter la fraude, mais elle perdure quand même.

Considérez-vous que Meta est une entreprise socialement responsable?

• (1715)

[Traduction]

Rachel Curran: Écoutez, nous payons tous nos impôts applicables, au Canada, ce qui inclut l'impôt sur les sociétés et les charges sociales. Nous payons tous les impôts imposés par le gouvernement du Canada.

Ce que nous refusons, c'est le cadre prévu dans la Loi sur les nouvelles en ligne, qui nous aurait obligés à verser plus d'argent aux éditeurs pour du contenu qu'ils ont volontairement placé sur nos plateformes parce qu'ils en tirent un avantage considérable. Selon nos estimations, le contenu qu'ils mettent sur nos plateformes génère un revenu d'environ 300 millions de dollars par an. Ils ont tiré parti de la distribution sur nos plateformes. Nous pensons que l'échange de valeur a profité aux éditeurs, et non pas à Meta. Nous avons refusé de verser une somme supplémentaire aux éditeurs pour avoir volontairement partagé du contenu sur Facebook et Instagram.

[Français]

Gabriel Ste-Marie: Je vais vous poser ma question de nouveau.

Considérez-vous que Meta est une entreprise socialement responsable?

[Traduction]

Rachel Curran: Excusez-moi. Je n'ai pas entendu la question.

[Français]

Gabriel Ste-Marie: Considérez-vous que Meta est une entreprise socialement responsable au Canada?

[Traduction]

Rachel Curran: Notre présence au Canada a vraiment de l'importance pour nous. Nos utilisateurs canadiens et les échanges avec le gouvernement canadien sur une foule de sujets sont tout aussi importants pour nous.

En ce qui me concerne, en tant que citoyenne canadienne, j'aimerais voir de nouveau du contenu d'information canadien sur Facebook et Instagram. J'avais l'habitude de suivre les médias canadiens sur Facebook, et je me tenais donc informée de l'actualité sur Facebook. J'aimerais revoir ce contenu sur nos plateformes, et j'espère que nous parviendrons à trouver une solution à ce problème.

[Français]

Gabriel Ste-Marie: Vous dites payer de l'impôt et suivre la loi à la lettre, mais la loi permet aux entreprises américaines qui ont des filiales dans les paradis fiscaux de les utiliser pour ne pas payer d'impôt ici.

Pour la dernière année, à quel montant s'élevait l'impôt sur le revenu que vous avez payé?

Quel pourcentage de votre chiffre d'affaires cela représentait-il?

[Traduction]

Rachel Curran: Nous n'avons pas d'abri fiscal. Nous payons, au Canada, tous les impôts imposés par le gouvernement du Canada, et nous nous plions à toutes les exigences applicables des autorités fiscales canadiennes, ici. Meta respecte toutes les lois fiscales du Canada.

[Français]

Gabriel Ste-Marie: Je vous rappelle bien humblement que la taxe sur les services numériques a été mise en place par le G20, à l'initiative de l'Organisation de coopération et de développement économiques, parce que, grâce à des montages financiers, les plateformes Web comme les vôtres ne paient pas leur juste part d'impôt. Ce que je viens d'entendre est décevant, je trouve.

Le Payment Systems Regulator, au Royaume-Uni, a indiqué, dans un rapport publié à la fin de 2024, que, en 2023, vos plateformes au Royaume-Uni étaient associées à 54 % du volume des escroqueries par virement autorisé.

Reconnaissez-vous ce fait? Reconnaissez-vous que c'est le cas dans l'ensemble des pays où vous êtes présent, notamment au Canada?

Reconnaissez-vous que ça doit diminuer? La majorité des escroqueries par virement autorisé se fait sur vos plateformes.

[Traduction]

Rachel Curran: Je ne peux pas parler de ce qui se passe au Royaume-Uni. Je peux dire que nous payons tous les impôts applicables au Canada. Je pense que, lorsque vous parlez de la taxe sur les services numériques, vous faites référence à la taxe supplémentaire que le gouvernement souhaitait imposer à des plateformes

comme la nôtre, car, selon lui, nous devrions payer plus d'impôts et de taxes que ce que la loi canadienne exige. La décision revient au gouvernement, mais à l'heure actuelle, nous payons tous les impôts requis au Canada.

[Français]

Gabriel Ste-Marie: Nous ne sommes pas d'accord sur ça.

Le président: Monsieur Ste-Marie, il vous reste du temps pour poser une question de plus.

Gabriel Ste-Marie: Je vais poser à nouveau la dernière question que j'ai posée concernant le Royaume-Uni.

Le rapport ne parlait pas de la taxe sur les services numériques, mais des escroqueries. Selon leur analyse, 54 % du volume des escroqueries par virement autorisé étaient réalisés sur les plateformes de Meta. Autrement dit, la majorité de ces escroqueries était réalisée sur vos plateformes.

Reconnaissez-vous que c'est la même situation ici et que c'est inacceptable?

Merci beaucoup.

● (1720)

[Traduction]

Jon Camfield: Il faudrait que je regarde les détails de ce rapport pour répondre à cette question très spécifique. La fraude de paiement initié par le payeur est une tendance que nous voyons apparaître parmi les arnaques, et nous devons également lutter contre cela. Cela va à l'encontre de nos politiques, et lorsqu'une telle fraude est détectée, on l'élimine.

[Français]

Gabriel Ste-Marie: D'accord.

Merci beaucoup, monsieur le président.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Monsieur Hoback, la parole est à vous, et vous avez cinq minutes.

Randy Hoback (Prince Albert, PCC): Merci, monsieur le président.

Je tiens à remercier le Comité de me donner l'occasion de participer, aujourd'hui. Je ne suis normalement pas membre de ce comité, mais cela tombe vraiment à point nommé. Ma circonscription compose avec les arnaques, les fraudes en ligne et ce genre de choses.

Nous venons tout juste d'organiser un événement communautaire portant sur la fraude en ligne. Nous avons travaillé avec notre coopérative de crédit locale, Affinity Credit Union, qui a fait venir ses propres spécialistes des services bancaires. Nous avons fait intervenir la GRC, la police de la ville en l'occurrence. Nous avons limité l'assistance à 120 personnes. Il aurait pu y avoir 300 personnes, dans la pièce, à parler des arnaques dont elles ont été victimes en ligne ou hors ligne.

D'après la police, ce qui limite vraiment les possibilités, c'est qu'il est compliqué d'informer les gens sur les escroqueries commises dans la collectivité, à un moment donné. Par exemple, à Prince Albert, on faisait croire aux gens que le petit Johnny, leur petit-fils, Johnny, s'était fait arrêter, car il avait commis un délit. Ce n'était pas grave, et ce n'était pas de sa faute, mais quelqu'un devait payer le cautionnement. Les arnaqueurs venaient frapper à la porte en disant « nous sommes ici pour récupérer le paiement du cautionnement de Johnny ». Les aînés sont des gens confiants, surtout à l'égard d'une personne bien habillée qui porte un uniforme. Ils tombent dans le piège.

Donc, ces 120 personnes ont été informées de l'escroquerie, et elles sont allées en parler avec leurs amis, autour d'un café, cette semaine. Désormais, tout le monde à Prince Albert est au courant de l'escroquerie qui avait eu lieu, cette semaine-là.

Je suis curieux. Vous dites que Meta éliminait les escroqueries à mesure qu'elles sont détectées. Avez-vous une mesure de déclaration proactive? Dites-vous « ceci est une arnaque » afin que les gens soient au courant des types d'arnaques qui existent?

Jon Camfield: Oui. Nous gérons un centre de prévention de la fraude où on trouve exactement de ce genre de contenu. Il n'est pas toujours adapté à une collectivité aussi ciblée que la vôtre, mais il est adapté aux différents pays. Nous avons également une série de publications de salles de presse qui traitent des escroqueries ciblées spécifiques que nous voyons. Nous collaborons avec des entreprises de recherche externes pour examiner différentes collectivités et différentes tendances. Une de nos publications a récemment porté sur la fraude ciblant les aînés, les tendances actuelles et les tactiques utilisées pour cibler les aînés à l'échelle de la planète. Une autre a porté sur les escroqueries romantiques, et ainsi de suite.

Randy Hoback: Vous parlez de ce centre. J'ignorais son existence. Je pense que personne ici ne le connaissait. Que faites-vous proactivement pour informer les gens de l'existence de ce centre?

En réalité, est-ce que vous stigmatisez ces escrocs? Si vous tombez sur une escroquerie qui, disons, se passe dans un autre pays, pouvez-vous vraiment poursuivre les responsables dans le pays en question? Pouvez-vous dire, « hé, vous commettez une escroquerie au Canada, donc nous allons vous punir », qu'ils soient en Asie ou peu importe le pays?

Jon Camfield: Deux choses. En ce qui concerne l'aspect proactif, l'un des outils que nous utilisons, qui est, en réalité, l'un de mes outils préférés, c'est une série d'avertissements juste-à-temps que nous envoyons aux utilisateurs, que ce soit par rapport à un message ou à l'ajout d'un nouvel ami. Nous dirons: « Hé, cet utilisateur ne fait pas partie de votre cercle social. Il dit qu'il vient d'ici, mais d'après nous, ce n'est pas vraiment là qu'il se trouve. » Il est facile pour un escroc de contourner ces signaux, de passer par-dessus, mais nous pouvons en envoyer toute une série à l'utilisateur, et lui dire: « Cela semble suspect. Cela pourrait être légitime, car il se peut que ce soit votre ami qui voyage, mais vous devriez tout de même vous méfier. »

C'est vraiment la base de la prévention. Il n'est pas question de se focaliser sur une tendance spécifique, car plus vous faites cela, plus vite les escrocs réagiront. Il s'agit vraiment de se focaliser sur cela...

Randy Hoback: Je suis d'accord avec vous. Il faut également que l'acheteur soit averti. C'est exactement comme avec les nouvelles sur Facebook, la personne qui regarde doit être avertie.

Vous avez parlé du fait que 90 % de vos annonceurs sont contrôlés. Ce qui me dérange, ici — je suis d'accord pour dire qu'ils sont contrôlés —, c'est que la publication qu'ils font circuler est du pipeau. C'est un influenceur rémunéré par quelqu'un d'autre, à l'arrière. Il peut s'agir des minifigurines Lego, en Iran, ou de ce genre de groupes. Tout à coup, mon visage apparaît dans cette microvidéo.

Que faites-vous pour vous assurer que je ne sois pas dans une microvidéo, et que je ne me retrouve pas à appuyer une publication, qui, comme nous le savons tous, est du pipeau?

Jon Camfield: Nous avons de multiples outils pour protéger les gens contre l'usurpation d'identité, en particulier les personnalités publiques. Nous pouvons...

• (1725)

Randy Hoback: Ce n'est pas une usurpation d'identité, dans ce cas-ci. On utilise mon nom sans mon consentement, et on dit que j'appuie quelque chose. À mon sens, c'est problématique, surtout que je suis une personnalité publique.

Mon ami dit « je n'ai pas appuyé cela », mais tout le monde sur sa plateforme de média lui dit, « non, tu l'as appuyé sur la plateforme ». Est-ce un bon comportement d'entreprise?

Jon Camfield: Je dirais que notre réponse et nos outils pour combattre et gérer cela sont très efficaces et témoignent d'un bon comportement. Nous collaborons avec les propriétaires de marque et de propriété intellectuelle, dont des célébrités et des personnalités publiques, afin de leur donner des outils pour signaler, cerner et détecter proactivement...

Randy Hoback: Je parle des gens ordinaires. C'est mon voisin en bas de la rue. Je pense que c'est un gars honnête, et tout à coup, il appuie quelque chose qu'il n'a jamais vu avant. On saisit ses renseignements et on les met dans cette microvidéo.

Vous avez dit que les choses changeaient. L'autre chose que je vois est assez nouvelle. C'est un présentateur du journal télévisé qui semble très réel, mais en réalité, c'est de l'IA à 100 %. Il parle d'un événement actuel, et l'information concernant cet événement actuel est assez précise, de sorte que vous pensez que c'est vrai. Cela influence sur votre opinion, mais c'est du pipeau. Cela risque d'arriver de plus en plus. Les gens ne peuvent plus distinguer le réel du faux.

Est-il juste de dire que Facebook devrait être vu comme une simple plateforme de divertissement, et non pas comme une plateforme de nouvelles?

Rachel Curran: Je ne pense pas qu'il faut choisir entre les nouvelles et le divertissement. La question est d'éliminer la chose, ou, du moins, d'y appliquer une étiquette, lorsque quelqu'un bafoue nos politiques, induit les gens en erreur et fait de la désinformation, pour que les gens comprennent qu'il s'agit d'un contenu généré par l'IA, que ce n'est pas réel et qu'ils doivent faire preuve d'un certain scepticisme. Ce sont tous les outils que nous déployons à l'heure actuelle.

Écoutez, je suis d'accord pour dire que nous pouvons et devrions en faire plus, à ce chapitre, mais lorsque des gens utilisent des contenus hypertruqués générés par l'IA, par exemple, ou des vidéos générées par l'IA, nous les obligeons à utiliser des étiquettes pour indiquer qu'il s'agit d'un contenu d'IA. Lorsque le contenu présente un risque considérable d'induire les gens en erreur, nous retirons cette vidéo ou ce matériel généré par l'IA, ou nous y plaçons une étiquette en indiquant que ce n'est pas réel et qu'il faut faire preuve d'un grand scepticisme.

Randy Hoback: J'ai donc une question à ce propos. Je ne veux pas parler de la Loi sur les nouvelles en ligne. Nous en avons assez parlé et nous avons nos opinions sur le sujet. En ce qui concerne vos activités proactives visant à éliminer ces choses de vos plateformes, quelles lois ou quels règlements — quoi d'autre — nous permettraient d'habiller des groupes à mieux contrôler ce qui est mis sur votre plateforme, afin que vous puissiez vous assurer que personne n'appuie quelqu'un d'autre qu'il n'a pas envie d'appuyer ou que vous avez les outils nécessaires pour retirer ces personnes le plus rapidement?

Je souhaite également savoir ce que vous allez faire. Vous avez parlé de votre centre. Personne n'est au courant de son existence. Vous devez faire un meilleur travail pour cerner les arnaques.

En dernier lieu, je vais utiliser un exemple. Sur Marketplace, sur Facebook, il y a un ensemble de meubles de jardin à vendre, dans la ville voisine. Il a l'air magnifique et il n'est vraiment pas cher. C'est trop beau pour être vrai. Lorsque je regarde l'arrière-plan de l'image, il y a des palmiers. Je suis en Saskatchewan. Maintenant, il ne fait pas aussi froid qu'à Winterpeg, mais l'IA va-t-elle intercaler...?

Vous avez deux questions, ici. Il faut une loi capable d'ouvrir la porte et de faciliter l'arrestation de ces personnes. Nous devons punir les responsables, d'une façon ou d'une autre. Nous devons trouver un moyen de le faire. De plus, en ce qui concerne la prévention, comment pouvons-nous rapidement reconnaître que ce n'est pas réel?

Jon Camfield: Pour ce qui est de la loi, je suis entièrement d'accord avec ma collègue sur les mesures de protection entourant l'échange d'informations. Nous permettre de communiquer des avertissements en temps réel sera incroyablement efficace. Comme je l'ai mentionné, le résultat de n'importe quelle information unique que nous recevons des banques, c'est que nous pouvons supprimer 600 fois plus d'avis, qui ne sont pas nécessairement des avis actifs. Ce pourrait être des avis dormants, mais qui seront utilisés un jour ou l'autre. Cela touche également à certaines mesures de prévention.

En ce qui concerne l'application directe de la loi, les interactions du gouvernement sont ce qui importe le plus. L'échange d'information avec les agents d'application de la loi et entre ces derniers et leurs homologues aux quatre coins de la planète a été incroyablement efficace. Cela a vraiment permis d'arrêter de véritables escrocs, en particulier lorsqu'ils traversent les frontières pour obtenir des soins médicaux ou pour aller en vacances. Sinon, ils agissent avec impunité, du Cambodge, du Myanmar et d'autres endroits où l'application de la loi n'est pas assez fonctionnelle pour punir leur mauvais comportement. Communiquer l'information peut vraiment faire toute la différence.

Randy Hoback: J'ai une autre petite question.

Le président: Veuillez la poser très rapidement.

Randy Hoback: Vous avez parlé des forces de l'ordre. Avez-vous travaillé de façon proactive avec les forces de l'ordre pour créer un système leur permettant de se raccorder rapidement à vous, de sorte que lorsqu'elles tombent sur une escroquerie — dans ce cas-ci, le jeune Johnny qui est arrêté pour escroquerie — elles peuvent diffuser ce message dans une région? Vous avez la capacité, grâce à la publicité, de dire: « Nous ne ferons de la publicité que dans cette région. » Le faites-vous également avec les forces policières? Le faites-vous avec la GRC locale, la police municipale locale et les shérifs de comté?

● (1730)

Rachel Curran: Oui, nous le faisons régulièrement.

Je ne peux pas parler de ce qui se passe au Canada. Nous travaillons avec la GRC ainsi qu'avec les forces policières régionales et municipales sur des enjeux comme les escroqueries. Nous faisons régulièrement la liaison avec eux sur ce que nous observons. Ils nous signalent également ce qu'ils observent. Nous disposons d'un portail spécial destiné aux forces de l'ordre, grâce auquel elles peuvent nous faire des signalements, et s'il y a une demande urgente, elles peuvent nous la faire parvenir très rapidement. Si ce n'est pas une demande urgente, nous pouvons ensemble trouver la façon de retirer le matériel et la façon de régler le problème à long terme.

Le président: Merci beaucoup, monsieur Hoback.

Madame Begum, je crois comprendre que vous partagerez peut-être votre temps avec Mme O'Rourke. La parole est à vous.

Doly Begum (Scarborough-Sud-Ouest, Lib.): Merci beaucoup, monsieur le président.

Bonjour — ou bonsoir, pratiquement — à vous tous. Merci beaucoup d'être ici et de nous donner l'occasion de vous poser des questions.

Je vais commencer par Mme Curran.

Pensez-vous que Meta dispose d'un mécanisme d'application de la loi solide pour faire le suivi de la désinformation, de la désinformation, des escroqueries et des fraudes à l'heure actuelle?

Rachel Curran: Ce sont tous des enjeux différents — la désinformation et la désinformation, oui, et les escroqueries, oui — mais il y a toujours des écarts entre ce que nous interdisons en vertu de nos politiques relatives au contenu et ce contre quoi nous prenons des mesures d'application. Nous nous efforçons constamment de combler cet écart.

Doly Begum: Dans ce cas, d'après ce dont le député Bardeesy parlait, il semble que vous ayez été en mesure de retirer très rapidement un article du *Globe and Mail*. Meta dispose d'un mécanisme d'application de la loi pour retirer quelque chose rapidement, comme un article qui était inoffensif et qui aurait en réalité contribué à la qualité de vie de la population et de la société.

J'aimerais citer l'article de Reuters mentionné par M. Shipley et d'autres intervenants ici. Le document inédit révélait que Meta « n'avait pas réussi à repérer et à stopper une avalanche d'annonces qui ont exposé des milliards d'utilisateurs de Facebook, d'Instagram et de WhatsApp à des stratagèmes de commerce électronique et d'investissement frauduleux, des casinos en ligne illégaux et la vente de produits médicaux interdits ».

Vous avez été en mesure de retracer rapidement un article du *Globe and Mail*, or vous avez une avalanche d'annonces qui ont exposé des milliards d'utilisateurs. N'avez-vous pas de mécanismes pour ce type d'enjeux?

Jon Camfield: Nous en avons. La grande différence tient à l'envergure de l'adversaire. Tout dépend du dévouement et des fonds dont dispose le complexe industriel escroc qui cible notre système.

Doly Begum: Au sujet du financement, on a estimé que Meta avait réalisé 10 % de son revenu annuel des dix dernières années grâce aux annonces frauduleuses.

Jon Camfield: Ce chiffre — 10 % — constitue une fausse représentation des recherches réelles.

Doly Begum: Quel était le pourcentage?

Jon Camfield: Selon les recherches réalisées à cette époque, il se situait plutôt autour de 3 à 4 %, pas 10 %.

Doly Begum: D'accord. Selon les données dont je dispose, c'est entre 5 et 10 %. Malgré tout, si nous additionnons les revenus tirés des annonces en partant de votre chiffre de 5 %, cela représente environ 6 milliards de dollars de revenu que Meta a tiré à partir d'annonces qui étaient des arnaques et qui étaient frauduleuses. Les gens se faisaient arnaquer. Des personnes âgées se faisaient arnaquer.

Jon Camfield: Nous avons abaissé ce chiffre. C'était le chiffre de 2024.

Doly Begum: C'est ahurissant.

Jon Camfield: Nous l'avons réduit de 50 % l'an dernier, et nous essayons maintenant de le réduire — le nombre de signalements d'arnaque, du moins — de 50 % de plus cette année.

La lutte contre ces complexes d'arnaqes sera très longue. Nous sommes déterminés à poursuivre notre travail... et à les démanteler.

Doly Begum: Monsieur Camfield et madame Curran, même si je reconnais les efforts continus que vous avez déployés, les gens de ma communauté et des personnes de l'ensemble du Canada n'arrivent pas à mettre de la nourriture sur leur table. Ils ne peuvent pas acheter de nourriture. Ils dépensent 50, 100, 200 ou 300 \$ — une partie importante de leur revenu — et reviennent à la maison avec des sacs d'épicerie pas assez grands pour tenir toute la fin de semaine. Meta a gagné, disons, 6 milliards de dollars parce que des gens se faisaient arnaquer. Meta a permis que cela arrive. C'est ce que j'observe, alors je ne sais pas quel type d'efforts vous avez déployés, mais vous avez été en mesure de retirer des articles qui auraient pu informer des gens sur la manière de se renseigner d'avantage et de ne pas être la cible d'arnaqueurs.

Je n'ai pas assez de temps. J'ai tant d'autres questions concernant les normes et les lignes directrices de votre communauté.

Le *Guardian* a déclaré que Meta est le « marché des prédateurs ». Vous avez récemment perdu une cause dans laquelle des enfants étaient vendus, et Meta était l'une des principales plateformes utilisées. Avez-vous quelque chose à dire à ce sujet?

• (1735)

Rachel Curran: Écoutez, ces arnaqueurs sont des organisations industrielles qui réalisent leurs activités dans des administrations en dehors du Canada, et elles ciblent des plateformes numériques d'un bout à l'autre du spectre. Elles ciblent des entreprises de télécommunication. Nous recevons tous des appels et des textos frauduleux constamment, tous les jours.

Je pense qu'il faudra vraiment adopter une approche qui tient compte de l'ensemble de l'industrie pour nous attaquer à ces réseaux industriels et les démanteler. Il faudra collaborer avec les forces de l'ordre à l'échelle mondiale — les organismes d'application de la loi d'autres administrations — pour nous attaquer à ces réseaux industriels. Ils ciblent non seulement nos plateformes, mais les plateformes numériques de façon générale. Ils ciblent également nos sociétés de télécommunications.

Doly Begum: Nous avons reçu ici des entreprises de télécommunications, des intervenants du secteur bancaire ainsi que d'autres acteurs. Ils font des efforts. La différence que je constate ici, c'est que Meta gagne des milliards de dollars en devenant une plateforme pour les arnaqueurs, pour la fraude et pour d'autres choses comme la sextorsion et pour les prédateurs. Je trouve cela renversant. Il nous faut de bien meilleurs mécanismes pour nous attaquer à ce problème. En ce moment, Meta échoue à le faire.

Monsieur le président, je vais céder le reste de mon temps à ma collègue. Merci beaucoup.

Dominique O'Rourke (Guelph, Lib.): Merci.

Ce sujet a réussi à faire quelque chose qui est pourtant difficile à accomplir. J'ai l'impression que cette question a vraiment galvanisé le Comité. Nous sommes lasses d'entendre des électeurs nous dire qu'ils ont été escroqués. Nous le lisons tous les jours dans le journal. Les plateformes sont les conduits de ce... des plateformes sur lesquelles les gens souhaitent uniquement partager des photos de leurs petits-enfants ou prendre des nouvelles d'amis un peu partout dans le monde.

En décembre 2024, le Payment Systems Regulator du Royaume-Uni a déclaré que, en 2023, les plateformes de Meta étaient associées à « 54 % du volume et à 18 % de la valeur totale de [toutes les fraudes par paiement initié par le payeur autorisé] ». Ce sont des fraudes qui manipulent les gens et les entreprises. Nous ne parlons pas beaucoup des entreprises. Nous ne parlons pas non plus beaucoup des escroqueries romantiques, qui sont presque deux fois plus dévastatrices parce qu'elles s'en prennent à la solitude des gens.

Monsieur Camfield, vous avez dit que vous pouviez repérer des tendances en matière de fraude, même dans des messages cryptés de bout en bout. Vous dites disposer d'une protection contre l'usurpation et qu'il faut combattre ces réseaux à l'échelle industrielle. Toutefois, Meta est un géant mondial exerçant ses activités à l'échelle industrielle, alors je suis vraiment perplexe.

En permettant à ce volume de fraude de proliférer sur votre plateforme, comment pouvez-vous prétendre ne pas agir de manière irresponsable ou ne pas être complices de cette publicité trompeuse? En faites-vous suffisamment avec votre Centre de protection contre les arnaques? Vous souciez-vous des personnes dans ces centres de fraude, que vous dites être celles qui commettent ces crimes, ainsi que des personnes dans nos circonscriptions qui se font arnaquer?

Jon Camfield: La difficulté avec les arnaques, c'est que les victimes se trouvent vraiment de tous les côtés. Toutes ces histoires de victimes qui perdent de l'argent dans des arnaques sont horribles. Les histoires qui émergent de ces complexes d'arnaques sont également horribles.

Nous travaillons directement dans la région. Nous avons une campagne publicitaire visant à intercepter les personnes qui cherchent un emploi, car c'est souvent ainsi qu'elles sont recrutées et acheminées vers ces arnaques. Nous réalisons des interceptions au stade de la recherche: lorsque des gens cherchent un emploi dans les régions où ils sont le plus souvent recrutés, nos messages apparaissent pour leur fournir cette information en temps réel. Ces fenêtres contextuelles redirigent également les personnes vers le Centre de protection contre les arnaques pour les sensibiliser.

La sensibilisation n'est qu'une partie de la solution. Il faut vraiment beaucoup de messages diffusés au bon moment pour rejoindre les gens avant qu'ils ne s'engagent. C'est un véritable défi.

Dominique O'Rourke: Je dirais que ce qui doit être fait, c'est d'empêcher que ces arnaques se retrouvent sur votre plateforme en premier lieu. Retirez-les et réaffectez beaucoup plus de financement à la prévention des arnaques.

Le président: Merci beaucoup, madame O'Rourke.

Je vais prendre quelques dernières minutes avant que nous nous interrompions pour la prochaine séance, chers collègues.

Madame Curran, mes questions s'adressent à vous.

La première est la suivante: si une personne âgée de ma circonscription de Winnipeg-Centre-Sud perdait ses économies de toute une vie dans une arnaque provenant de Facebook, vous sentiriez-vous responsable de cette perte?

• (1740)

Rachel Curran: Monsieur Carr, je vais laisser le soin à mon collègue...

Le président: La question s'adresse à vous, madame Curran.

Vous êtes ici devant un...

Rachel Curran: ... Jon Camfield, qui est l'expert des fraudes et des arnaques à l'interne.

Le président: Non, vous êtes ici devant un comité parlementaire, à notre demande. Je vous demande ceci: dans le scénario où une personne âgée de ma circonscription perdait ses économies de toute une vie dans une fraude survenue sur votre plateforme, vous sentiriez-vous, en tant que directrice des politiques publiques pour Facebook Canada, responsable de cette perte?

Rachel Curran: Je pense que nous avons la responsabilité de réduire les fraudes et les arnaques sur notre plateforme le plus possible, en collaborant avec l'industrie, le gouvernement et les forces de l'ordre. Je pense que c'est ce en quoi consiste notre responsabilité.

Le président: D'accord. Alors si cela se produisait sur votre plateforme, diriez-vous que c'est partiellement votre responsabilité, et en partie celle de la police?

Rachel Curran: Je pense que, comme l'a décrit mon collègue Jon Camfield, la chaîne d'attaques frauduleuses s'étend à un éventail d'acteurs. Elle pourrait commencer sur Facebook. Elle pourrait commencer au sein d'une entreprise de télécommunications ou sur les SMS. Elle pourrait continuer jusqu'à un transfert bancaire. Je pense que Meta a un rôle à jouer dans cette chaîne d'attaques frauduleuses. Notre partie consiste à réduire l'incidence des fraudes et des arnaques sur notre plateforme dans la mesure du possible.

Le président: Madame Curran, combien d'argent Facebook dépense-t-elle au Canada ou mondialement par année en investisse-

ments en matière de prévention des fraudes et de prévention des arnaques?

Rachel Curran: Je n'ai pas réponse à cette question, mais je pourrai faire le suivi auprès du Comité.

Le président: Vous ne savez pas combien d'argent Meta investit annuellement pour régler un problème qui coûte aux Canadiens des milliards de dollars?

Rachel Curran: Je ne le sais pas, mais je peux vous dire que, au cours des dix dernières années, nous avons consacré 30 milliards de dollars à la sécurité sur nos plateformes, et cela comprend les fraudes et les arnaques.

Le président: Craignez-vous que les investissements dans la prévention des fraudes nuisent à votre rentabilité en tant qu'entreprise?

Rachel Curran: Pas du tout. Écoutez, Meta ne souhaite pas faire d'argent à partir de fraudes et d'arnaques. Je pense que mon collègue, Jon Camfield, peut en parler. Nous voulons que notre plateforme...

Le président: Mais faites-vous de l'argent grâce à cela?

Rachel Curran: ... soit un lieu sûr et agréable pour nos utilisateurs, et cela n'inclut pas le fait qu'ils se fassent arnaquer ou escroquer sur Facebook ou Instagram.

Le président: Gagnez-vous de l'argent grâce à la fraude?

Rachel Curran: À ma connaissance... Je l'ignore. Je ne peux pas répondre à cette question.

Monsieur Camfield...

Le président: Je vais permettre à M. Shipley, en tant qu'expert dans ce domaine, de fournir peut-être un point de vue rapide à ce sujet.

Rachel Curran: Eh bien, M. Shipley semble fournir des statistiques du Royaume-Uni...

Le président: Madame Curran, la question s'adresse à M. Shipley. Vous n'avez pas la parole.

Rachel Curran: ... qui ne s'appliquent pas au Canada.

Le président: Monsieur Shipley, allez-y.

Rachel Curran: Il semble également tirer ses statistiques des médias britanniques qui...

Le président: Madame Curran, je dois vous rappeler à l'ordre. Je sais que vous avez une longue expérience au Parlement, madame Curran. Vous connaissez sans aucun doute les règles du Parlement. En tant que président du Comité, c'est moi qui décide qui a la parole, et je vais la donner à M. Shipley pour un moment. Je poserai une autre question avant de suspendre la séance.

La parole est à vous, monsieur Shipley.

David Shipley: Merci, monsieur le président.

Je voudrais revenir sur une question soulevée par un député plus tôt, quand nous parlions de certains calculs, où le montant était non pas de 16 milliards de dollars, mais bien de 6 milliards de dollars. Cela provenait des pourcentages que nous avons entendus, et nous avons fait un calcul rapide. Il s'agissait de revenus. Ils ont tiré des profits de la fraude. Ils ne voulaient peut-être pas l'argent — et je les crois vraiment —, mais ils ont bel et bien fait de l'argent.

J'aimerais soulever un dernier point. J'étais journaliste. Nos médias locaux ont disparu du pays. Nous sommes des déserts médiatiques. Les recettes publicitaires qui soutenaient autrefois le journalisme local, sans pages entières de publicités frauduleuses, ont été absorbées par des entreprises comme celle-ci. Ils n'ont pas pris la responsabilité de ces déserts, mais leur ont offert une somme dérisoire d'environ 300 millions de dollars. Ils permettent le vol de milliards de dollars. C'est scandaleux.

Rachel Curran: Nous voyons maintenant la véritable motivation de M. Shipley, qui est...

Le président: Madame Curran, vous n'avez pas la parole.

Rachel Curran: ... de s'assurer que les éditeurs de presse reçoivent de l'argent d'entreprises comme Meta.

Le président: Vous pouvez couper le microphone de Mme Curran, s'il vous plaît, à tout moment.

Rachel Curran: Eh bien, c'est sa véritable motivation. Il ne s'agit pas de...

Le président: Je demanderais un peu de silence. Merci.

Ma dernière question s'adresse à vous, madame Curran.

Vous vous êtes engagée — et je vous remercie de cet engagement — à fournir par écrit au Comité, par l'intermédiaire de la greffière, le montant que Facebook a investi au Canada, ou à l'échelle mondiale, dans la prévention de la fraude. Je pense que si les députés des partis politiques autour de la table ne reçoivent pas rapidement cette information, ils pourraient vouloir soulever la question sur d'autres plateformes parlementaires.

Si l'on suppose que vous nous transmettiez rapidement ce chiffre, que celui-ci soit exact et qu'il prouve, une fois que vous avez effectué vos recherches à l'interne... Nous avons besoin d'un deuxième élément. Je voudrais vous demander trois choses. Premièrement, combien Facebook Canada investit-il au Canada — ou à l'échelle internationale, si vous pensez que vous ne pouvez pas dissocier les deux marchés — dans la prévention de la fraude. Deuxièmement, selon vous, à combien s'élèvent les revenus générés par des fraudes ou des escroqueries sur vos plateformes, au Canada ou à l'échelle internationale?

Ensuite, la troisième chose que je voudrais que vous transmettiez, s'il vous plaît, au Comité serait la suivante. S'il se révèle que les montants que vous avez gagnés — peut-être involontairement, comme l'a souligné M. Shipley — sur vos plateformes grâce à la fraude dépassent ce que vous avez investi, ce que je soupçonne être largement le cas, vous engagerez-vous à transmettre une réponse écrite au Comité l'informant que vous investirez la différence dans la prévention de la fraude?

Ce sont les trois points sur lesquels je vous demanderais, madame Curran, de faire rapport au Comité, s'il vous plaît, à votre convenance.

• (1745)

Rachel Curran: Oui, nous pouvons tout à fait le faire.

Je dirais que nous avons investi 30 milliards de dollars dans des mesures pour lutter contre la fraude, et dans des mesures de sécurité sur nos plateformes au cours de la dernière décennie. Je serais très surprise si ce chiffre était inférieur aux pertes causées, malheureusement, par des cas de fraude particulièrement graves et regrettables sur nos plateformes, mais nous répondrons certainement à ce sujet.

Le président: Madame Curran, la dernière question que je vous poserai est la suivante. Il s'agit peut-être davantage d'un point de réflexion que d'une question de politique technique. Cela rejoint une question que ma collègue, Mme O'Rourke, vous a posée, il y a quelques instants.

Cela fait maintenant plusieurs années que je suis parlementaire. Je travaille au Parlement depuis très longtemps. Je n'ai jamais vu, dans mon rôle de président ou de député, des témoins faire autant d'unanimité dans les parties concernant le sujet ou le contenu des questions que vous avez reçues aujourd'hui. Je voudrais que vous y réfléchissiez. Pourquoi, selon vous, des députés conservateurs, du Bloc et des députés libéraux consacrent-ils le temps précieux dont ils disposent au Comité pour vous poser les mêmes questions, et pourquoi semblent-ils, tous partis confondus, exprimer une insatisfaction quant aux réponses qu'ils reçoivent?

Rachel Curran: Je pense que c'est parce qu'il s'agit d'une question importante. C'est une question importante pour les Canadiens. Nous devons y répondre. Je sais que vous avez invité certains de nos collègues ici aujourd'hui, d'autres membres de l'industrie de la technologie, qui ont refusé de comparaître, mais nous avons accepté d'être ici parce qu'il s'agit d'une question importante.

Nous voulons veiller à réduire les fraudes et les escroqueries au Canada. Nous voulons veiller à ce que les Canadiens ne soient pas victimes de fraudes ou d'escroqueries sur nos plateformes. Nous voulons collaborer avec les décideurs comme les députés du Comité pour nous assurer que nous travaillons ensemble afin de réduire le nombre de fraudes. Monsieur le président, en toute honnêteté, c'est la raison pour laquelle nous sommes ici.

Le président: Je comprends.

Monsieur Shipley, madame Quaid, monsieur Camfield et madame Curran, merci de vous être présentés devant le Comité aujourd'hui pour tenir une discussion importante concernant le rôle que jouent divers acteurs de l'industrie et, bien sûr, les citoyens et les décideurs publics au Canada pour veiller à la santé et au bien-être de l'ensemble de la population du pays, notamment en ce qui concerne la protection contre la fraude et les escroqueries. Je vous remercie de votre temps.

Chers collègues, je vais suspendre la séance pour cinq minutes, le temps d'accueillir les prochains témoins, qui comparaitront en ligne.

• (1745)

(Pause)

• (1750)

Le président: Nous allons poursuivre notre deuxième heure.

Chers collègues, merci de reprendre vos places. Nous sommes très en retard, et nous allons faire de notre mieux pour tenir une discussion constructive et approfondie.

Nous accueillons M. Nicholas Giurietto, de l'Australian Banking Association. Monsieur, vous êtes à l'autre bout du monde, à un autre moment de la journée. Votre journée ne fait que commencer, tandis que la nôtre est terminée, et nous cherchons à y ajouter un peu de temps. Merci beaucoup de vous être rendu disponible. Nous apprécions vraiment le lien solide et le partenariat entre nos deux pays.

Vous aurez jusqu'à cinq minutes. Je sais qu'il y a beaucoup d'intérêt pour ce que vous allez dire. Ce n'est que la deuxième réunion que nous tenons concernant cette étude, mais l'exemple australien a été mentionné à plusieurs reprises, et nous avons hâte d'en découvrir davantage à l'aide de votre témoignage.

Sur ce, vous avez la parole pour cinq minutes ou moins.

• (1755)

Nicholas Giurietto (Responsable des politiques futures, Australian Banking Association Inc.): Merci, monsieur le président.

Bonsoir, et bonjour de l'Australie.

Je m'appelle Nicholas Giurietto, et je suis le responsable de la politique sur les crimes financiers à l'Australian Banking Association. Il s'agit du principal organisme qui représente le secteur bancaire en Australie. Mon domaine de responsabilité comprend la lutte contre le blanchiment d'argent et le financement du terrorisme, la cybersécurité et les escroqueries, et j'ai participé activement à l'élaboration et, désormais, à la mise en œuvre du cadre de gouvernement australien relatif à la prévention des escroqueries. Cela a nécessité une collaboration avec des organismes politiques du gouvernement, divers organismes de réglementation et des collègues provenant d'autres secteurs de l'industrie.

Le but commun de tous ces intervenants est de protéger autant que possible les Australiens contre le fléau des escroqueries commises par des gangs du crime organisé à l'échelle mondiale. Notre approche est de travailler en collaboration pour mettre fin aux escroqueries avant qu'elles ne soient commises, et non pas simplement exiger qu'une seule partie de la chaîne de l'escroquerie assume la responsabilité de protéger ou de rembourser les clients. Il est question de reconnaître la complexité de notre monde numérique en travaillant en collaboration pour mettre fin aux escroqueries à la source. Le cadre australien de prévention des escroqueries a suscité beaucoup d'attention à l'échelle mondiale en tant que premier exemple du régime réglementaire de lutte contre les escroqueries reposant sur le principe selon lequel tous les secteurs de l'industrie doivent contribuer à la lutte contre les escroqueries.

Il est difficile d'être le premier. De nombreux détails doivent encore être réglés pour traduire une proposition de politique simple et importante en mise en œuvre concrète. Cela peut être difficile, en pratique. Il reste quelques problèmes à résoudre en Australie. Néanmoins, les premiers signes sont positifs, et nous restons plus que jamais convaincus que la seule manière de réduire au minimum les préjudices dévastateurs que les escroqueries causent tous les jours aux Australiens est d'adopter une approche écosystémique coordonnée et intersectorielle dans laquelle chaque secteur de l'industrie fait sa part.

Le cadre de prévention des escroqueries repose sur deux principes de base. Le premier principe consiste à reconnaître que les méthodes perfectionnées des attaques frauduleuses se produisent dans tous les secteurs de l'industrie et exploitent souvent, de manière délibérée, les failles entre eux. Le cadre de prévention des escroqueries nécessite que tous les secteurs faisant partie de la chaîne de l'escroquerie prennent des mesures appropriées pour prévenir les attaques frauduleuses, les détecter et y réagir.

Chaque secteur a la responsabilité de renforcer ses processus opérationnels pour se protéger contre les fraudeurs, au moyen d'obligations analogues, mais adaptées à chaque industrie. Par exemple, les exigences imposées aux banques de procéder à des vé-

rifications rigoureuses de l'identité du client lors de l'ouverture d'un compte sont assorties d'une obligation analogue pour les sociétés de télécommunications de vérifier le besoin légitime d'une entreprise de disposer d'un boîtier SIM pouvant envoyer des dizaines de milliers de messages textes à l'heure, ou l'obligation imposée à des plateformes numériques de confirmer la bonne foi d'un annonceur d'un produit d'investissement. Les obligations exactes sont différentes, mais l'objectif de chaque secteur est le même: s'efforcer d'empêcher les acteurs malveillants d'entrer dans le système dès le départ.

En Australie, nous avons entamé la mise en œuvre du cadre de prévention des escroqueries auprès des trois principaux secteurs: les banques, les sociétés de télécommunications et les plateformes numériques, ce qui reconnaît qu'en pratique il faut commencer quelque part. Il est toutefois reconnu que notre dispositif national de protection contre les escroqueries ne sera pas complet tant que tous les autres secteurs pouvant intervenir dans une chaîne de fraude ne feront pas également partie de l'intervention coordonnée. Ils comprennent les échanges de cryptomonnaie, les expéditeurs non bancaires de fonds, les fournisseurs de logiciel d'accès à distance, les marchés en ligne, les fournisseurs de cartes-cadeaux et bien d'autres. Malheureusement, l'ingéniosité des fraudeurs n'a presque pas de limite, et cela reconforte peu une victime d'escroquerie de savoir que la porte d'accès à ses économies a été sécurisée si des voleurs ont pu s'introduire par la fenêtre.

Le deuxième principe clé du cadre de prévention des escroqueries est l'échange de données dans l'ensemble de l'industrie: faciliter l'échange sécurisé et conforme aux exigences de protection de la vie privée de données indiquant un risque de fraude. Les renseignements exploitables sur les escroqueries, tels que définis dans les lois relatives au cadre de prévention des escroqueries, sont un outil essentiel de la lutte contre les fraudes.

Malgré les meilleurs efforts de l'ensemble des intervenants, il n'est pas toujours possible de protéger la première victime d'une escroquerie, mais l'échange rapide de renseignements exploitables sur les fraudes, suivi d'une action immédiate — par exemple la fermeture d'un site Web frauduleux ou le blocage d'un numéro de téléphone ou d'un compte bancaire compromis — peut rapidement combler cette faille et protéger des centaines, voire des milliers d'éventuelles victimes subséquentes. Les fraudeurs peuvent continuer de tester les dispositifs de défense, mais en réduisant leur taux de réussite et en augmentant le coût de leur modèle économique, nous rendons l'Australie moins attrayante comme cible.

L'approche la plus efficace pour assurer un échange de données dans l'ensemble de l'industrie est la collaboration des secteurs privés — par exemple, par l'entremise de l'Australian Financial Crimes Exchange, dont les représentants, à ce que je comprends, comparaissent aujourd'hui — à l'aide de liens appropriés vers les organismes d'application de la loi. Le rôle principal du gouvernement est de fournir le cadre politique qui permet un échange de données sécurisées conformes à la protection de la vie privée, assorti de protections de sécurité.

• (1800)

Je vais maintenant conclure mes premiers commentaires, et je serai ravi de fournir au Comité tout autre renseignement qu'il souhaite obtenir au sujet de notre expérience en Australie.

Le président: Merci beaucoup, monsieur.

Je ne vous ai pas posé la question, mais de quelle partie de l'Australie nous parlez-vous?

Nicholas Giurietto: Je suis à Sydney.

Le président: C'est merveilleux.

Monsieur Guglielmin, vous avez la parole pour six minutes.

Michael Guglielmin (Vaughan—Woodbridge, PCC): Merci, monsieur le président.

Je remercie notre témoin de sa déclaration préliminaire et de prendre le temps de témoigner devant nous depuis les antipodes.

Comme les membres du Comité le savent, il s'agit d'une étude très importante qui arrive à point nommé. Nous avons tous entendu dans nos circonscriptions d'innombrables histoires au sujet de différents cas de fraude et de personnes âgées qui ont été victimes de fraude.

J'ai une histoire à raconter au sujet d'une personne qui, sur une période de neuf mois, a été victime d'une fraude qui lui a fait perdre toutes ses économies. Tout a commencé par une fraude informatique commise par l'envoi d'un message sur son ordinateur, puis la situation s'est transformée en une fraude psychologique interminable, qui a duré neuf mois. Cette personne croyait avoir affaire au FBI et a fini par verser toutes ses économies au fraudeur, sans qu'aucune des institutions bancaires ayant autorisé cette transaction ait à rendre de comptes. Cette personne ne disposait en fait d'aucun recours.

La situation de l'Australie est particulièrement importante pour nous, parce que votre cadre de prévention semble reposer sur une approche écosystémique, qui reconnaît, comme vous l'avez dit, que les fraudes sont d'abord commises en amont, avant même que de l'argent ne soit versé. Je me demandais si vous pouviez expliquer au Comité ce que cela signifie concrètement. Qui est assujéti à la réglementation? Quelles obligations s'appliquent? Comment le système parvient-il à intégrer les banques, les entreprises de télécommunications et les entreprises de plateformes numériques à la même chaîne de reddition de comptes?

Nicholas Giurietto: Le Parlement australien a adopté un cadre législatif de prévention des escroqueries en février de l'année dernière. Le règlement habilitant a commencé à faire son chemin dans le système. Le règlement repose essentiellement sur le principe selon lequel chaque secteur d'activité clé — les entreprises de plateformes numériques, le secteur des télécommunications et le secteur bancaire — est assujéti à un ensemble d'obligations définies dans les rubriques « détecter », « prévenir » et « contrer » les escroqueries. Il y a quelques autres rubriques, dont la gouvernance, mais ce sont les trois plus importantes.

Ces secteurs relèvent de leur propre organisme de réglementation. Dans le cas du secteur bancaire, notre organisme de réglementation habituel, l'Australian Securities and Investments Commission, est responsable de la réglementation en matière d'escroqueries. Il en va de même pour les entreprises de télécommunications et leur organisme de réglementation, tandis qu'un nouvel organisme de réglementation destiné aux entreprises de plateformes a dû être mis sur pied, puisqu'il n'en existait pas jusqu'à maintenant.

Chacun de ces secteurs est assujéti à des obligations prévues par un code, qui sont gérées par les organismes de réglementation. D'ailleurs, il y a un nouveau « super organisme » de réglementation, si vous voulez, qui chapeaute de façon transversale la réglementation relative aux escroqueries et vise tous les secteurs. Il a pour rôle de s'assurer que les obligations sont harmonisées et équivalentes.

Dans ma déclaration préliminaire, j'ai affirmé que tenir tout d'abord les mauvaises personnes à l'écart du système est une façon de protéger vos citoyens. Les banques le font en appliquant la règle de la connaissance du client et par l'intermédiaire des entreprises de télécommunications. Si une personne souhaite vraiment envoyer 10 000 textos en une minute — et il y a des raisons légitimes de vouloir le faire —, renseignez-vous au sujet de cette personne. S'agit-il d'une utilisation légitime? Ne laissez pas simplement n'importe qui utiliser ce produit. Il en va de même pour les entreprises de plateformes; si une personne veut faire la publicité d'un produit financier, vérifiez qu'elle détient effectivement une licence australienne l'autorisant à offrir des services financiers — c'est-à-dire la licence requise pour la vente de produits d'investissement en Australie — avant de l'autoriser à faire la publicité de son produit.

Les obligations qui s'appliquent à chaque secteur sont différentes, mais elles sont de même nature, puisqu'elles ont le même objectif...

Le président: Je suis désolé, monsieur Giurietto. Je pensais que vous aviez terminé.

Avant de redonner la parole à M. Guglielmin, je voulais simplement dire qu'un autre témoin vient de se joindre à nous, M. David Pegley, qui est le directeur général de l'Australian Financial Crimes Exchange.

Monsieur Pegley, bienvenue. Malheureusement, nous n'aurons pas le temps d'entendre vos remarques préliminaires.

Toutefois, chers collègues, n'hésitez pas à poser des questions à M. Pegley qui est présent ici, aujourd'hui, à titre de témoin.

Monsieur Guglielmin, il vous reste un peu plus de deux minutes.

• (1805)

Michael Guglielmin: À l'heure actuelle, le Canada impose l'essentiel de ses obligations aux banques, qui ne détectent la fraude qu'une fois que l'argent a été transféré. Pour ce qui est de l'Australie, que se passe-t-il si le gouvernement impose cette responsabilité aux banques, alors que les entreprises de plateformes et de télécommunications ont moins d'obligations?

Nicholas Giurietto: L'écosystème australien, en particulier, fait en sorte que tous les secteurs, actuels et futurs, sont tout autant responsables de lutter contre la fraude. Si l'on impose seulement cette obligation aux banques, on finit par essayer de contenir un feu qui brûle déjà. Il existe des mesures que les banques peuvent, devraient et doivent prendre pour sécuriser leurs plateformes.

Surtout dans le cas des entreprises de télécommunications et de plateformes, lorsqu'elles prennent des mesures plus tôt, elles peuvent contrer les escroqueries plus rapidement. Ce qui est essentiel ici, c'est que les secteurs puissent s'échanger des renseignements. Lorsqu'une banque apprend qu'une personne a été victime d'une arnaque, si nous pouvons transmettre cette information à une entreprise de télécommunications ou à une entreprise de plateforme... Il est peut-être trop tard pour venir en aide à cette première victime — c'est vrai, et c'est dévastateur —, mais, au moins, l'information transmise peut empêcher qu'il n'y ait de nouvelles victimes.

Au fil du temps, il devient donc plus coûteux pour les fraudeurs de prendre pour cible l'Australie plutôt qu'un autre pays, et ils pourraient donc concentrer leurs efforts ailleurs.

Michael Guglielmin: Vous avez indiqué qu'environ 90 % des pertes liées aux escroqueries en Australie sont attribuables à des pertes individuelles de plus de 5 000 dollars australiens. Ce sont des pertes que l'Australian Banking Association décrit comme étant « bouleversantes ». Qui subit le plus durement ces pertes?

Nicholas Giurietto: Les victimes d'escroqueries sont issues de tous les groupes de la société. On croit parfois à tort que seules les personnes âgées en sont victimes. En réalité, les fraudeurs sont de fins psychologues, et ils trouveront une façon de piéger pratiquement n'importe qui. Il pourrait s'agir d'un parent qui dépose ses enfants à l'école et qui répond à un texto pendant qu'il essaie de garer sa voiture. Les fraudeurs peuvent employer tant de moyens pour y parvenir qu'il n'y a pas de manière typique de s'y prendre.

Chaque citoyen est une victime potentielle d'arnaque, et chaque citoyen a donc besoin de soutien pour s'en protéger.

Michael Guglielmin: Merci.

Le président: Merci beaucoup, monsieur Guglielmin.

Nous allons maintenant passer à Mme O'Rourke pour six minutes.

Dominique O'Rourke: Merci, monsieur le président.

Monsieur Giurietto ou monsieur Pegley, la Chambre est actuellement saisie d'un projet de loi présenté par le gouvernement concernant l'accès légal, qui permettrait aux organismes d'application de la loi d'avoir un meilleur accès aux plateformes afin d'intercepter rapidement des activités criminelles, qu'il s'agisse de fraudes ou de traite de personnes.

Je me demandais si vous pourriez nous dire à quel point les mesures relatives à l'accès légal en Australie vous ont aidés à lutter contre la fraude.

Nicholas Giurietto: Je vais peut-être laisser M. Pegley répondre en partie à la question, mais la collaboration avec les organismes d'application de la loi est absolument essentielle à l'ensemble des interventions de lutte contre les escroqueries et la fraude. Tout comme au Canada, le système fédéral de l'Australie comporte des responsabilités policières qui se chevauchent, ce qui peut parfois compliquer les choses. Toutefois, il est très important de pouvoir échanger des renseignements et prendre des mesures, que ce soit en communiquant des renseignements ou, dans certains cas, en appuyant les organismes d'application de la loi.

L'échange de renseignements entre entités privées est tout aussi important, du fait que, parfois, le secteur privé peut se servir de ce qu'on appelle des indices de fraude qui ne satisfont pas à la norme juridique que les organismes d'application de la loi pourraient devoir respecter avant d'engager des poursuites ou de prendre d'autres mesures. Il s'agit simplement de renseignements qui peuvent être communiqués afin de prévenir un secteur qu'il faudrait surveiller certaines activités et envisager de prendre certaines mesures; il s'agit de signaler un risque. Cela est également très important. Ces deux approches peuvent être adoptées conjointement.

Dominique O'Rourke: Souhaitez-vous dire rapidement autre chose à ce sujet? J'ai deux autres questions à poser.

David Pegley (directeur général, Australian Financial Crimes Exchange Ltd.): Certainement. Merci de m'en donner la possibilité.

Pour donner suite aux commentaires de M. Giurietto, je dirais que, selon notre expérience, le travail que nous réalisons en matière

de prévention et de détection fait nécessairement en sorte que nous intervenons avant qu'un crime ne soit commis ou pendant qu'il est commis. Nous avons constaté que...

Le président: Monsieur Pegley, je dois vous interrompre un instant. En fait, cela s'adresse aux deux témoins. Il est vraiment important que vos microphones soient correctement placés.

Nous allons reprendre avec vous, monsieur Pegley, pour voir si tout fonctionne bien. Nous allons faire un petit essai avant que vous ne poursuiviez.

Je vais arrêter la minuterie, madame O'Rourke.

• (1810)

David Pegley: Est-ce que ça fonctionne? Le micro est-il mieux placé?

Le président: Pourriez-vous relever un peu le support du microphone? Essayez cela.

David Pegley: Merci.

Bien que nous échangions du renseignement avec les intervenants du secteur privé, nous entretenons également des relations officielles avec tous les organismes étatiques et fédéraux d'application de la loi. Cela leur permet de nous demander d'obtenir des renseignements opérationnels qui appuieront leurs activités, qui se déroulent généralement après coup. Nous essayons toujours de communiquer le plus rapidement possible à l'ensemble de l'écosystème des renseignements provenant des consommateurs. Par la suite, les organismes d'application de la loi sont très désireux d'obtenir des données de masse qui sont nécessaires pour appuyer leurs activités. La plupart du temps, le crime a déjà été commis.

La plupart des crimes auxquels nous avons fait face ont été commis à l'étranger, malheureusement. Certaines activités nationales impliquant des mules financières ont été repérées, ainsi que des activités liées aux boîtiers SIM dont M. Giurietto parlait plus tôt. Toutefois, la grande majorité des malfaiteurs qui ciblent la population australienne se trouve à l'étranger.

Dominique O'Rourke: J'ai quelques questions à poser. Pouvez-vous rappeler au Comité les résultats que vous avez observés en Australie un an seulement après la mise en place de votre nouveau cadre? Comment les entreprises de plateformes ont-elles réagi en Australie? À quel point est-il important que les clients sachent qu'il est difficile de récupérer des fonds perdus?

Nicholas Giurietto: Il faut tenir compte de quelques éléments.

Le projet de loi relatif au cadre de prévention des escroqueries a été adopté, mais sa mise en œuvre est encore en cours. Il est en fait encore un peu trop tôt pour se prononcer sur l'effet direct qu'aura cette mesure législative, même si l'annonce du cadre de prévention des escroqueries a déjà eu un effet positif, puisqu'il a favorisé la collaboration entre les secteurs.

Nous avons constaté une diminution du volume des arnaques. Les chiffres sont, malheureusement, un peu difficiles à interpréter, parce qu'ils proviennent de multiples sources et que certaines questions légitimes se posent quant à la meilleure façon de les comptabiliser. On pourrait probablement dire que, au pire, les chiffres restent stables, mais que toute autre option serait préférable. Il y a une collaboration entre les secteurs.

À ce stade-ci, nous sommes parvenus à mener certains projets pilotes importants avec les entreprises de plateformes. Les banques ont transmis des renseignements aux entreprises de plateformes, qui ont pu les utiliser pour retirer du contenu frauduleux. À mesure que le cadre de prévention des escroqueries sera mis en œuvre à l'échelle industrielle, nous nous attendons à ce qu'il contribue encore plus à la réduction des pertes causées par les escroqueries.

Dominique O'Rourke: Merci.

Le président: Merci beaucoup, madame O'Rourke.

[Français]

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

Gabriel Ste-Marie: Merci, monsieur le président.

Je salue les deux témoins qui sont ici aujourd'hui. Nous leur sommes reconnaissants d'être des nôtres.

Monsieur Pegley, vous n'avez pas eu le temps de faire votre présentation. Si vous voulez la faire maintenant, je vous offre le temps qui m'est alloué pour poser mes questions. Cela va nous permettre de bien comprendre le message que vous avez à nous transmettre.

[Traduction]

Le président: Monsieur Pegley, est-ce que tout fonctionnait? Est-ce que vous pouviez entendre?

David Pegley: Oui, en français.

Le président: D'accord. Je vais vous faire l'interprétation. Nous allons régler le problème.

En gros, M. Ste-Marie disait que vous n'aviez pas eu la possibilité, au début, de faire votre déclaration préliminaire, et il serait heureux de vous offrir le temps qui lui est alloué pour que vous puissiez donner votre opinion.

David Pegley: Merci.

Peut-être devrais-je brièvement décrire ce que fait l'Australian Financial Crimes Exchange, soit surtout de soutenir le travail de l'ABA et d'autres organismes de l'industrie. Nous assurons un partage de renseignement entre de multiples industries. En ce moment, nous avons environ huit industries différentes avec lesquelles nous partageons du renseignement. Il y a environ 100 membres avec qui nous partageons du renseignement en Australie. Nous soutenons également, de façon distincte, le partage de renseignement parmi des banques néo-zélandaises dans le même but.

Ces industries vont d'entreprises de contenus multimédias numériques aux compagnies de téléphone et compagnies d'assurance en passant, bien sûr, par des banques, des compagnies de télécommunications et des compagnies d'échange de devises numériques pour répondre aux trois parties du cadre de prévention des escroqueries, comme l'a décrit M. Giurietto. Dans le cadre de prévention, nous recueillions les informations d'une victime et nous les communiquons aux plateformes d'échange numérique concernées, ou nous les transmettons à la compagnie de télécommunications. Cela a été une façon très fructueuse de contrer rapidement et en temps réel les mauvais acteurs qui évoluent autour de la communauté. Nous transmettons également du renseignement qui permet de détecter des transactions vers de mauvais comptes bancaires ou des régimes de devises numériques qui ont été utilisés pour exfiltrer des fonds, de façon à nuire économiquement aux criminels.

Nous sommes également en faveur du suivi — et, on l'espère, du blocage — en temps réel des fonds au sein des institutions pour

permettre, du mieux que nous le pouvons, la restitution des fonds des victimes en leur nom partout dans le secteur bancaire. Il existe un mécanisme de signalement des fraudes qui permet tout, depuis l'échange de devises numériques avant que les devises ne passent de monnaie fiduciaire à numérique... et dans le secteur bancaire pour tenter d'empêcher les fonds de circuler, car ils circuleront très rapidement hors de l'Australie.

• (1815)

Le président: Monsieur Pegley, au bas de votre écran, il devrait y avoir l'option de passer au canal en anglais. Ça devrait régler le problème d'interprétation. Sinon, c'est correct. Je traduirai pour vous.

[Français]

Monsieur Ste-Marie, vous avez la parole.

Gabriel Ste-Marie: Monsieur Pegley, pouvez-vous me dire si vous avez accès à l'interprétation?

Le président: Je ne pense pas que ce soit le cas, monsieur Ste-Marie.

Cela dit, vous pouvez poser votre question. Si je ne traduis pas exactement vos paroles, vous pourrez me corriger.

Gabriel Ste-Marie: C'est très bien.

Quand le nouveau modèle a été mis en place, quelles ont été les difficultés? Quels étaient les commentaires des diverses entreprises?

[Traduction]

Le président: Monsieur Pegley, avez-vous entendu cela?

David Pegley: Oui, j'ai entendu. Merci.

Le président: Bien. Allez-y, je vous en prie.

David Pegley : L'aspect le plus intéressant du modèle des trois secteurs est sûrement l'identification d'attributs pertinents destinés à être partagés entre ces secteurs. Ce qui est utile à une banque pour détecter les transactions frauduleuses n'est pas nécessairement ce qui serait utile à une compagnie de téléphone. Une plateforme de devises numériques a une manière très différente de suivre les transactions. Les plateformes de contenus multimédias numériques ne sont pas du tout habituées à suivre des transactions de cette manière. Nous avons travaillé très dur pour déceler les attributs pertinents à communiquer et le renseignement destiné à être transmis entre les plateformes.

Un aspect intéressant est que, dans de nombreux cas, ces industries ne travaillent pas nécessairement ensemble très souvent sur les problèmes les plus courants. Les plateformes numériques sont invariablement de solides compétiteurs. Les compagnies de téléphone sont à peu près pareilles. L'idée selon laquelle ils collaboreraient est un concept étranger.

Beaucoup du travail que nous faisons est axé sur l'établissement d'une certaine confiance entre les parties lorsque nous transmettons du renseignement et de façon à cerner les mauvais acteurs, si vous le voulez, comme justification. Le milieu bancaire est beaucoup plus habitué à collaborer dans le cadre de cette activité. Il l'est depuis des années, alors cette partie du processus est beaucoup plus facile. La traduction, si vous voulez, entre les différents secteurs de différentes formes de renseignement qui les aideront à arrêter les arnaques, a exigé des efforts, mais nous y arrivons.

[Français]

Gabriel Ste-Marie: Merci beaucoup.

Merci, monsieur le président.

Le président: Merci beaucoup.

Vu que nous avons accumulé du retard, je vais réduire le dernier tour de parole de quelques minutes.

[Traduction]

Monsieur Falk, vous disposerez de deux minutes et demie, et serez suivi de M. Ma, qui disposera de deux minutes et demie. Ensuite, nous suspendrons brièvement la séance, puis passerons un moment à huis clos pour arriver au rapport dont nous devons discuter aujourd'hui.

Monsieur Falk, la parole est à vous pour deux minutes et demie, monsieur.

• (1820)

Ted Falk: Merci.

Merci beaucoup de votre témoignage de cet après-midi, ou de ce matin — quelle que soit l'heure de votre côté.

Selon vous, quelle est la partie la plus efficace du projet de loi pour lutter contre les arnaques?

Nicholas Giurietto: Je dirais que la composante la plus efficace est le fait qu'il présente les responsabilités de chaque secteur comme étant équivalentes, mais différentes. Ce que je veux dire par cela, c'est qu'il reconnaît que chaque secteur, en raison de la technologie qu'il utilise, de son modèle d'affaires, etc., a inévitablement des capacités différentes et des responsabilités différentes. Une partie de cela tient aux problèmes de données dont parlait M. Pegley.

L'idée générale selon laquelle il existe une responsabilité de travailler à prévenir, à détecter et à répondre aux arnaques — ces trois étiquettes — devient vraiment importante. En travaillant dans les banques, je peux examiner les obligations des compagnies de téléphone et des plateformes et demander ce qu'elles font pour empêcher les arnaques et ce que nous faisons. Est-ce à peu près la même chose? Tentons-nous de faire le même genre de choses? Que faisons-nous pour détecter les arnaques? Surtout dans le secteur du partage de données, c'est très important. Les données que nous fournissons sont-elles utiles, et quelle est la réponse?

Il est question d'avoir un cadre général qui transcende le cloisonnement réglementaire, car, historiquement, chacun de ces secteurs était réglementé dans son propre vase clos. Le secteur a son propre organisme réglementaire, et les secteurs ne travaillent pas nécessairement ensemble à l'extérieur de ces limites verticales. Forcer un dialogue à l'échelle non seulement sectorielle, mais également réglementaire — en éliminant les vases clos — est sûrement l'élément de base qui bénéficie le plus au cadre de prévention des arnaques.

Ted Falk: Trouvez-vous que les plateformes de réseaux sociaux ont aussi été coopératives?

Nicholas Giurietto: Elles travaillent avec nous sur un certain nombre d'initiatives dans le cadre. Il est juste d'affirmer qu'elles avaient un long chemin à parcourir et peut-être un peu plus à faire, mais, pour le moment, l'obligation légale encourage la collaboration, et nous travaillons avec elles sur plusieurs fronts pour concrétiser cette collaboration.

Ted Falk: Merci.

Le président: Merci beaucoup, monsieur Falk.

Monsieur Ma, vous avez la parole. Vous disposez de deux minutes et demie, monsieur.

Michael Ma: Merci.

Merci, messieurs, d'être venus à court préavis.

Bien évidemment, je salue le modèle australien, et nous avons été témoins de certaines réussites. Malgré ces succès, il subsiste des vulnérabilités dans le traitement des fraudes financières au sein du système bancaire australien. Par exemple, selon la Consumers' Federation of Australia, les pertes liées aux arnaques pour les peuples des Premières Nations ont augmenté de 70 % pour atteindre 6,5 millions de dollars. Cela soulève quelques inquiétudes de bonne foi concernant l'équité.

Si nous venions à appliquer le modèle australien dans un contexte canadien, pourquoi cette disparité existe-t-elle?

Nicholas Giurietto: Je crois que j'ai fait remarquer plus tôt qu'il existe une arnaque pour tout le monde dans la société, et que les arnaqueurs sont très doués pour cibler les caractéristiques et les vulnérabilités propre à chaque communauté.

Pour donner un autre exemple, plusieurs des personnes qui arrivent en Australie du Vietnam ou de la Chine seront victimes d'arnaques où des gens font semblant d'être des autorités judiciaires originaires de ces pays. Pour les peuples des Premières Nations, il y a une difficulté particulière concernant ce que nous appelons le piège du « scrambling », le faux jeu en ligne, qui est un genre d'arnaque qui ressemble à un jeu en ligne. Ce genre d'arnaque est devenu assez populaire parmi les communautés. L'intervention principale à faire là, que les banques prennent très au sérieux, est d'assurer une éducation communautaire pour expliquer que ce qui semble être une manière de se divertir et de peut-être gagner un peu d'argent est en réalité une arnaque.

Un de ces défis tient au fait que la limite entre le jeu légal et illégal n'est pas toujours claire, alors travailler avec les organismes de réglementation pour préciser cela est aussi important. Je crois que votre argument plus général est le fait que tout le monde dans la société est susceptible d'être la proie d'un certain type d'arnaque, et l'éducation est un des principaux outils pour remédier à cela et s'assurer que les gens sont au courant de la manière dont ils sont ciblés par les arnaqueurs.

Michael Ma: Comment est-ce que le Canada peut miser sur le succès de l'Australie tout en s'assurant qu'aucune communauté n'est laissée pour compte?

Nicholas Giurietto: Je crois qu'un succès général découle d'une approche fondée sur l'écosystème, où la responsabilité est répartie entre tous ces acteurs. Je sais qu'en ce moment on met beaucoup l'accent sur les banques, les compagnies de télécommunications et les plateformes numériques, mais il existe d'autres secteurs qui jouent un rôle crucial. Ils doivent aussi être inclus si l'on veut s'assurer que personne n'est laissé pour compte.

La meilleure manière d'y parvenir est d'être informé quant à l'utilisation des données. Nous travaillons à améliorer la qualité des données qui nous indiquent qui a été arnaqué, de quel type d'arnaque il s'agit, quelles sont les données démographiques, etc. Si nous pouvons bien utiliser ces données, nous pourrions beaucoup mieux comprendre la nature spécifique de l'arnaque, sa cible et la façon dont l'arnaque a été mise en place. Cela permet l'implantation de mesures préventives, éducatives ou de tout ce sur quoi il faut attirer l'attention.

Un message général de type « faites attention aux arnaqueurs » fonctionne seulement pendant quelques mois — s'il fonctionne tout court — et il devient ensuite un simple bruit de fond. Vous avez besoin d'un message ciblé concernant des arnaques spécifiques, fondé sur les données.

● (1825)

Michael Ma: Je crois que mon temps est écoulé.

Le président: Merci, monsieur Ma.

Messieurs, merci beaucoup d'avoir comparu ici aujourd'hui. Je sais que cela vous a semblé un peu court, mais nous avons en fait un groupe de témoins beaucoup plus petit que d'habitude, ce qui veut dire que nous avons probablement pu poser plus de questions qu'en temps normal, ce qui est très bien.

Je vous encourage, du mieux que vous pouvez, à surveiller les prochaines réunions du Comité concernant le sujet qui nous occupe. S'il y a des choses que vous voyez et que vous pensez être une erreur pour le gouvernement du Canada ou des choses que vous approuveriez comme futures orientations en fonction des expériences que vous avez vécues en Australie, nous serions certainement ouverts à votre rétroaction, car vous n'êtes pas qu'un allié: vous êtes clairement des leaders dans ce domaine dans vos administrations respectives.

Messieurs, je vous remercie. Nous vous souhaitons une excellente fin de journée en Australie.

Chers collègues, nous allons brièvement suspendre la séance.

[*Français*]

Monsieur Ste-Marie, on va vous envoyer un nouveau lien.

[*Traduction*]

Nous allons prendre une pause de cinq minutes tandis que nous passons à la suite des choses, et puis nous reprendrons nos travaux.

La séance est levée.

[*La séance se poursuit à huis clos*]

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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