



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

45^e LÉGISLATURE, 1^{re} SESSION

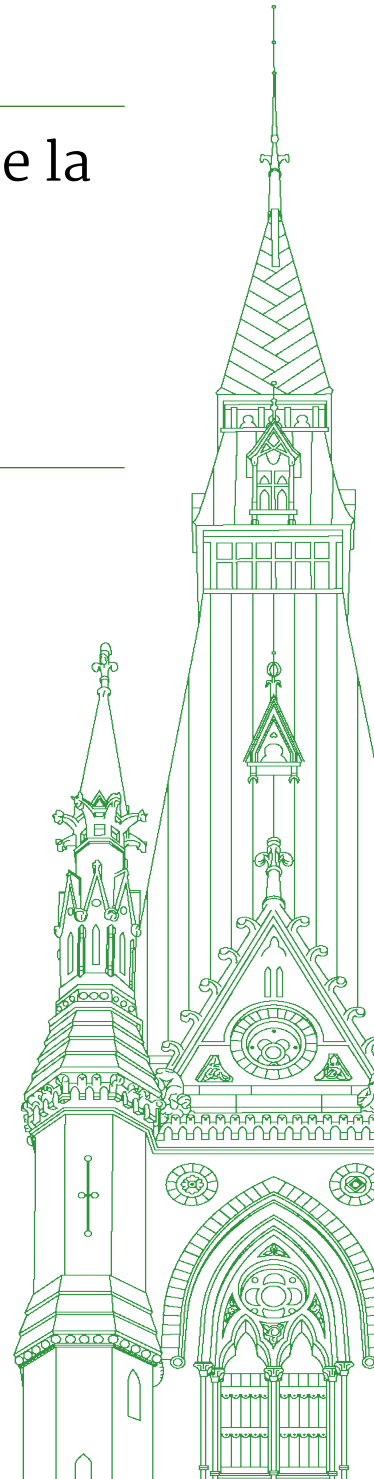
Comité permanent de l'industrie et de la technologie

TÉMOIGNAGES

NUMÉRO 044

Le jeudi 11 juin 2026

Président : Ben Carr



Comité permanent de l'industrie et de la technologie

Le jeudi 11 juin 2026

• (1100)

[Traduction]

Le président (Ben Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour, chers collègues. Nous allons commencer. Je demande au personnel et à toutes les personnes qui discutent de bien vouloir parler plus bas, s'il vous plaît.

Chers collègues, nous poursuivons notre étude sur les fraudes. Aujourd'hui, c'est la troisième réunion que nous tenons sur ce sujet ici, au comité de l'industrie.

À l'intention des témoins présents dans la salle, je vous rappelle que si votre oreillette est branchée mais qu'elle ne se trouve pas dans votre oreille, veuillez vous assurer qu'elle est posée sur l'auto-collant devant vous afin de protéger la santé et le bien-être des interprètes.

[Français]

Je peux aussi confirmer qu'on a fait aussi tous les tests visuels et de son.

[Traduction]

Deux témoins se joignent à nous virtuellement aujourd'hui en plus du témoin présent dans la salle. Nous accueillons Sarah Corrigan-Brown, avocate générale à la British Columbia Securities Commission.

Madame Corrigan-Brown, je comprends bien que, au petit matin en Colombie-Britannique, vous vous êtes montrée très compréhensive face à la nécessité pour nous d'effectuer tous les examens, alors nous tenons à vous remercier d'emblée de votre coopération à cet égard.

Nous accueillons M. Jude Pinto, chef de la mise en œuvre à Paiements Canada, qui est présent dans la salle avec nous aujourd'hui, et nous accueillons M. Ian Paterson, président-directeur général de Plurilock Security Inc.

Mesdames et messieurs les témoins, vous aurez chacun jusqu'à cinq minutes pour présenter votre déclaration préliminaire; après, nous nous tournerons vers nos collègues autour de la table pour les questions et les réponses.

Sur ce, madame Corrigan-Brown, vous avez la parole pour cinq minutes ou moins pour présenter votre déclaration préliminaire.

Sarah Corrigan-Brown (avocate générale, British Columbia Securities Commission): Monsieur le président, et membres du Comité, merci beaucoup de m'avoir invitée à me joindre à vous et à contribuer à votre étude importante sur les fraudes financières et les escroqueries au Canada.

Je m'appelle Sarah Corrigan-Brown. Je suis l'avocate générale de la B.C. Securities Commission, la BCSC. Je me joins à vous virtuellement aujourd'hui depuis Vancouver.

Le fléau des fraudes financières existe depuis longtemps, mais au cours de la dernière décennie, et surtout depuis la pandémie, il s'est propagé et intensifié à la manière d'un virus mutant, bien plus contagieux et virulent que jamais auparavant. Nous sommes très heureux de voir que le gouvernement fédéral prend actuellement des mesures visant à lutter contre les fraudes, y compris l'intention du gouvernement de lancer un nouvel organisme de lutte contre les crimes financiers.

La B.C. Securities Commission et les organismes de réglementation canadiens des valeurs mobilières, qui surveillent les marchés nationaux des investissements et contribuent à l'intégrité du système financier du Canada, ont été en première ligne dans ce combat. Les organismes de réglementation des valeurs mobilières ont le mandat de protéger les investisseurs contre les pratiques frauduleuses, abusives et trompeuses. Nous considérons la croissance exponentielle des fraudes financières comme étant l'une des plus grandes menaces aux investisseurs aujourd'hui.

La prévention et la détection des fraudes sont essentielles, mais la lutte contre les fraudes nécessite également l'application rigoureuse et efficace de la loi. Aujourd'hui, je veux vous parler de l'un des aspects de la loi canadienne qui mine nos efforts d'application de la loi.

Quand les fraudeurs se trouvent au Canada, les organismes de réglementation des valeurs mobilières comme la BCSC engagent des procédures officielles devant les tribunaux administratifs. Ces tribunaux, bien que composés d'experts reconnus en droit des valeurs mobilières et liés par des règles d'équité procédurales, ont le pouvoir d'exclure du marché de l'investissement les contrevenants et de leur imposer des sanctions financières. Ces sanctions peuvent parfois s'élever à des millions de dollars. Elles jouent un rôle essentiel pour dissuader les contrevenants eux-mêmes de commettre de nouveaux actes répréhensibles, mais elles dissuadent également d'autres personnes qui pourraient être tentées d'escroquer des investisseurs peu méfiants. Cependant, pour que ces sanctions aient un pouvoir dissuasif, il ne suffit pas que les tribunaux rendent des ordonnances. Il faut pouvoir faire appliquer les sanctions, sinon, ce ne sont que des mots.

Les contrevenants peuvent tirer parti de nombreux obstacles pour entraver nos efforts de recouvrement. L'un d'entre eux est une loi fédérale, la Loi sur la faillite et l'insolvabilité, ou la LFI. La LFI est conçue pour permettre le retour à la stabilité financière de débiteurs honnêtes, mais en situation difficile, et leur offrir un nouveau départ en les libérant de leur dette à l'issue d'une réhabilitation d'un failli. La LFI le fait très bien, et les organismes de réglementation canadiens des valeurs mobilières soutiennent sans réserve cet objectif.

Cependant, la LFI traite les sanctions imposées par les organismes de réglementation des valeurs mobilières pour faute grave de la même manière que les dettes des consommateurs. Cela signifie que les personnes qui étaient sanctionnées pour des infractions graves aux règles du marché peuvent voir leurs sanctions effacées dans le cadre de la procédure de faillite. Ce sont des personnes dont les dettes découlent de leur propre comportement prédateur envers d'autres Canadiens et qui cherchent à ne pas s'acquitter de ces dettes. Quand elles font cela, cela mine les efforts des organismes de réglementation canadiens des valeurs mobilières d'appliquer la loi et de protéger les investisseurs contre les fraudes.

Pour donner un exemple en Alberta, Saileshwar Narayan a admis avoir commis une fraude dans le cadre de montages financiers hypothécaires qui ont entraîné des pertes pour les investisseurs s'élevant à 4 millions de dollars. Un mois après que l'Alberta Securities Commission, l'ASC, lui a imposé une sanction administrative de 300 000 \$, il a déclaré faillite et a été libéré d'une faillite 10 ans plus tard. La sanction a été effacée, et l'ASC n'a recouvré que 6 300 \$ de la dette de Narayan.

Nous estimons que des exemples comme celui-ci minent la confiance envers la capacité du régime de réglementation canadien de tenir les fraudeurs responsables de leurs actions. Cela mine les principes d'honnêteté et d'équité que nous attendons tous des marchés canadiens. Nous estimons également qu'ils vont à l'encontre de la lutte louable menée par le gouvernement fédéral contre la criminalité financière. Il existe, toutefois, une solution.

La LFI prévoit une liste de dettes que le Parlement a décidé de ne pas effacer en cas de faillite. Nous, ainsi que tous les autres organismes de réglementation canadiens des valeurs mobilières, demandons que le gouvernement ajoute à cette liste les sanctions financières imposées par les organismes de réglementation canadiens pour les formes les plus graves de pratiques abusives sur le marché, soit les fraudes, la manipulation des marchés et les fausses déclarations.

Nous avons discuté de cette demande avec les fonctionnaires d'Innovation, Sciences et Développement économique Canada, ISDE, et avons présenté des mémoires au comité des finances de la Chambre et au ministère des Finances. Le gouvernement de la Colombie-Britannique et l'ensemble des organismes de réglementation des valeurs mobilières dans tout le Canada appuient cette demande. Elle est également appuyée par un large éventail d'organisations, y compris le groupe de défenseurs des investisseurs FAIR Canada, le Conseil des consommateurs du Canada, les CFA Societies Canada et l'Association canadienne des personnes retraitées.

Le fait d'apporter cette modification à la LFI n'aurait aucun effet sur les débiteurs honnêtes, mais en situation difficile, que la LFI vise à servir, et n'imposerait aucun fardeau supplémentaire aux tribunaux de la faillite qui s'acquittent avec brio de la mission essentielle prévue par la LFI. Elle permettrait d'harmoniser la loi provin-

cial sur les valeurs mobilières et la loi fédérale sur la faillite qui, sur ce point précis, vont à contre-courant l'une de l'autre.

Cela répondrait également à un impératif plus concret. Alors que le Canada s'efforce d'atteindre le plus haut niveau possible de compétitivité et de résilience économiques, nous devons veiller à ce que notre marché soit perçu comme étant honnête et équitable, et donc comme un lieu sûr pour investir. Un élément essentiel de cette démarche réside dans une application rigoureuse et efficace de la loi, afin de tenir les personnes responsables lorsqu'elles portent préjudice à notre marché au moyen de fraude, de manipulation ou de fausse déclaration.

Je vous demande de considérer notre modification proposée à la LFI comme étant un moyen concret de soutenir une application rigoureuse de la loi et de mieux lutter contre les fraudes financières au Canada.

Merci encore de votre temps aujourd'hui. Je répondrai volontiers à vos questions.

• (1105)

Le président: Merci beaucoup.

Je vais vous donner la parole, monsieur Paterson. Vous avez cinq minutes ou moins pour présenter votre déclaration préliminaire, monsieur.

Ian Paterson (président-directeur général, Plurilock Security Inc.): Merci, monsieur le président et membres du Comité, de m'avoir invité.

Je m'appelle Ian L. Paterson. Je suis le PDG de Plurilock, une société canadienne spécialisée dans la cybersécurité. Pendant 10 ans, j'ai créé et breveté des systèmes permettant de vérifier l'identité des personnes, et j'ai fourni des solutions de cybersécurité à des organismes gouvernementaux et à des entreprises. Je suis ici à titre d'exploitant ayant un point de vue pratique sur la raison pour laquelle les fraudes fonctionnent et sur ce qui pourrait baisser leur nombre.

Je formulerai trois recommandations visant à lutter contre les fraudes qui nuisent tous les jours aux Canadiens, mais je vais d'abord vous raconter une histoire.

Un grand-père reçoit un appel. Il entend la voix de son petit-fils, qui lui dit qu'il a été impliqué dans un accident de voiture et qu'il a besoin d'argent tout de suite. Le grand-père se rend en voiture à la banque, retire l'argent et remet un mandat postal à un inconnu qui s'est présenté en personne pour le récupérer. Ce n'est que plus tard, lorsque les membres de la famille en ont discuté, que la vérité a été révélée. Le petit-fils allait bien. La voix était un hypertrucage. Il s'agissait d'une fraude.

C'est une histoire parmi tant d'autres. J'en ai beaucoup, comme la plupart des Canadiens, je pense.

Les Canadiens ont signalé au centre antifraude 704 millions de dollars de pertes en 2025, qui a été la pire année jamais enregistrée. La Gendarmerie royale du Canada, la GRC, estime que seulement 5 à 10 % des fraudes sont signalées, ce qui signifie que le coût réel pour l'économie canadienne se chiffre en milliards.

Que fait-on? En cybersécurité, on parle de prévention « en amont de l'incident » et d'intervention « en aval de l'incident ».

Premièrement, en ce qui concerne les mesures prises en amont de l'incident, la prévention, c'est avant tout une question d'identité.

Les fraudes fonctionnent parce que l'on continue de vérifier l'identité des personnes à l'aide d'éléments faciles à falsifier: les numéros de téléphone, les messages texte, les mots de passe et, aujourd'hui, les voix. En 2019, j'ai écrit dans le *Globe and Mail* que mon fournisseur de jeu vidéo avait une meilleure sécurité que ma banque. Sept ans plus tard, il n'y a pas eu beaucoup de changements, et les hypertrucages et le clonage des voix permettent aux malfaiteurs d'automatiser et de multiplier leurs attaques.

La solution réside dans un système d'identification plus sûr, auquel les simples citoyens canadiens puissent faire confiance. Lorsque votre compagnie de télécommunications, votre banque ou votre gouvernement vous contacte, cela doit se faire par un canal qui ne puisse pas être facilement piraté comme une notification pistée d'une application de téléphone intelligent. Lorsqu'on se connecte à un service, on devrait utiliser des identifiants difficiles à hameçonner, comme des clés d'accès, que personne ne pourrait communiquer à un criminel. Lorsqu'il s'agit d'un contact entre deux personnes, la solution est la résilience. Les criminels peuvent usurper un numéro de téléphone et imiter une voix familière, il faut donc raccrocher et rappeler un numéro que vous connaissez et poser des questions sur un contexte commun comme « Qu'est-ce que tante Bertha a apporté au repas de Noël de l'année dernière? »

Les petites habitudes l'emportent sur les technologies coûteuses. Ce grand-père dans l'histoire n'était pas imprudent. Il a fait tout ce que nous tous avons appris à faire, soit faire confiance à la personne au bout du fil. C'est cela qui doit changer, et nous pouvons y remédier.

Le gouvernement devrait montrer l'exemple. Tous les Canadiens connaissent les faux appels de l'Agence du revenu du Canada, l'ARC. Si l'ARC et les organismes similaires utilisaient des canaux difficiles à pirater, ils mettraient fin à l'une des escroqueries les plus courantes dans le pays et établiraient la norme pour tout le monde.

Deuxièmement, en ce qui concerne les mesures prises en aval de l'incident, tout est une question de coordination.

Quand la victime, la banque, la compagnie de téléphone et le criminel se trouvent dans des administrations différentes, la première question est de toujours savoir à qui appartient le dossier. Nos agents de police comptent parmi les personnes les plus dévouées à leur mission que je connaisse, mais trop souvent, le service de police local chargé du dossier ne dispose ni de la formation, ni des outils, ni du mandat nécessaire pour lutter contre ce type de criminalité, et ce détachement de police doit alors choisir entre une escroquerie de 5 000 \$ et un vol à main armée un peu plus loin dans la rue. Les criminels comptent sur cette faiblesse et l'exploitent.

Nous avons un bon point de départ avec le Centre national de coordination en cybercriminalité, mais il joue un rôle de soutien. L'enquête incombe toujours aux agents de police. Le Canada a besoin d'une intervention nationale qui dirige ces dossiers et qui ne se contente pas de les soutenir: une intervention qui dépasse les frontières des territoires et rassemble autour d'une même table les banques et les compagnies de télécommunications, en intégrant la protection de la vie privée et en ayant pour mandat de poursuivre ces crimes, quel que soit le montant en jeu.

Troisièmement, le Canada ne peut pas s'attaquer à ces problèmes à lui seul. Certaines des opérations les plus importantes ont leur origine à l'étranger. Dans la région indo-pacifique, des réseaux d'escroqueries exercent leurs activités à une échelle industrielle, souvent composés par des travailleurs victimes de trafic humain qui

prennent pour cible des Canadiens. Nous devons investir davantage dans l'aide internationale afin de contribuer à démanteler ces réseaux à la source, avant qu'ils n'atteignent les Canadiens.

La fraude est un problème d'identité, de coordination et un test de notre résilience. Tous les jours, des Canadiens sont victimes de vols électroniques perpétrés par des criminels qui en ont fait une véritable industrie, une industrie qui tire profit des failles de notre système. C'est à nous de combler ces failles.

Merci. Je serai heureux de répondre à vos questions.

● (1110)

Le président: Merci, monsieur Paterson.

Monsieur Pinto, je vous donne maintenant la parole, monsieur, pour cinq minutes ou moins.

Jude Pinto (chef de la livraison, Paiements Canada): Merci, monsieur le président, et merci à tous de m'avoir invité à prendre la parole aujourd'hui.

En tant que chef de la mise en œuvre de Paiements Canada, je dirige un programme de mise en œuvre à grande échelle, y compris la voie de paiement en temps réel et ses services centraux de lutte contre la fraude. J'ai plus de 35 ans d'expérience dans la transformation des technologies et des opérations financières.

Paiements Canada possède et exploite l'infrastructure nationale essentielle de paiement du Canada, à savoir les systèmes, les règles et les normes qui aident l'économie canadienne à fonctionner. Créée en vertu de la Loi canadienne sur les paiements, notre organisation nationale d'intérêt public ne poursuit pas de but lucratif. Notre conseil d'administration est majoritairement indépendant, et le ministre des Finances est responsable de notre loi habilitante.

Nos systèmes, qui sont supervisés par la Banque du Canada, comprennent Lynx, le système de paiement canadien de grande valeur, utilisé par les participants pour traiter et régler principalement des virements électroniques et des paiements de montant élevé; le Système automatisé de compensation et de règlement, le SACR, qui assure le traitement et le règlement de détail par lots, tels que les virements et les prélèvements automatiques, et le système canadien de paiement en temps réel, dont je parlerai dans un instant.

En 2025, notre système de sécurité a permis le traitement et le règlement de 103 billions de dollars entre les institutions. Notre vision est de favoriser la prospérité, la productivité et la sécurité au Canada grâce à des systèmes de paiement fiables et de calibre mondial. Les objectifs de notre politique publique, adoptée par voie législative, sont de promouvoir l'efficacité, la sécurité et la fiabilité de nos systèmes.

Notre point de vue sur les fraudes nécessite des précisions au sujet du rôle unique que nous jouons. Les systèmes, les règles et les normes de Paiements Canada permettent aux participants à notre système, y compris les institutions financières, les fournisseurs de services de paiement et les coopératives de crédit, de transférer des fonds en toute sécurité entre eux. Nous ne détenons aucun compte bancaire individuel de nos clients, n'y avons pas accès et ne les gérons d'aucune façon; nous n'avons pas non plus accès à des données privées. Cependant, à mesure que les menaces de fraude évoluent, nous avons tous un rôle à jouer.

Nos propres recherches confirment le rythme auquel les menaces de fraude se multiplient. Ces menaces ne sont pas réparties de manière uniforme au sein de la population canadienne, et touchent souvent les personnes les plus vulnérables du pays.

Les fraudes se manifestent par de multiples canaux, secteurs et acteurs. Il n'existe pas de solution unique ni d'institution capable d'y remédier à elle seule. C'est pourquoi Paiements Canada soutient fermement la création par le gouvernement d'une agence de lutte contre les crimes financiers et son engagement à élaborer une stratégie nationale de lutte contre la fraude.

Notre mémoire de consultation concernant cette stratégie met l'accent sur la nécessité d'un échange de données axées sur des objectifs dans tous les secteurs; d'une réglementation et d'une surveillance coordonnées afin de garantir des résultats équitables et prévisibles dans toutes les industries; et d'une sensibilisation renforcée et collaborative des consommateurs.

Paiements Canada est également un membre actif de la Coalition canadienne antifraude.

Notre plus grande contribution à la lutte contre la fraude, et à l'innovation en matière d'infrastructure de paiement au Canada, est le système de paiement en temps réel du Canada, qui sera lancé au quatrième trimestre de cette année avec des services centralisés de lutte contre la fraude. Associé à un accès plus large à nos membres et aux systèmes, le système de paiement en temps réel favorisera la concurrence, l'innovation, la croissance économique et l'inclusion financière en permettant des paiements instantanés et irrévocables, disponibles 24 heures sur 24, sept jours sur sept et une norme de messagerie ISO 20022 riche en données.

Nous avons tiré profit des leçons tirées et d'une collaboration étroite avec d'autres administrations qui ont constaté que, même si de nouveaux risques apparaissent, les transactions en temps réel peuvent être sécurisées.

Aucun type de paiement n'est à l'abri de la fraude. C'est pourquoi le Canada sera le premier à lancer son système national de paiement en temps réel doté de mesures de prévention de la fraude obligatoires dès le premier jour.

Les quatre exigences sont les suivantes: premièrement, une évaluation en temps réel des transactions frauduleuses, s'appuyant sur des informations au niveau du réseau, afin d'étayer la gestion des fraudes et des prises de décisions en matière de paiement; deuxièmement, une plateforme de renseignement centralisée permettant la production de rapports nationaux et fournissant des informations agrégées sur la fraude; troisièmement, une liste des risques commune et gérée de manière centralisée, permettant de suivre et de signaler les caractéristiques des personnes impliquées dans des cas de fraude avérés; et, quatrièmement, une confirmation de la capacité du bénéficiaire, permettant aux particuliers de vérifier l'identité du compte du destinataire.

L'adoption par le système de paiement en temps réel de la norme de messagerie ISO 20022 ouvrira la voie à de nouvelles analyses plus puissantes, en permettant aux participants de mieux suivre et de perturber les schémas de fraude complexes. De plus, le système de paiement en temps réel est conçu pour faciliter le respect des exigences en matière de lutte contre le blanchiment d'argent pour les indicateurs transfrontaliers.

La modernisation de l'infrastructure de paiement du Canada est un projet qui contribue à l'édification de la nation. Paiements

Canada s'engage pleinement à soutenir les efforts collaboratifs visant à protéger les Canadiens en cette période charnière pour le secteur des paiements.

Merci, et je répondrai volontiers à vos questions.

● (1115)

Le président: Merci beaucoup, monsieur Pinto.

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

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

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

Merci à tous les témoins de leur témoignage sur ce dossier.

Monsieur Pinto, je voudrais commencer par vous poser quelques questions. Votre organisation, Paiements Canada, traite principalement les transactions entre institutions.

Jude Pinto: C'est exact.

Ted Falk: À quelle étape de la transaction constate-t-on généralement des cas de fraude?

Jude Pinto: Voilà une excellente question.

Si une transaction se répartit entre l'échange de valeurs entre consommateurs et entreprises, nous n'intervenons généralement pas. Historiquement, le règlement entre l'émetteur et l'établissement ou la banque destinataire est la partie que nous traitons au moyen de comptes de règlement de la Banque du Canada. Cette combinaison d'échange, de compensation et de règlement par l'intermédiaire des comptes de la Banque du Canada avec le système de paiement en temps réel est en réalité intégrée; ces trois étapes s'enchaînent en une fraction de seconde.

C'est pourquoi il était important... En ce qui concerne le système de paiement en temps réel, le PTR, c'est la première fois que nous avons un aperçu de l'origine de certaines fraudes. Les discussions auxquelles nous avons assisté jusqu'à présent portaient généralement sur le niveau de l'échange.

Ted Falk: Vous êtes très enthousiaste à l'idée de voir le lancement du système de paiement en temps réel prévu plus tard cette année, et vous pensez que cela vous aidera à réduire au minimum les escroqueries et les fraudes et à les signaler en temps réel.

Jude Pinto: Oui.

Ted Falk: Y a-t-il des mesures qui pourraient être prises d'ici là pour limiter une partie des fraudes qui ont actuellement lieu au sein du système?

● (1120)

Jude Pinto: La réponse globale est oui. Dans le cadre de Paiements Canada, nous exploitons actuellement Lynx et le système automatisé de compensation et de règlement, et il ne nous reste plus qu'un trimestre avant de lancer notre première initiative dans le domaine de la lutte contre la fraude et de la sécurité des paiements. Cela relève peut-être davantage de la compétence des banques et des institutions qui participent actuellement à l'échange des transactions, plutôt que de celle de Paiements Canada, qui s'occupe du règlement.

Ted Falk: Participez-vous à tous les règlements au Canada?

Jude Pinto: Oui.

Ted Falk: Votre organisation participe...

Jude Pinto: En monnaie fiduciaire...?

Ted Falk: Oui.

Jude Pinto: Oui.

Ted Falk: Merci d'avoir précisé ce point.

Monsieur Paterson, j'aimerais également vous poser quelques questions.

Dans votre histoire du grand-père escroqué... Lors d'une précédente réunion du Comité, un représentant de Meta avait comparu ici. L'une des questions que nous avons posées au représentant de Meta portait sur le niveau de responsabilisation de Meta en tant que plateforme qui fournit le canal ou le moyen par lequel l'escroquerie est commise. Selon vous, quel degré de responsabilité les intermédiaires devraient-ils assumer?

Ian Paterson: Quand on parle de prévention de la fraude, il s'agit en réalité d'un exercice de résilience à l'échelle de la société que nous devons mener à bien. Bien sûr, les plateformes technologiques — que ce soit les plateformes des médias sociaux, les banques, les compagnies de télécommunications, etc. — peuvent toutes jouer un rôle. Je ne pense pas qu'il y ait une plateforme ou un fournisseur en particulier qui me semble poser davantage de problèmes que les autres.

Le problème, dans son ensemble, réside dans le fait qu'il existe certaines habitudes, coutumes et pratiques que nous avons adoptées, dans l'ensemble de la société, que ce soit de manière implicite ou explicite. Ce sont des choses comme le fait de se connecter à l'aide d'un mot de passe, de croire qu'un appel téléphonique que l'on reçoit provient d'une personne autorisée et de penser que la voix que l'on entend est bien celle de cette personne. Ce sont en fait les causes profondes de la façon dont certaines de ces fraudes sont commises. Selon moi, ce sont les éléments sur lesquels nous devons nous pencher.

Ted Falk: Selon certaines des informations que nous avons reçues ici au Comité, deux tiers des escroqueries sont commises sur les plateformes de Meta. Ne pensez-vous pas que Meta a une responsabilité à cet égard?

Ian Paterson: Toutes les plateformes de technologie ont une responsabilité, mais j'ajouterais que les courriels et les messages texte sont également à l'origine d'une grande partie des escroqueries. La réalité, du moins d'après ce que j'ai pu constater au cours de ma carrière ces dix dernières années, c'est que les malfaiteurs s'adaptent à tout ce qui est utilisé. Si Meta est la plateforme la plus populaire, c'est certainement là où ils iront. Si WhatsApp devient la plateforme de communication la plus utilisée, je suis convaincu que ce sera la première plateforme qu'ils utiliseront.

Je ne pense pas que ce soit la responsabilité d'une seule entreprise. Je crois sincèrement que nous pouvons tous jouer un rôle de chef de file pour renforcer la résilience dans l'ensemble de la société.

Ted Falk: Selon vous, quel rôle Plurilock jouerait-il dans la lutte contre les escroqueries et les fraudes?

Ian Paterson: Plurilock est principalement une compagnie inter-entreprises. Généralement, nous ne travaillons pas directement avec les clients, même si, compte tenu de notre rôle de chef de file dans le domaine de la cybersécurité, je suis souvent la personne que les gens appellent lorsqu'ils rencontrent un problème. L'histoire que je vous ai racontée à propos du grand-père concernait une personne de

mon entourage qui m'avait contacté pour me demander simplement de l'aide.

En ce qui concerne l'accompagnement des organisations dans le renforcement de leur cyberrésilience, c'est effectivement l'une de nos activités. Je tiens à préciser que, historiquement, mon organisation était beaucoup plus présente aux États-Unis. Je suis ici principalement en tant que citoyen canadien qui fait part de ses expériences afin de faire du Canada un pays plus sûr et plus prospère.

Ted Falk: Merci.

Enfin, madame Corrigan-Brown, pensez-vous que nous ayons actuellement les ressources suffisantes pour poursuivre les personnes accusées de crime ou d'infractions de fraude?

Le président: Madame Corrigan-Brown, veuillez, s'il vous plaît, répondre en 30 secondes.

Merci.

Sarah Corrigan-Brown: Certainement, nous, le gouvernement fédéral et les sociétés d'État, travaillons avec ce que nous avons. Il y a toujours — comme nous l'avons tous relevé — l'ampleur du problème et le nombre de Canadiens touchés.

Nous nous réjouissons vivement de l'attention que porte le gouvernement fédéral à ce domaine et de la possibilité qui nous est offerte de collaborer avec les organismes de réglementation des valeurs mobilières. Je suis d'accord avec ce que mes collègues ont dit. Il doit y avoir une intervention nationale, faisant intervenir l'ensemble de la société. Il est important et nécessaire de consacrer des ressources et de l'attention à cette question.

Le président: Merci, monsieur Falk.

Monsieur Bains, vous êtes en ligne aujourd'hui. Vous avez la parole pour six minutes, monsieur.

● (1125)

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

Merci aux témoins de se joindre à nous pour cette étude importante.

Monsieur Paterson, vous nous avez raconté une histoire, mais j'en ai entendu bien d'autres de la part de mes électeurs et de membres de ma famille. Nous-mêmes recevons ces appels et ces messages texte. Le problème que nous rencontrons aujourd'hui est assez complexe. Il s'agit d'un enjeu mondial. En fin de compte, nous faisons face à des problèmes liés à l'extorsion. Nous essayons de cerner toutes les différentes formes d'attaque dont les gens sont victimes.

Je me demandais si vous pouviez très rapidement nous expliquer en quoi les cybermenaces auxquelles sont exposés les différentes organisations et les gouvernements diffèrent-ils entre le Canada et les États-Unis. Y a-t-il une vulnérabilité spécifique que vous pourriez mettre de l'avant? Quelles sont les cibles que les fraudeurs exploitent plus couramment? Il peut s'agir des systèmes dont dispose chaque gouvernement ou des règlements qu'ils appliquent pour superviser certaines de ces plateformes, telles que Meta et WhatsApp.

Pouvez-vous nous dire quelque chose à cet égard?

Ian Paterson: Merci de la question.

Je pourrais parler de la [difficultés techniques] résilience et également des vulnérabilités.

Je pense que l'une des choses qui ne surprendront personne ici, c'est que l'IA a véritablement rendu les escroqueries [*difficultés techniques*] pour écrire dans un anglais parfait, tandis que, autrefois, l'un des moyens les plus courants de savoir si un courriel était authentique ou frauduleux [*difficultés techniques*].

Le président: Monsieur Paterson, je ne sais pas si le problème vient de notre côté ou du vôtre, mais malheureusement, la connexion est un peu saccadée. Je vais laisser passer une dernière fois. Si la connexion se coupe, cela rendra la tâche un peu trop difficile pour les interprètes. Je devrai peut-être revenir à vous... si nous parvenons à rétablir cette connexion.

Je regarde en ce moment même, et votre image semble figée.

Monsieur Bains, je vais vous demander de poser de nouveau cette question. Je vous redonnerai du temps de parole.

Monsieur Paterson, si vous pouvez m'entendre, nous allons devoir réessayer dans quelques minutes.

Monsieur Bains, vous avez toujours la parole.

Parm Bains: Je vais passer à Mme Corrigan-Brown.

Une grande partie de votre travail et de votre défense de la réforme des lois sur la faillite vise à empêcher les malfaiteurs d'abuser des lois et de dissimuler les gains issus de leurs fraudes derrière des mesures de protection offertes par la procédure de faillite. Comment peut-on améliorer la situation?

Sarah Corrigan-Brown: Merci beaucoup de la question.

L'organisme de réglementation des valeurs mobilières accorde une attention particulière à cet aspect. Nous intervenons également à tous les niveaux en matière de prévention, de détection, de lutte contre ces pratiques et d'application de la loi. Nous constatons toutefois que ce problème persiste depuis des années. Nous avons pris des mesures pour détecter, mener des enquêtes et organiser des audiences, et nous avons demandé des comptes aux responsables en leur imposant des sanctions. Ils n'ont ensuite fait aucun effort pour payer leurs amendes et ont eu recours à notre régime de faillite afin d'éviter de payer leur dette dans le cadre de la procédure de faillite, évitant ainsi de payer ces amendes et d'assumer toutes les conséquences de leurs actes.

Certaines dettes survivent à la faillite. Une personne peut être libérée de ses dettes à l'issue d'une procédure de faillite, mais elle reste tenue de s'acquitter de certaines dettes. Nous demandons que les dettes imposées par les organismes de réglementation des valeurs mobilières pour les cas de fautes les plus graves — fraude, manipulation du marché et fausse déclaration — soient ajoutées à la Loi sur la faillite et l'insolvabilité, que l'on modifie la loi pour que ces dettes survivent à la faillite. Nous pourrions continuer de recouvrer ces créances tant que cette personne continue à les contracter, et le reste des dettes pourrait être effacé. Nous pensons que cette mesure est indispensable.

Nous reconnaissons l'importance capitale et la nécessité de combattre la fraude avant qu'elle ne soit commise. C'est la meilleure façon de s'assurer que les investisseurs ne perdent pas leur argent, de maintenir leur confiance envers leur participation à notre économie et de protéger les Canadiens. Il est essentiel de lutter contre la fraude dès son apparition, mais le système doit également s'appuyer sur des mécanismes d'application de la loi solides et efficaces. Nous devons montrer que nous sommes capables de gérer et de réglementer notre économie, ainsi que de protéger les Canadiens. Selon

nous, le fait de disposer de mesures d'application solides et de modifier la Loi sur la faillite et l'insolvabilité, pour que les personnes qui commettent ce genre d'actes répréhensibles ne puissent pas déclarer faillite et, par conséquent, éviter d'assumer toutes les conséquences de leurs actes, est un élément essentiel pour combler une lacune à la dernière étape. Si nous avons tenu quelqu'un responsable de ses actes, nous estimons qu'il devrait continuer à être tenu de payer ces amendes.

• (1130)

Parm Bains: Il arrive assez souvent que l'on voie des gens déménager. S'ils commettent une fraude, ils déménagent dans une autre administration. D'abord, pourriez-vous nous dire si les provinces et les territoires sont sur la même longueur d'onde à ce sujet au Canada, et pourriez-vous ensuite citer d'autres administrations avec lesquelles vous collaborez étroitement pour vous attaquer à ce problème, et nous dire s'il existe des administrations qui pourraient nous servir de modèle à titre de comparaison?

Le président: Vous avez environ 45 secondes pour répondre, madame Corrigan-Brown.

Sarah Corrigan-Brown: Tous les organismes canadiens de réglementation des valeurs mobilières, provinciaux et territoriaux, appuient cette demande. C'est un problème qui se pose dans l'ensemble du pays, et nous soutenons tous cette demande. Les organismes de réglementation provinciaux des valeurs mobilières travaillent en très étroite collaboration entre eux afin d'avoir un régime harmonisé de réglementation des valeurs mobilières qui protège les investisseurs et garantit l'équité et l'intégrité de nos marchés.

Les marchés sont mondiaux, et la fraude l'est aussi; nous travaillons donc également en très étroite collaboration avec des homologues en Europe, en Asie et aux États-Unis. Le régime américain en matière de faillite mérite d'être cité. Les sanctions imposées par les organismes de réglementation des valeurs mobilières ne disparaissent pas en cas de faillite. C'est une décision stratégique que les États-Unis ont prise, et c'est ce que nous recommandons de reproduire ici.

Le président: Merci beaucoup, monsieur Bains.

[Français]

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

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

Madame et messieurs les témoins, je vous remercie de votre présence et de vos témoignages. C'est très riche en contenu, tout ce que vous nous apportez.

Madame Corrigan-Brown, je reviens sur votre demande et les échanges que vous venez d'avoir. Est-ce que le gouvernement fédéral semble ouvert à apporter à la Loi sur la faillite et l'insolvabilité la modification que vous demandez?

[Traduction]

Sarah Corrigan-Brown: L'année dernière, nous avons eu des discussions fructueuses avec les fonctionnaires d'ISDE, et nous avons rencontré les fonctionnaires du ministère des Finances ainsi que du ministère de l'Industrie. Nous avons également rencontré des représentants de votre Comité, et nous avons été invités à comparaître devant le Comité. Je dirais que le gouvernement fédéral s'est montré très ouvert à la discussion, à l'écoute de notre demande et désireux de mieux comprendre le défi que cela représente pour les organismes de réglementation des valeurs mobilières.

[Français]

Gabriel Ste-Marie: D'accord, c'est bien. On va continuer à lui rappeler que cette demande est très importante.

Sur un autre sujet, j'aborde la question des cryptomonnaies. Est-ce que vous considérez que la cryptomonnaie est une forme de monnaie ou plutôt une valeur mobilière qui relève de vous?

[Traduction]

Sarah Corrigan-Brown: C'est une excellente question. Nous considérons que la cryptomonnaie en elle-même, quand elle est utilisée comme moyen de paiement, est une monnaie. Nous ne réglementons pas la cryptomonnaie elle-même en tant que valeur mobilière.

[Français]

Gabriel Ste-Marie: D'accord.

Dans ce cas, est-ce que les plateformes d'échange de cryptomonnaie sont considérées comme des intermédiaires financiers qui ne relèvent pas de vous?

[Traduction]

Sarah Corrigan-Brown: Nous réglementons les plateformes d'échange de cryptomonnaies, si ces plateformes de négociation s'inscrivent dans le cadre de ce que nous appelons des « contrats sur cryptomonnaies ». Il s'agit essentiellement de contrats dont la valeur est établie en cryptomonnaie sous-jacente. Le contrat sur cryptomonnaie est un instrument dérivé. Nous réglementons la négociation de ces contrats sur cryptomonnaies. Ces plateformes d'échange de cryptomonnaies sont soumises à notre réglementation.

[Français]

Gabriel Ste-Marie: D'accord. Très bien. Merci.

Dans la lutte à la fraude, quand il est question des cryptomonnaies, le rôle du fédéral est-il d'intervenir pour vous réglementer ou bien, avec toutes les commissions de sécurité des valeurs mobilières entre elles, et les mécanismes d'échange et de bonne collaboration auxquelles vous faisiez référence, avez-vous tout ce qu'il faut pour suivre les échanges de cryptomonnaies?

[Traduction]

Sarah Corrigan-Brown: Dans le domaine des cryptomonnaies, tout comme sur les marchés financiers et en matière de fraude, nous estimons qu'il est nécessaire que le gouvernement fédéral et les organismes provinciaux de réglementation des valeurs mobilières travaillent en collaboration. Quand la cryptomonnaie elle-même est utilisée comme moyen de paiement, par exemple cela relève de la compétence fédérale, et il existe des organismes fédéraux qui réglementent ce domaine. Les règlements et les mesures de protection qu'ils offrent aux Canadiens sont essentiels; toutefois, les cryptomonnaies peuvent également être utilisées sur les marchés d'investissement et à des fins d'investissement, ce que nous réglementons.

Nous disposons de différents mécanismes de protection et pouvoirs pour faire face aux risques que cela crée pour les Canadiens.

Il est vraiment essentiel de travailler en collaboration, sinon, il y aura des lacunes. Encore une fois, c'est là que le fait que le gouvernement fédéral se concentre sur cette question et adopte une approche aussi globale de la lutte contre la fraude et de l'utilisation des cryptomonnaies non seulement à des fins légitimes, mais aussi à des fins frauduleuses... il faut en prendre conscience et travailler ensemble aux paliers provincial et fédéral.

● (1135)

[Français]

Gabriel Ste-Marie: Je vous remercie beaucoup.

Monsieur Pinto, de Paiements Canada, ma première question concerne la plateforme centralisée dont vous avez parlé. Au sujet des différents intermédiaires, comme les banques et autres acteurs, est-ce une participation obligatoire ou volontaire?

[Traduction]

Jude Pinto: Pour tous nos participants qui utilisent le système de paiement en temps réel ou une plateforme d'échange tierce dont le règlement s'effectue par l'entremise du système de compensation et de règlement du système de PTR, la participation est obligatoire. Il y a les quatre services que j'ai décrits. Le score de risque au niveau du réseau leur sera transmis. Ils y ont accès. Il doit être intégré à leur processus de décision visant à déterminer s'il convient de procéder au paiement. Nos règles prévoient l'exigence de signaler les fraudes, notamment les fraudes de compte à compte, en utilisant une taxonomie nationale commune. La spécification impose l'obligation de contribuer à la liste des risques. Il est également obligatoire d'utiliser la confirmation du bénéficiaire pour identifier un compte valide.

Cela comprend tous les nouveaux participants qui font directement partie du système de PTR ainsi que la plateforme d'échange tierce, qui est le virement électronique d'Interac. Ils sont tous obligatoires.

[Français]

Gabriel Ste-Marie: D'accord. Merci beaucoup.

Pouvez-vous nous donner plus de détails sur le fonctionnement du système de pointage, d'évaluation des transactions frauduleuses, entre autres? Si c'est trop complexe, vous pourrez nous faire parvenir une réponse écrite. Je voudrais cependant que vous nous donniez un aperçu en 30 secondes.

[Traduction]

Jude Pinto: Le son s'est coupé pendant un petit moment. Pouvez-vous répéter la première partie de la question?

[Français]

Gabriel Ste-Marie: Oui.

Pouvez-vous nous donner plus de détails sur le fonctionnement du système de pointage d'évaluation des transactions frauduleuses?

[Traduction]

Jude Pinto: Nous travaillons en collaboration avec nos membres sur les types d'indicateurs dont ils ont besoin dans un score afin de les réintégrer dans leur système. Ce sont eux qui contribuent à définir les exigences. Nous traitons ces données à l'aide d'algorithmes qui génèrent ensuite, effectivement, un signal d'avertissement indiquant qu'il vaut peut-être mieux ne pas poursuivre l'opération, un feu jaune invitant à approfondir la vérification, ou un feu vert leur permettant de prendre une décision. Ces types de scores sont intégrés dans les contrôles antifraude mis en place par nos participants lors du lancement des opérations de paiement.

Avant qu'ils n'envoient un paiement par l'entremise du système de paiement en temps réel, ils disposent de l'ensemble de leur système interne. Disons que vous êtes une banque ou une entreprise de technologie financière. Ils analyseraient ces données et prendraient une décision, à l'aide d'algorithmes, afin de déterminer s'il convient ou non de procéder au paiement. Cela leur permet de bloquer le paiement et de mener une enquête plus approfondie, ou de le refuser s'il a été identifié comme étant frauduleux.

[Français]

Gabriel Ste-Marie: Merci beaucoup.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Madame Borelli, vous avez la parole pour cinq minutes.

Kathy Borrelli (Windsor—Tecumseh—Lakeshore, PCC): Ma question s'adresse à M. Pinto.

De nombreuses victimes de fraude, y compris les personnes âgées et les petites entreprises, sont manipulées pour qu'elles fassent des virements massifs de fonds, mais les systèmes de paiement gèrent la transaction comme définitive.

Quelles sont les options disponibles pour interrompre ou récupérer plus facilement les paiements à haut risque, par exemple, les suspensions temporaires, les mécanismes de rappel, le règlement différé pour les virements suspects, etc.?

Jude Pinto: C'est une excellente question, et on confond souvent ce qui est récupérable et ce qui est irrévocable. Nos règles ont essentiellement été définies pour permettre à des fonds visés par certaines catégories de paiements à haut risque ou de fraudes connexes, etc., d'être restitués. Nous fixons des règles qui prévoient des mécanismes par lesquels l'organisme émetteur et l'organisme destinataire conviendront, sous réserve de certains mécanismes, de procéder effectivement au remboursement des fonds.

L'irrévocabilité concerne le moment où cette règle ne s'applique pas. Si cette règle n'indique pas la nécessité d'un remboursement, alors elle est irrévocable, et même lorsque l'argent doit être restitué, c'est la deuxième transaction qui est annulée. C'est ainsi qu'il faut voir les choses.

En ce qui concerne les blocages, nous revenons à la discussion que nous venons d'avoir au sujet des indicateurs de fraude et du pointage. Avant une transaction dans le cadre du système de paiement en temps réel, une opération de paiement véritable est lancée en moins d'une seconde; le contrôle antifraude, l...a vérification par rapport à la liste des risques et l'intégration du score seraient alors intégrés à l'algorithme des participants, qui peuvent alors décider de bloquer la transaction et d'enquêter, ou de déterminer la marche à suivre, au cas par cas.

• (1140)

Kathy Borrelli: À votre avis, le gouvernement fédéral devrait-il définir une attente claire en matière de politiques selon laquelle la modernisation des paiements doit comprendre non seulement des paiements accélérés, mais une réponse à la fraude plus rapide?

Jude Pinto: C'est une bonne question. Je vous remercie de la poser.

Dans la mesure où nous en sommes venus à concevoir et à lancer le système de PTR, cela a toujours été l'attente. Nos membres, nos futurs membres grâce à l'arrivée de nouveaux participants dans le cadre d'une expansion plus large, ainsi que nos orientations réglementaires ont tous exigé que nous rendions cette mesure obligatoire, tant par nos règles que par une offre initiale sur le marché lancée simultanément avec le système.

Kathy Borrelli: Faut-il mettre en place un organisme central où des secteurs comme les services policiers pourraient collaborer en ayant accès aux données nécessaires pour poursuivre les fraudeurs?

Jude Pinto: Je pense que c'est une question très pertinente.

L'organisme central... distinguons-le de la nécessité de collaborer. Quant à la nécessité de collaborer... absolument. Pour l'application de la loi et les poursuites, dans les différents canaux dont nous avons parlé — les médias sociaux peuvent détenir des données, les services de télécommunications, les banques, etc. — il doit exister un mécanisme permettant de collaborer et d'échanger des données, au besoin, pour lutter contre la criminalité financière. Avec la Stratégie nationale antifraude et l'Agence contre les crimes financiers, nous nous attendons à être largement engagés dans ce type de discussions dans le cadre de ces initiatives.

L'idée d'un organisme central regroupant les données provenant de toutes ces sources n'a pas occupé une place importante dans les discussions. Il a plutôt été question de mécanismes officiels permettant d'échanger les données de manière collaborative et d'élaborer des cadres d'échange de données entre tous les acteurs liés à la prévention, à la détection et à la poursuite des fraudes, au sein d'un réseau assez vaste.

Kathy Borrelli: Monsieur Paterson, de nombreux aînés sont ciblés par de faux services de soutien technique ou par des escroqueries par usurpation d'identité bancaire, dans lesquels on convainc la victime d'installer un logiciel d'accès à distance. Une fois cela fait, l'escroc peut parfois guider ou contrôler la transaction.

Quelles mesures techniques pourraient aider à détecter les cas où une personne est guidée ou contrôlée à distance au cours d'une transaction financière?

Ian Paterson: Merci de poser la question.

[Difficultés techniques] est essentiel. Par ailleurs, en ce qui concerne les contrôles techniques précis pouvant être mis en place, il y a d'abord la question de la visibilité: comprendre ce que l'on installe et ce que cela fait, et, franchement, utiliser les technologies existantes comme les pare-feux. Cela ne nécessite aucun coût supplémentaire [Difficultés techniques].

[Français]

Gabriel Ste-Marie: Monsieur le président, j'invoque le Règlement: les interprètes signalent qu'ils ne sont pas capables de faire leur travail.

Le président: Oui, je comprends. Merci.

[Traduction]

Monsieur Paterson, malheureusement, même si nous avons saisi certains éléments de vos propos, votre intervention demeure continuellement saccadée. Je vais devoir poursuivre avec un autre intervenant. Toutefois, je donnerai à Mme Borrelli l'occasion de poser de nouveau ses questions plus tard si nous constatons une amélioration de la connexion. Sinon, elle vous la soumettra par écrit, et vous pourrez transmettre votre réponse au Comité. Nous parvenons à vous entendre suffisamment, mais le problème se trouve du côté de l'interprète. Malheureusement, je ne peux pas me fier avec confiance à l'état de la connexion pour le moment, alors nous tenterons de revenir à vous, monsieur.

Madame Borelli, votre temps était presque écoulé, mais...

• (1145)

Kathy Borrelli: Il me restait environ une minute, je crois.

Le président: Non, ce n'est pas le cas. Vous aviez cinq minutes, et nous les avons dépassées. Je reviendrai vers vous pour vous permettre de poser de nouveau cette question — ou une autre, si vous le souhaitez — en raison des difficultés techniques.

Kathy Borrelli: Que voulez-vous dire par « revenir vers vous »?

Le président: Dans quelques minutes, si la connexion se stabilise, je vous permettrai de prendre 45 secondes ou une minute pour poser de nouveau cette question, ou en poser une autre.

Kathy Borrelli: C'est formidable. Merci.

Le président: Merci.

Monsieur Bardeesy, la parole est à vous pour cinq minutes.

Karim Bardeesy (Taiaiaiko'n—Parkdale—High Park, Lib.): Merci beaucoup.

Madame Corrigan-Brown, vous avez mentionné la relation entre les cryptomonnaies et la question à l'étude aujourd'hui. Le gouvernement du Canada a annoncé son intention de créer un cadre pour les cryptomonnaies stables, et il met sur pied une Agence contre les crimes financiers.

Pouvez-vous vous prononcer à ce sujet? Des conseils écrits par la suite seraient également très utiles. Quelle est la position collective des organismes de réglementation en matière de sécurité quant au fait de conjuguer ces deux éléments en même temps, soit l'introduction d'un cadre pour les cryptomonnaies stables et la création d'une Agence contre les crimes financiers?

Sarah Corrigan-Brown: Je vous remercie de votre question.

Nos directeurs de l'application de la loi et le comité des ACVM chargé de l'application de la loi ont rencontré des représentants au sujet de l'Agence contre les crimes financiers. Ils consultent également le gouvernement fédéral et lui transmettent leurs points de vue dans le cadre de l'élaboration de la Loi sur les cryptomonnaies stables. C'est un enjeu important. Il faudra veiller au respect des compétences respectives et à ce qu'il existe une capacité très claire de communiquer l'information et d'assurer une surveillance coopérative et conjointe des entités, puisque les cryptomonnaies stables sont utilisées par différents participants du marché à des fins diverses. Ces produits et ces entreprises circulent entre les administrations, ce qui exige que nous travaillions ensemble.

Au plus haut niveau, nous collaborons déjà. Nous avons exprimé notre ferme appui et notre conviction que la collaboration et l'échange d'information sont absolument essentiels.

Karim Bardeesy: Très bien.

Le président: Monsieur Bardeesy, je vais arrêter le chronomètre un instant.

Monsieur Paterson, si vous m'entendez, j'essaie de régler le problème. Des membres de l'équipe technique de la Chambre des communes tentent de communiquer avec vous. Si vous voulez prendre un moment pour vérifier votre téléphone ou votre courriel, nous allons essayer de vous faire vous déconnecter puis vous reconnecter. Je vous invite à rester attentif.

Monsieur Bardeesy, il vous reste trois minutes.

Karim Bardeesy: Merci, madame Corrigan-Brown. Nous aimerions recevoir des recommandations écrites à ce sujet, accompagnées de vos réflexions supplémentaires.

Monsieur Pinto, je comprends qu'Interac est le fournisseur de solutions d'échange pour le système de paiement en temps réel. Dans le cadre de ce projet, quelles questions Paiements Canada pose-t-elle à Interac — qui exploite également le réseau Virement Interac, bien connu des Canadiens — concernant certaines des vulnérabilités potentielles pouvant découler du partenariat que vous avez? À votre avis, à quoi faut-il porter une attention particulière?

Jude Pinto: Parlez-vous de vulnérabilités techniques ou de quelque chose de plus large?

Karim Bardeesy: À vous de voir.

Jude Pinto: Paiements Canada est le propriétaire et l'exploitant de l'ensemble de la solution de PRT. Elle se compose de plusieurs éléments. Elle comprend un volet de compensation et de règlement. Elle comprend un tout nouveau système d'échange. Ce système a tiré parti de l'expertise d'Interac en matière de virement Interac au cours des 22 dernières années, en y intégrant une architecture moderne et en faisant d'Interac un fournisseur à cet égard. Le service de Virement Interac sera converti pour utiliser le nouveau moteur de compensation et de règlement qui a été construit.

Ce n'est pas tant une vulnérabilité qu'une occasion qui s'offre à nous. La protection contre la fraude couvre même la solution déjà en place depuis 24 ans, notamment en tirant parti des enseignements du service de Virement Interac et en l'améliorant grâce aux fonctionnalités supplémentaires que nous y ajoutons. Nos règles permettent une vaste gamme de contrôles obligatoires en matière de fraude.

• (1150)

Karim Bardeesy: Je vais simplement reprendre la question de M. Falk plus tôt. Le service de Virement Interac est, malheureusement, l'un des seuls vecteurs par lesquels les médias sociaux... Les médias sociaux, comme vecteur vers le virement Interac, constituent le mécanisme par lequel les fraudes facilitées par les médias sociaux sont exécutées. Posez-vous des questions particulières à Interac dans le cadre de ce projet, compte tenu de cette réalité?

Jude Pinto: Nos participants au PTR, dans les deux cas, sont les banques, les institutions financières, les coopératives de crédit et les prestataires de services de paiement, les PSP. L'interaction avec les médias sociaux se produit à ce niveau-là. Encore une fois, ce sont les participants directs qui se trouvent à l'intersection entre leurs clients, les médias sociaux, les entreprises de télécommunication, etc.

Ce que nous avons mis en place avec Interac, là où nous pouvons intervenir à mesure que les opérations passent par l'échange, la compensation et le règlement, c'est un degré accru de rapports obligatoires en fonction d'une taxonomie commune. Cela permet de dégager des tendances et d'observer des mouvements, et ces informations peuvent ensuite être communiquées aux participants d'Interac et aux nôtres, selon les besoins.

La liste des risques sera utile à tout le monde. Si une institution repère une fraude confirmée, sept autres peuvent empêcher qu'elle se reproduise et s'en servir pour bloquer un paiement. Nous nous situons un peu au milieu ou vers l'aval du processus, mais nous ajoutons des outils qui aideront les participants en amont, là où les fraudes et les arnaques se produisent.

Karim Bardeesy: Merci.

Le président: Merci, monsieur Bardeesy.

[Français]

Monsieur Ste-Marie, vous avez deux minutes et demie.

Gabriel Ste-Marie: Merci, monsieur le président.

Monsieur Pinto, je poursuis avec vous. Est-ce qu'une banque ou une institution financière pourrait décider de ne pas du tout utiliser le système de paiement en temps réel ou est-ce qu'elle n'a aucun droit de ne pas l'utiliser?

[Traduction]

Jude Pinto: C'est une excellente question. Vous parlez de l'utilisation des quatre piliers du contrôle de la fraude.

Il est obligatoire pour les participants de les utiliser, mais une fois qu'ils le font, ce sont leurs politiques internes de gestion des risques qui déterminent leurs seuils individuels pour décider ce qui passe et ce qui échoue. Ils disposent tous d'outils supplémentaires. Par exemple, ils peuvent intégrer quatre différents scores, y compris celui que nous fournissons, qui comporte une efficacité à l'échelle du réseau venant s'ajouter à ce qu'ils utilisent déjà. Pour cette partie, ils choisiront quel score et quel seuil utiliser, parmi l'ensemble des outils, pour décider de laisser passer les paiements ou de les bloquer, et ce, parce qu'ils assument la responsabilité en tant qu'expéditeurs. Ils effectuent les vérifications en amont, et, en général, doivent gérer la fraude qui survient, qu'il s'agisse de leurs propres pertes ou de celles de leurs clients. C'est ce qui explique cette approche.

Les éléments de la solution qui sont obligatoires, en vertu de nos règles, sont la contribution à la liste des risques et la contribution au système national de rapports normalisés.

[Français]

Gabriel Ste-Marie: D'accord. Merci beaucoup.

Je vais m'assurer d'avoir très bien compris. Votre système de paiement en temps réel vise à mettre en place le processus avec les services de lutte contre la fraude dont on a parlé. Il ne vise pas à accélérer davantage les systèmes de paiement qui vont déjà très vite, mais à améliorer la sécurité. C'est ce qui vous fait dire qu'avec ça, le Canada serait parmi les premiers à lancer un système avec ces services de sécurité. Est-ce que c'est bien ça?

[Traduction]

Jude Pinto: C'est une excellente question.

Nous avons constaté que d'autres pays ont lancé leurs systèmes de paiement instantané sans accorder une attention directe aux

types de fraudes nouvelles et différentes pouvant accompagner les paiements en temps réel. Nous avons examiné les solutions qu'ils ont ensuite mises en place, puis nous avons travaillé avec nos membres. Je crois qu'il y avait une vingtaine de mesures possibles à l'échelle nationale. Ils ont finalement retenu ces quatre-là et ont dit: « Assurons-nous qu'elles seront déployées dès le premier jour, comme partie intégrante de la solution. »

Elles sont accessibles à toutes les banques en place qui utilisent le virement Interac, ainsi qu'à tous les nouveaux participants qui utiliseront soit le virement Interac, soit le système direct de PTR. Elles sont accessibles à tous. Que vous ayez 20 ans d'expérience dans le secteur bancaire ou que vous soyez une entreprise de technologie financière existant depuis deux ans, elles sont disponibles pour vous, avec un niveau de protection et de visibilité à l'échelle du réseau.

• (1155)

[Français]

Gabriel Ste-Marie: Merci.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Monsieur Lawton, la parole est à vous pour cinq minutes.

Andrew Lawton (Elgin—St. Thomas—London-Sud, PCC): Merci beaucoup, monsieur le président. Je suis ravi d'être ici pour la première fois devant le Comité.

Je commencerais par vous, monsieur Paterson. Espérons que les problèmes techniques ont été réglés. Une chose que je comprends en matière de protection contre les fraudes et les arnaques, c'est qu'il s'agit vraiment d'un effort à plusieurs niveaux. Il y a les décisions individuelles que les gens peuvent prendre pour se protéger. Puis, à l'échelle des systèmes, il y a également des mesures de protection nécessaires.

Je me demande simplement, compte tenu du travail que vous faites en matière de sécurité, quel avertissement pourrait être donné à l'intention du gouvernement, dans le contexte du projet de loi C-22, la Loi concernant l'accès légal, qui exige en fait l'insertion de portes dérobées dans des systèmes qui sont, à l'heure actuelle, sécurisés... Je pense à la manière dont cela pourrait accroître la vulnérabilité des personnes face à des acteurs malveillants, plutôt qu'à la seule utilisation par les forces de l'ordre de ces mêmes portes dérobées.

Ian Paterson: Je m'excuse pour le problème de connectivité à Internet.

Je suis très préoccupé par les portes dérobées proposées. Depuis des dizaines d'années, nous voyons dans l'industrie des efforts bien intentionnés visant à créer des vulnérabilités à l'intérieur des systèmes, lesquelles sont, inévitablement, exploitées par des acteurs malveillants pour accéder aux données. Nous l'avons vu récemment aux États-Unis, lorsqu'un acteur étatique a réussi à compromettre l'accès légal au système téléphonique américain.

J'orienterais davantage l'attention du gouvernement vers la manière de renforcer les systèmes de façon générale. Il existe assurément des technologies. J'ai mentionné les codes d'accès ainsi que les canaux de communication résistant à l'hameçonnage ou à l'usurpation. Il existe, sans aucun doute, des technologies plus récentes qui peuvent avoir un effet concret sur la réduction de la fraude. À mon avis, c'est par là qu'il faut commencer, plutôt que de chercher à affaiblir les systèmes.

Andrew Lawton: Si j'extrapole à partir de ce que vous dites, ou si j'essaie de formuler vos propos de manière à ce que d'autres puissent en tirer une conclusion, toute vulnérabilité qui pourrait exister pour les « bons » existe aussi pour les « méchants ». Est-ce une description fidèle de ce que vous avancez?

Ian Paterson: C'est tout à fait exact, monsieur.

Andrew Lawton: En ce qui concerne la manière dont nous abordons ces enjeux et d'autres questions connexes, je suis un peu perplexe. Nous avons fait énormément, je crois, pour tenter d'empêcher que les gens soient ciblés. Ce qui me frappe, c'est que nous sommes essentiellement dans un jeu de taupe, où la technologie évolue plus vite que l'éducation. Selon vous, quel rôle joue la littératie dans la protection contre la fraude?

Ian Paterson: Je pense que la littératie est d'une importance cruciale. Je dirais également que c'est un jeu de taupe pas seulement sur le plan technologique, mais aussi sur le plan législatif.

Je ne crois pas que la fraude puisse être abolie par voie législative. Il faut un effort collectif, réunissant les organismes publics, les entreprises privées et les citoyens, chacun assumant ses responsabilités dans son propre domaine pour s'attaquer à ces enjeux. Cela peut sembler difficile, mais avec un [*Difficultés techniques*] regain d'attention à l'égard de cette question, nous pouvons avoir un effet concret sur la réduction de la fraude pour les Canadiens.

Andrew Lawton: Merci beaucoup, monsieur Paterson.

Je vais prendre ce pépin technique comme signal pour passer à mes autres questions destinées à Mme Corrigan-Brown.

Madame Corrigan-Brown, vous représentez évidemment la B.C. Securities Commission. Je sais que la structure générale du système de valeurs mobilières au Canada dépasse la portée de cette étude. Du point de vue de la prévention des fraudes et des arnaques, et en examinant que les éléments qui relèvent des autorités en valeurs mobilières, je me demande si nous faisons face à un problème au Canada, celui d'une mosaïque d'organismes de réglementation et de règlements, alors que bon nombre de ces fraudes et arnaques sont de nature nationale, voire mondiale.

Sarah Corrigan-Brown: Je pense que nous en sommes pleinement conscients. C'est précisément parce que ces fraudes sont nationales et mondiales que les autorités canadiennes en valeurs mobilières travaillent en étroite collaboration dans leurs efforts d'application de la loi. Il peut arriver que des victimes se trouvent dans plusieurs administrations, et dans de tels cas, nos équipes d'application collaborent étroitement.

Comme vous l'avez dit, le fait que ces enjeux soient nationaux et que le gouvernement fédéral, en vertu du Code criminel, ait un rôle à jouer explique également pourquoi — comme je l'ai dit ici, en tant que représentante de la BCSC, mais aussi des ACVM — nous sommes très enthousiastes et fermement engagés à travailler avec le gouvernement fédéral quant au rôle ciblé qu'il sera appelé à jouer.

• (1200)

Andrew Lawton: Selon vous, n'y a-t-il aucune inefficacité ou aucun élément qui passe entre les mailles du filet du fait qu'il existe plusieurs autorités en valeurs mobilières au Canada?

Sarah Corrigan-Brown: Je pense que, au Canada, nous travaillons très bien ensemble pour ce qui relève des organismes de réglementation provinciaux. Nos règles sont en grande partie harmonisées. Nous menons nos actions d'application de la loi conjointement et collaborons régulièrement sur presque toutes nos activités.

Il y a toujours des lacunes. Il y a toujours des possibilités d'amélioration. Toutefois, pour ce qui est d'offrir un régime de réglementation solide pour les marchés financiers canadiens, je crois que les organismes de réglementation provinciaux travaillent très bien et s'efforcent de bien servir les marchés canadiens.

Le président: Merci, monsieur Lawton.

Monsieur Paterson, je vais tenter de profiter de ce qui semble être une connexion stable pour honorer mon engagement de donner à Mme Borrelli ses 60 secondes. Nous allons essayer de nouveau.

Madame Borrelli, je vous donne l'occasion de poser une question et d'obtenir une réponse de M. Paterson. Ensuite, je passerai à M. Joseph.

Kathy Borrelli: Merci.

Monsieur Paterson, j'ai entendu des personnes âgées me dire qu'elles se sont fait convaincre d'installer un logiciel d'accès à distance et que, une fois le logiciel installé, elles ont fini par perdre beaucoup d'argent. Quelles mesures de protection techniques pourraient aider à détecter ce genre de fraude? Les banques ou les plateformes de paiement devraient-elles être tenues de prévoir des vérifications supplémentaires à cet égard?

Ian Paterson: La sensibilisation est essentielle. Outre la sensibilisation, des mesures de protection techniques, comme l'utilisation de pare-feux intégrés, pourraient très certainement permettre de détecter, en particulier, l'utilisation d'outils d'accès à distance. Ces activités peuvent être détectées et arrêtées à même le système d'exploitation. Par ailleurs, une coordination avec les entreprises de paiement pourrait certainement s'avérer utile à ce chapitre.

Kathy Borrelli: Savez-vous s'il existe des programmes qui pourraient apprendre aux personnes âgées à détecter ces activités?

Ian Paterson: Malheureusement, il s'agit d'un seul type d'escroquerie parmi tant d'autres. Les personnes âgées sont souvent aussi la cible de fraudes amoureuses, malheureusement. Comme certains députés l'ont mentionné, c'est comme le jeu de la taupe. De façon globale, il devrait y avoir de la sensibilisation au sujet des escroqueries qui peuvent être commises, et il s'agit du premier moyen de défense.

Le président: Merci, madame Borrelli.

[Français]

Monsieur Joseph, vous avez la parole pour cinq minutes.

Natilien Joseph (Longueuil—Saint-Hubert, Lib.): Merci, monsieur le président.

Je vais m'adresser dans un premier temps à M. Jude Pinto, mais je profite de l'occasion pour remercier tous les témoins de leur présence.

Monsieur Pinto, on sait que la plupart des fraudeurs ou des organismes qui fraudent les gens qui habitent au Canada n'habitent pas eux-mêmes au Canada, mais dans d'autres États. Je ne sais pas si vous avez des données. Est-ce que vous pouvez nous dire quel est le pays qui est en tête de liste?

[Traduction]

Jude Pinto: Je n'ai pas en main ces données. Nous disposons d'un service actif de recherche qui recueille ces données. Si je pouvais revenir avec de l'information et vous la transmettre, par l'intermédiaire du président, ce serait l'idéal.

[Français]

Natilien Joseph: Merci, monsieur Pinto.

Je vais poursuivre dans la même veine que ma collègue, mais je vais aller un petit peu plus loin en ce qui est à trait aux hypertrucages, qui peuvent désormais imiter de façon très convaincante la voix ou l'image d'une personne. Ils sont de plus en plus utilisés dans les cadres de fraudes et d'escroqueries.

Selon vous, quelle menace ce phénomène représente-t-il pour les Canadiens, et quelle mesure devrait être priorisée pour y faire face?

[Traduction]

Jude Pinto: Si je peux revenir sur la question, il s'agit de choses comme les hypertrucages qui sont perfectionnés sur le plan technologique et qui font de plus en plus de victimes au Canada.

Du point de vue de Paiements Canada, la meilleure manière de contribuer à cette démarche, à partir des infrastructures, est la centralisation des signalements des différents types de fraude et l'examen des tendances qui s'observent, afin que l'ensemble de l'écosystème des paiements puisse en bénéficier. Ensuite, lorsque nous réussissons à identifier ou à poursuivre l'un des acteurs responsables des fraudes, nous mettons cette information à la disposition de tous au moyen de notre liste des risques.

Je ne suis pas bien placé pour faire des commentaires au sujet des meilleurs moyens d'assurer cette protection dès le départ, au moment où l'échange a lieu. Il vaudrait probablement mieux que l'un de mes collègues réponde à cette question.

• (1205)

[Français]

Natilien Joseph: Merci.

Madame Corrigan-Brown, on sait bien que les fraudeurs qui ciblent les Canadiens opèrent de plus en plus à partir de l'étranger. Quelles seraient vos recommandations principales pour le gouvernement fédéral, afin de réduire efficacement ce type de criminalité transfrontalière?

[Traduction]

Sarah Corrigan-Brown: C'est une excellente question.

Il est difficile pour nous de prendre des mesures contre des étrangers qui s'en prennent à des Canadiens depuis l'étranger. C'est l'une des raisons pour lesquelles nous travaillons en étroite collaboration avec des organismes de réglementation européens et américains ainsi qu'avec des organismes de réglementation de l'Asie et de l'Australie, et que nous établissons des protocoles d'entente avec eux. Nous collaborons étroitement avec eux en vue d'échanger de l'information et d'identifier des fraudeurs qui se trouvent à l'extérieur de notre pays, afin qu'ils puissent les poursuivre dans leur pays.

Je dirais que, dans les faits, comme d'autres intervenants l'ont dit, la détection, la prévention et la perturbation dès le départ notamment grâce à une collaboration avec... Les fraudeurs ciblent les Canadiens par l'entremise d'Internet. Ils se servent des fournisseurs de technologies. Il faut donc réfléchir à ce que le gouvernement peut faire sur le plan législatif et aux mesures qu'il peut prendre à cet égard, afin de pouvoir intercepter des acteurs se trouvant dans le pays...

[Français]

Natilien Joseph: Excusez-moi de vous interrompre.

Combien de minutes est-ce qu'il me reste, monsieur le président?

Le président: Il vous reste 45 secondes.

Natilien Joseph: Je vais donc vous poser une dernière question, madame Corrigan-Brown, puisque vous avez mentionné la prévention.

Le budget de 2025 a annoncé la création de l'Agence des crimes financiers du Canada, tandis que la mise à jour économique du printemps a lancé une stratégie de lutte contre la fraude. Selon vous, quel impact ces initiatives auront-elles sur la prévention, la détection et la répression des crimes financiers au Canada?

[Traduction]

Sarah Corrigan-Brown: Selon moi, elles devraient avoir des répercussions globales. Nous appuyons fermement ces deux initiatives. Il est essentiel de prendre des mesures en amont dans le cadre d'une stratégie de lutte contre la fraude qui permet aux investisseurs de se protéger, de recevoir l'information nécessaire et d'être sensibilisés, tout en perturbant les activités frauduleuses qui se produisent. Le fait est que les fraudes continueront de se produire, et nous devons montrer que nous sommes vigilants et que l'intégrité de nos marchés est préservée. C'est pourquoi nous appuyons très fermement la mise sur pied d'un organisme fédéral de lutte contre les crimes financiers, puisque cela indiquera que des mesures d'application de la loi sont prises et qu'il y aura des conséquences. Je pense que cela découragera les fraudeurs de venir mener des activités dans notre pays.

[Français]

Le président: Merci, monsieur Joseph.

Je remercie tous les témoins.

[Traduction]

Merci beaucoup à tous les témoins d'avoir accepté de comparaître devant nous aujourd'hui. Nous vous sommes reconnaissants des observations et des conseils que vous nous avez fournis, alors que nous poursuivons cette discussion importante.

Chers collègues, je vais suspendre la séance brièvement afin que nous puissions nous préparer pour la prochaine heure. Nous reprendrons la séance dans environ cinq minutes.

Merci beaucoup.

• (1205)

(Pause)

• (1215)

Le président: Chers collègues, bienvenue. Nous entamons maintenant la deuxième heure de la séance. Je remercie M. Lynam, le directeur général du Centre antifraude du Canada de la GRC, de se joindre à nous. Je crois que votre témoignage nous aidera grandement à comprendre le rôle que le gouvernement fédéral joue pour régler ce problème.

Monsieur Lynam, vous avez jusqu'à cinq minutes. Vous êtes le seul témoin à comparaître pour cette période de questions, ce qui nous permettra d'examiner en profondeur votre domaine d'expertise.

Chers collègues, j'ai mentionné à quelques-uns d'entre vous tout juste avant le début de la séance que nous tirons un peu de l'arrière. Comme nous siégeons pendant trois heures aujourd'hui, nos travaux coïncideront avec le début de la période des questions. Le temps alloué à cette période et à la période suivante pourrait donc être légèrement réduit, mais nous veillerons à ce que chacun ait la possibilité de prendre la parole.

Sur ce, monsieur Lynam, merci encore une fois de vous joindre à nous. La parole est à vous, monsieur.

Chris Lynam (directeur général, Centre antifraude du Canada, Gendarmerie royale du Canada): Bonjour, monsieur le président et honorables membres du Comité. Je vous remercie de m'avoir invité à comparaître aujourd'hui. Je tiens à reconnaître que nous sommes réunis sur le territoire traditionnel non cédé de la Nation anishinabe et à souligner la présence durable des Premières Nations, des Inuits et des Métis.

Je m'appelle Chris Lynam. Je suis le directeur général du Centre national de coordination contre la cybercriminalité et du Centre antifraude du Canada à la Gendarmerie royale du Canada.

La fraude financière et les escroqueries représentent une menace importante, en constante évolution et de plus en plus complexe pour les Canadiens et pour notre économie, avec des répercussions majeures partout au pays. En 2025 seulement, le Centre antifraude du Canada a reçu des signalements de pertes liées à la fraude et à la cybercriminalité totalisant plus de 700 millions de dollars. Cela marque huit années consécutives de pertes record, et nous estimons que cela ne représente qu'une fraction des pertes réelles subies.

La fraude est devenue organisée, industrialisée et hautement automatisée. Les Canadiens sont ciblés par des centres d'arnaques très structurés qui emploient des milliers de personnes et exercent leurs activités dans diverses régions du monde. Il existe également des fraudeurs individuels qui exploitent des plateformes de fraude en tant que service, faciles à utiliser et peu coûteuses. Ces stratagèmes sont facilités par les plateformes numériques et les technologies émergentes, permettant même à des acteurs ayant peu d'expertise technique de frauder des Canadiens à grande échelle.

À titre d'exemple, une récente plateforme d'hameçonnage en tant que service a été utilisée par des milliers de personnes basées au Canada, et près d'un million de Canadiens ont été victimes de cette seule plateforme. L'environnement de menace continue d'évoluer rapidement, en grande partie sous l'impulsion des progrès technologiques et de l'automatisation, notamment l'intelligence artificielle. Les acteurs criminels utilisent l'intelligence artificielle pour générer des messages d'hameçonnage convaincants, rédiger et traduire des

courriels et des textos frauduleux, produire des vidéos et des appels trompeurs à l'aide d'hypertrucages, exploiter des données volées afin d'identifier de nouvelles victimes et tirer parti des vulnérabilités des réseaux.

Face à ces menaces, le Centre antifraude du Canada joue un rôle central dans la lutte contre la fraude au Canada, selon quatre axes d'intervention: la prévention, le soutien aux victimes, la perturbation et la poursuite des criminels responsables des escroqueries.

Pour faciliter la prévention, le CAFC utilise des communications ciblées pour sensibiliser le public aux menaces de fraude sur son site Web, par l'entremise des médias sociaux et lors d'activités en personne. L'objectif est d'aider les Canadiens à reconnaître et à éviter la fraude, et d'encourager les personnes à risque, en particulier les jeunes, à ne pas s'engager dans des activités de fraude et de cybercriminalité.

Pour ce qui est du soutien aux victimes de fraude, nous aidons les victimes en leur fournissant des conseils pour limiter les pertes supplémentaires et, dans certains cas, en coordonnant des interventions rapides avec des partenaires afin de geler ou de récupérer des fonds. Nous donnons également des conseils pour aider les victimes à éviter d'être ciblées de nouveau. Le CAFC reçoit souvent des renseignements concernant des victimes qui ignorent qu'elles font l'objet d'une fraude, par exemple dans les cas de fraude amoureuse. Dans ces situations, des employés du CAFC communiquent avec les victimes pour les avertir.

En ce qui concerne la perturbation, nous collaborons avec les institutions financières, les fournisseurs de télécommunications et les plateformes numériques afin de perturber l'écosystème de la fraude en identifiant et en neutralisant les entités, outils et services — les facilitateurs — qui permettent les activités frauduleuses.

Il faut également poursuivre les fraudeurs. Pour ce faire, nous appuyons les enquêtes et aidons nos partenaires à poursuivre les responsables en fournissant des renseignements exploitables et des pistes d'enquête, en coordonnant les efforts entre plusieurs organismes et en reliant les initiatives canadiennes à des enquêtes et opérations criminelles multinationales.

Les signalements reçus du public et des entreprises ciblées ou victimes sont essentiels aux efforts du CAFC. Grâce à notre plateforme de signalement modernisée, reportcyberandfraud.canada.ca, les Canadiens peuvent plus facilement signaler les incidents de fraude et de cybercriminalité. De plus, le CAFC a établi de nombreux partenariats au Canada et à l'échelle internationale pour lutter contre la fraude; ces partenariats sont essentiels dans un contexte d'enquête souvent complexe, transfrontalier et exigeant en ressources.

Enfin, le CAFC continue de mettre en œuvre des approches novatrices et globales afin de réduire les répercussions de la fraude sur les Canadiens. Nous croyons que nos quatre axes d'intervention sont sensés et donnent des résultats opérationnels concrets, mais nous devons collaborer avec davantage de partenaires, à plus grande échelle, pour réduire le nombre de victimes de fraudes au Canada. Soyez assurés que nous nous engageons pleinement à nous acquitter de notre mission.

Je vous remercie. Je serai heureux de répondre à vos questions.

• (1220)

Le président: Merci beaucoup, monsieur Lynam.

Monsieur Lawton, vous avez la parole pour six minutes.

Andrew Lawton: Merci beaucoup, monsieur le président.

Merci beaucoup, monsieur Lynam, d'être ici aujourd'hui.

Pour remettre un peu les choses en contexte, j'ai pris conscience de manière plutôt brutale de cet enjeu au cours des derniers mois alors que j'ai discuté avec un certain nombre d'électeurs qui ont été victimes de fraude; dans certains cas, ils ont perdu des petites sommes, et dans d'autres, ils ont perdu des sommes extrêmement importantes.

Un cas qui est gravé dans ma mémoire est celui d'un homme qui était en larmes durant une assemblée publique que j'avais organisée avec le service de police de St. Thomas au sujet de la prévention de la fraude. Il s'était fait voler une petite somme d'argent après avoir été victime d'une fraude liée à la cryptomonnaie. Puis, il s'est fait escroquer de nouveau par une personne qui prétendait faire partie d'une agence qui l'aiderait à récupérer ses pertes. Au bout du compte, lui et sa femme ont perdu tout ce qu'ils possédaient: 80 000 \$. Lorsqu'il a raconté ce qui lui était arrivé, tous les autres ont levé la main parce qu'ils avaient eux aussi une histoire à raconter.

Ces situations se produisent de plus en plus souvent. Je sais et je crois sincèrement que vous êtes déterminés à tenter de mettre fin à tout cela du mieux que vous pouvez. À quelle fréquence parvenez-vous à récupérer des fonds? À quelle fréquence les sommes volées sont-elles récupérées?

• (1225)

Chris Lynam: Merci de poser la question.

Malheureusement, nous entendons effectivement, tout comme vous l'avez entendu de vos électeurs, ces histoires tragiques de personnes qui perdent toutes leurs économies. Cela se produit partout au Canada.

Malheureusement, le pourcentage de cas où nous pouvons tenter d'aider les gens à récupérer leur argent, ou du moins geler les fonds, est relativement petit. Une partie du problème tient au fait qu'il y a beaucoup de honte associée au signalement d'une fraude, et les gens ne la signalent pas. Dans certains cas, il y a une marge de manœuvre. Si un virement électronique a été effectué et que la victime ne signale pas la fraude, il n'y a plus de marge de manœuvre. Il s'agit d'un faible pourcentage des cas que nous observons, mais nous encourageons les gens à signaler ces incidents. Comme nous en avons parlé, et comme nous allons en parler, la prévention est vraiment essentielle pour éviter d'être victime dès le départ.

Andrew Lawton: Je suis bien entendu plus au courant des histoires qui se produisent à l'échelle locale. Il y a eu tout récemment une fraude liée aux cartes-cadeaux à St. Thomas, ainsi qu'une fraude de 20 000 \$ liée à une application de cryptomonnaie. Une autre personne a investi de l'argent dans une plateforme qu'elle ne comprenait pas vraiment et elle a fini par perdre 10 000 \$. Il y a aussi ces faux projets d'investissement. Dans un autre cas qui nous a été signalé, une personne a perdu environ 3 000 \$.

Je sais que toutes les escroqueries sont différentes et ainsi de suite, mais si vous pouviez faire une généralisation, même dans une certaine mesure, combien d'entre elles sont commises au Canada par rapport à celles qui sont commises à l'étranger?

Chris Lynam: Il est souvent très difficile de déterminer, en amont, d'où provient la fraude, parce que ce sont des fraudeurs; ils

ne vous diront pas d'où ils exercent leurs activités. Une grande partie des différentes fraudes sont commises depuis l'étranger.

J'ai parlé un peu des centres d'arnaques. Ceux-ci se concentrent souvent sur des activités comme les fraudes liées aux investissements ou les fraudes liées à l'emploi. Toutefois, il y a des fraudes qui commencent au pays. J'ai parlé des fraudes commises au moyen de fausses plateformes de services, que peuvent utiliser des personnes ayant des compétences techniques très limitées pour frauder des Canadiens. C'est un mélange des deux, mais la majorité des fraudes sont commises depuis l'étranger.

Andrew Lawton: J'ai parlé plus tôt d'un homme qui s'est fait voler plus de 80 000 \$. L'entreprise, le faux cabinet d'avocats, qui était l'auteur de cette fraude a un site Web qui, encore à ce jour, est toujours en ligne, même après que la police a enquêté à son sujet.

Si quelqu'un consulte ce site Web, il verra les mêmes renseignements que cet homme a vus, les mêmes photos de personnes qui semblent être avocats et qui affirment avoir réussi à récupérer de l'argent. Si nous prenons cet exemple — et d'autres du même genre —, pourquoi ces sites Web restent-ils en ligne? Que devons-nous faire, du point de vue stratégique, pour que les sites qui sont reconnus comme étant frauduleux, comme étant des arnaques, soient retirés d'Internet?

Chris Lynam: Il s'agit, comme vous pouvez l'imaginer, d'une situation horrible à vivre lorsqu'on perd son argent et qu'on pense pouvoir le récupérer en s'adressant à ce qui semble être une institution réputée.

Il faut tenir compte de quelques facteurs. Tout d'abord, le problème est en quelque sorte lié à la nature même d'Internet, des noms de domaine enregistrés et du fonctionnement de l'hébergement Web, qui permet à presque n'importe qui de mettre en ligne un site Web. Il n'y a pas beaucoup de surveillance effectuée en amont.

Cela dit, lorsque nous obtenons cette information et que nous voulons perturber des activités de fraude, nous communiquons souvent avec l'hébergeur Web ou le registraire de noms de domaines pour l'aviser que nous croyons qu'un site contrevient à ses conditions d'utilisation. Idéalement, une enquête est menée en parallèle, mais il s'agit notamment de faire retirer le site Web pour éviter qu'il fasse d'autres victimes. C'est ce que votre Comité fait; il examine la question et cherche à savoir comment formuler des recommandations visant l'adoption d'une approche globale qui permettra de réduire le nombre de victimes dans tout le pays.

Andrew Lawton: Obtenez-vous des résultats à cet égard? Sinon, pour ce qui est des sites que nous pouvons désigner comme étant frauduleux, lorsque nous savons que le site Web sert de point d'entrée à des fraudes, quel mécanisme stratégique pourrions-nous mettre en place pour parvenir à le retirer d'Internet?

Chris Lynam: Je vais parler de ce que nous faisons sur le plan opérationnel.

Une partie de cette question est en quelque sorte un thème récurrent. En réalité, le processus à suivre, du point de vue de la collaboration opérationnelle, consiste à réunir de nombreux partenaires qui détiennent des données au sujet des facilitateurs de la fraude, puis à faire appel à des organisations qui sont en mesure d'intervenir.

Nous avons organisé une opération appelée « Opération Érable » en décembre dernier au cours de laquelle nous avons fait cela. Nous avons réuni un grand nombre de partenaires des secteurs privé et public. Nous avons été en mesure d'obtenir rapidement de l'information et de la transmettre aux bonnes entités qui pouvaient prendre les mesures nécessaires. Nous allons organiser une Opération Érable en 2026 et prendre des mesures à une échelle beaucoup plus grande. Nous avons simplement l'impression qu'il faut être en mesure de prendre des mesures presque en temps réel si nous voulons obtenir des résultats sur le plan opérationnel.

• (1230)

Le président: Merci beaucoup, monsieur Lawton.

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

Dominique O'Rourke (Guelph, Lib.): Merci beaucoup, monsieur le président.

Merci au directeur général d'être ici avec nous. J'aimerais vous poser une question un peu plus générale, puisque vous êtes directeur du Centre national de coordination en cybercriminalité et du Centre antifraude du Canada au sein de la GRC. C'est un mandat très large.

La Chambre des communes examine présentement le projet de loi C-22, qui vise à donner un accès légal à la GRC et aux agents de police, à l'échelle du pays, pour qu'ils puissent avoir des outils numériques plus à jour afin de lutter contre la criminalité. Pourriez-vous dire au Comité pourquoi le projet de loi C-22 serait utile pour lutter contre la cybercriminalité et mener des enquêtes dans ce domaine, mais aussi particulièrement contre la fraude et les escroqueries?

Chris Lynam: L'un des grands défis liés aux technologies visant à lutter contre ce que nous appelons le cybercrime ou la cyberfraude, c'est que les criminels, les victimes et les données sont souvent éparpillés dans une foule d'administrations du Canada. Pour mener ces enquêtes efficacement et rapidement, les policiers canadiens ont besoin d'outils appropriés.

Des projets de loi comme le projet de loi C-22 et certains des pouvoirs qu'il confère, peu importe le type de crime — particulièrement ceux qui comportent un important élément numérique — nous aideront à avoir les outils supplémentaires nécessaires pour poursuivre les fraudeurs et les cybercriminels.

Dominique O'Rourke: La GRC juge-t-elle que le projet de loi C-22 concernant l'accès légal est important pour lutter contre la fraude et un large éventail de cybercrimes?

Chris Lynam: Comme je l'ai mentionné, les outils numériques ou les lois s'appliquant aux infractions ayant une composante numérique importante... C'est très important pour nous d'avoir ces outils modernes. Le projet de loi C-22, s'il est adopté, aidera les policiers en leur donnant des outils supplémentaires pour faire leur travail.

Dominique O'Rourke: Avez-vous les outils dont vous avez besoin, ou les criminels ont-ils des outils toujours plus performants?

Chris Lynam: L'un des défis, pour les organismes d'application de la loi, c'est que nous plaçons la barre très haut en ce qui concerne le type de technologies et d'outils que nous adoptons. Ils doivent être légaux. Ils doivent respecter le droit à la vie privée des Canadiens. Le processus d'évaluation et de mise en œuvre peut souvent être chronophage. Les cybercriminels et les autres criminels ne respectent pas ces règles. Dès qu'ils auront accès à la première in-

telligence artificielle malveillante, ils vont adopter cette technologie et trouver un moyen de l'utiliser.

C'est toujours un peu le jeu du chat et de la souris; nous ne savons pas quelles nouvelles technologies les criminels vont adopter. Mon centre collabore entre autres avec le plus grand nombre possible de services de police, partout au pays, pour échanger de l'information et établir des stratégies coordonnées pour les poursuivre, soit avant qu'ils ne puissent utiliser ces nouveaux outils, soit dès que l'on sait qu'ils les utilisent.

Dominique O'Rourke: J'aimerais changer un peu de sujet.

Un rapport spécial publié dans *Reuters* a cité des documents internes de Meta, selon lesquels l'entreprise estimait qu'environ 10 % de son chiffre d'affaires annuel total, en 2024, soit 16 milliards de dollars, provenait de publicités frauduleuses.

J'ai une expérience dans le domaine des assurances et dans le secteur municipal. Je connais bien la responsabilité solidaire. Donc, cela veut-il dire que Meta est complice d'une fraude? Que devraient faire les plateformes pour faire obstacle aux fraudeurs présents sur leurs plateformes?

Chris Lynam: Pour répondre à la première partie de votre question, je ne crois pas être le mieux placé pour déterminer à qui incombe la responsabilité. Je dirais que toutes les plateformes numériques ont un rôle essentiel à jouer dans la lutte contre la fraude et la cybercriminalité au Canada. Nous avons établi d'excellentes relations et nous avons trouvé une façon de leur transmettre des informations et d'en recevoir de leur part, mais il reste beaucoup à faire. Il reste certainement beaucoup à faire à tous les niveaux, en ce qui concerne les rôles des plateformes numériques à ce chapitre.

Dominique O'Rourke: J'ai une dernière question.

Vous avez dit que les jeunes doivent être davantage sensibilisés à la fraude. Les bureaux de nos circonscriptions ont tous reçu des appels de personnes âgées qui ont été victimes de fraude. Il est possible que ce groupe démographique hésite moins à signaler les cas de fraude.

Expliquez-nous un peu mieux le paysage. Je pense à la fraude sentimentale. Les victimes ne sont pas nécessairement des personnes âgées. Comment lutter contre les fraudes en tenant compte de chaque public cible?

• (1235)

Chris Lynam: C'est une excellente question. Tout est dans la manière. Vous adoptez une approche différente en matière de prévention pour les aînés et pour les jeunes. Il s'agit souvent de personnes qui cliquent tout de suite et réfléchissent plus tard. Nous essayons d'adopter plusieurs approches. Une campagne de sensibilisation sur les médias sociaux ou en ligne pourrait être mieux adaptée à un public plus jeune, tandis que la mobilisation en personne ou la documentation imprimée... Nous faisons beaucoup de ce genre de travail.

Pour finir, il ne faut pas des compétences techniques très hautes pour devenir un fraudeur ou un cybercriminel. Nous faisons du travail de sensibilisation auprès des jeunes qui pourraient s'intéresser à ces plateformes ou à ces forums. Ils entendent dire que c'est très facile et que la police a du mal à les épingler. Nous leur disons: « Écoutez, vous ne devriez pas vous engager là-dedans. Vous allez gâcher votre vie. » Il reste encore du travail à faire à ce chapitre.

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.

Monsieur Lynam, je vous remercie de vous présenter devant le comité aujourd'hui.

Comme vous l'avez dit, il y a plusieurs types de fraudes. Je vais commencer par une qui a été abordée, les publicités frauduleuses publiées sur les plateformes comme Facebook. Il y a quelques semaines, le *Journal de Montréal* présentait un dossier dans lequel on apprenait qu'en raison des avancées technologiques, il y a maintenant de fausses vidéos qui semblent vraies et dans lesquelles on voit, par exemple, le premier ministre Carney, l'ancien premier ministre du Québec François Legault, des gens d'affaires comme Luc Poirier ou Kevin O'Leary, ou encore des acteurs internationaux comme Keanu Reeves, qui disent aux gens d'investir là-dedans parce que c'est payant.

Une personne à la retraite essaie en investissant quelques dollars. Elle retire son argent et réalise un profit. Après ça, elle investit quelques milliers de dollars, elle retire son argent et réalise un profit mirobolant. Il arrive souvent que la personne décide finalement d'investir tout son fonds de pension là-dedans, mais pouf, l'argent disparaît.

Dans l'article du *Journal de Montréal*, il y avait, entre autres, deux personnes qui avaient perdu plus de 100 000 \$ à cause de cette arnaque. *Enquête*, une émission d'affaires publiques de Radio-Canada, avait même parlé d'un cas où la personne avait perdu plus de 400 000 \$, si ma mémoire est bonne, des économies d'une vie qui s'envolent du jour au lendemain.

Selon les différents acteurs, qu'est-ce qui doit être fait pour que ce genre de fraude ne se reproduise plus jamais ici?

[Traduction]

Chris Lynam: C'est un type d'escroquerie ou de fraude très complexe. Il s'agit d'exploiter le besoin des gens de gagner de l'argent ou de saisir une occasion. On fait ensuite appel aux hypertrucages et ainsi de suite. L'un des défis, c'est que nous devons adopter une approche holistique. D'une part, il y a la prévention et la sensibilisation, pour que les gens comprennent que ce genre d'escroqueries existe et sachent comment s'en protéger. D'autre part, il s'agit d'empêcher ce genre d'activités. Il y a des publicités qui circulent. Il y a des publicités sur des sites Web. Au CAFC, nous travaillons avec nos partenaires de la police et nous essayons d'empêcher ces activités et d'y mettre fin.

Il y a ensuite les enquêtes. Notre centre reçoit souvent des signalements de la part des victimes. Nous pouvons alors établir des liens entre les différents éléments et collaborer avec nos partenaires de la police pour poursuivre les responsables. Cela implique souvent une dimension internationale, car les responsables mènent leurs activités depuis un autre pays.

Nous devons adopter une approche holistique et suivre une foule de pistes, pour combattre cela.

[Français]

Gabriel Ste-Marie: D'accord, merci.

Souvent, comme vous l'avez dit, les fraudeurs sont à l'étranger. Les émissions d'affaires publiques nous révèlent que, souvent, ça se fait dans des pays très pauvres. Souvent, même les personnes qui

sont obligées de commettre ces fraudes sont sous la menace de groupes organisés, qui les séquestrent ou les font chanter en leur disant qu'ils travaillent pour eux et qu'ils doivent rapporter de l'argent. Comment est-ce que la GRC collabore au niveau international pour arriver à démanteler ces réseaux?

● (1240)

Chris Lynam: C'est un grand défi pour les victimes, c'est aussi un grand défi pour la GRC de lutter contre les fraudes outremer. Premièrement, nous utilisons notre réseau d'officiers de liaison dans d'autres pays. De plus, il y a certaines organisations régionales, comme Europol, où la GRC a quelques officiers membres de ce qui s'appelle le Joint Cybercrime Action Taskforce. Grâce à ces organisations, des services de police internationaux peuvent échanger de l'information en temps réel. C'est une approche, un exemple, de la manière dont la GRC lutte contre la fraude outremer.

Gabriel Ste-Marie: D'accord, merci beaucoup.

Il y a un autre type de fraude. Avec toutes les fuites de données qu'il y a eu dans diverses institutions, il arrive souvent que des fraudeurs se présentent au domicile de la personne qu'ils visent pour la frauder en lui disant que son compte a été fraudé, qu'elle devrait les suivre et leur remettre sa carte de débit. Ces gens peuvent arriver avec des vêtements qui ressemblent à des costumes de policiers. Qu'est-ce qui peut être fait contre ça? Est-ce qu'il y a quelque chose à faire pour mieux contrer toutes les fuites de données de diverses entreprises?

[Traduction]

Chris Lynam: Je vais commencer par votre premier exemple de fraude, qui est généralement une arnaque liée à une fausse urgence. Les criminels disent aux victimes « je dois passer chez vous et récupérer de l'argent », ou quelque chose de ce genre. On l'a vu. Les aînés en sont souvent la cible.

Plusieurs enquêtes de qualité ont été menées sur ces fraudes. C'est un domaine où la prévention et la sensibilisation sont essentielles. Nous avons constaté que, quand les jeunes ou les proches disent aux aînés « je ne vais jamais t'appeler à l'improviste pour te dire que je suis en prison quelque part et que j'ai besoin de 5 000 \$ », quand ils ont cette discussion, c'est très efficace pour aider les aînés à comprendre et à éviter ce genre d'arnaque. Encore une fois, c'est un exemple de l'importance des discussions en personne.

Votre deuxième question portait sur les fuites de données et ainsi de suite. Malheureusement, énormément de fraudes exploitent des données qui ont été volées puis dépouillées pour obtenir l'identité d'une personne ou un moyen de s'en servir contre elle et la frauder. Cela relève de la deuxième partie de mes responsabilités globales en matière de lutte contre la cybercriminalité, à savoir poursuivre les cybercriminels qui piratent des systèmes pour voler des données et les exploiter à d'autres fins.

Nous utilisons la même approche. Nous faisons du travail de prévention. Nous travaillons avec le plus de partenaires possible, et nous perturbons l'écosystème des cybercriminels qui essaient de voler ces données.

[Français]

Gabriel Ste-Marie: Merci.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

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

Ted Falk: Merci, monsieur le président.

Merci, monsieur Lynam, de votre témoignage d'aujourd'hui.

Je voudrais simplement revenir rapidement sur les questions de Mme O'Rourke à propos du projet de loi C-22.

À votre avis, quels outils spécifiques prévus dans le projet de loi C-22 vous aideraient le mieux à prévenir les crimes ou les escroqueries?

Chris Lynam: En ce qui concerne le fonctionnement des autorisations judiciaires, évidemment, quand les services de police doivent obtenir légalement des données pour mener leur enquête et identifier les responsables, ils doivent demander les données aux institutions financières, aux fournisseurs de services de télécommunications ou à d'autres entités. Compte tenu de la rapidité de la cyberfraude, plus les organismes d'application de la loi récupèrent rapidement ces données, plus leur enquête avance.

Je vais vous donner un exemple des outils qui permettent aux services de police de demander une autorisation judiciaire, par l'entremise des tribunaux, puis de récupérer les données. Cela permet — comme on dit — d'évoluer au rythme de la cybercriminalité. Je vais utiliser cet exemple. Je vous le donne. C'est l'exemple que je donne pour montrer comment les outils ou les lois liés au projet de loi C-22 peuvent aider les organismes d'application de la loi.

Ted Falk: D'accord, et vous ne croyez pas avoir ces outils aujourd'hui.

Chris Lynam: C'est seulement...

Ted Falk: C'est simplement plus long, car il faut une autorisation judiciaire.

Chris Lynam: Il y a eu des changements législatifs en ce qui concerne les délais de traitement des ordonnances de communication dans le domaine de l'information financière. C'est simplement un exemple. La cyberfraude est un type de crime qui est accompli très rapidement. Pour que la police puisse poursuivre les cybercriminels et les fraudeurs, nous devons recevoir rapidement les données obtenues légalement pour pouvoir les analyser, identifier les tendances et procéder à l'attribution et ainsi de suite. Les réponses rapides aux autorisations judiciaires sont un exemple d'un outil important dont a besoin la police.

• (1245)

Ted Falk: On dit que 5 à 10 % seulement des escroqueries ou des fraudes sont signalées à la police. Je suis sûr que vous faites une analyse coûts-bénéfices quand une personne signale avoir été victime d'une escroquerie ou d'une fraude. Croyez-vous qu'il vaut toujours la peine de poursuivre ces escroqueries?

Chris Lynam: Quand vous dites « coûts-bénéfices », parlez-vous...

Ted Falk: C'est les efforts que la GRC doit déployer, le travail d'enquête.

Chris Lynam: D'accord. Nous adoptons cette approche, dans la mesure où... Cela est fondé sur plusieurs facteurs, y compris la présence de pistes d'enquête solides ou de renseignements pouvant faire l'objet d'un suivi. Le cas échéant, si des partenaires — nationaux et internationaux — veulent collaborer, cela pourrait devenir une enquête criminelle complète. Si ce genre de pistes n'est pas fa-

cilement accessible, on pourrait mener des activités dont le but est de perturber.

Parallèlement, nous faisons continuellement du travail de prévention, nous tirons des leçons de ce qui s'est passé et nous informons les gens des dernières escroqueries qui nous ont été signalées.

Ted Falk: D'accord. Quelqu'un vous signale une fraude. Vous regardez le signalement et vous dites que vous allez consacrer tous ces efforts, toutes ces heures-personnes, toutes ces ressources, et que vous allez essayer d'obtenir une condamnation. Puis l'affaire est portée devant les tribunaux, et le fraudeur reçoit une peine bonbon.

Je pense à une femme de Montréal qui, en mars dernier, s'est fait escroquer des milliers de dollars. Les criminels ont été condamnés à 18 mois de détention à domicile, avec de nombreuses dérogations pour aller au gym et d'autres choses de ce genre. Elle a dit que la peine était une vraie blague.

Croyez-vous vous aussi, en tant que représentant de la GRC, qu'il n'y a pas de peines adéquates pour les crimes commis?

Chris Lynam: Nous nous concentrons généralement sur les activités de type « retour sur investissement », ce que nous pensons pouvoir faire aboutir, que ce soit par l'entremise de poursuites judiciaires ou par des mesures perturbatrices. Nous concentrons nos efforts sur ce type de calcul, pour déterminer comment nous pouvons réduire au maximum la fraude et la cybercriminalité au Canada. Cela fait toujours partie de nos calculs. Nous avons tendance à concentrer nos efforts sur ce domaine, ainsi que sur la prévention, plutôt que sur les résultats obtenus au bout du compte.

Ted Falk: Vos agents ou vos employés sont-ils parfois frustrés de voir que la sanction ne correspond pas à la gravité du crime et aux efforts qui ont été déployés pour obtenir une condamnation?

Chris Lynam: En ce qui concerne le rôle du Centre antifraude du Canada et du Centre national de coordination en cybercriminalité, nous ne sommes pas l'organisme chargé de l'enquête. Nous travaillons avec tous les partenaires et, généralement, avec un organisme responsable. Je ne peux pas dire ce que fera l'enquêteur chargé de l'enquête... ni quels seront les résultats.

Notre rôle principal, c'est de rassembler ces entités, de leur fournir les renseignements et les technologies nécessaires et de les orienter de la meilleure façon possible pour obtenir les meilleurs résultats possibles.

Ted Falk: Merci.

Le président: Merci beaucoup, monsieur Falk.

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

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

Merci, monsieur Lynam, d'être ici.

Pour commencer, pourriez-vous décrire la façon dont le Centre antifraude du Canada coordonne ses efforts avec les institutions financières, les fournisseurs de services de télécommunications, les organismes d'application de la loi et les plateformes numériques pour identifier et contrer les nouvelles fraudes? En particulier, s'agit-il d'une approche de prévention proactive ou d'une approche visant à résoudre les crimes après qu'ils ont été commis?

Chris Lynam: Je dirais que ce sont les deux, mais nous visons principalement à être proactifs. Comme je l'ai dit dans ma déclaration préliminaire et en réponse à l'une des questions, on nous signale qu'un site Web, une adresse courriel ou un portefeuille de cryptomonnaie sont utilisés pour commettre des fraudes. Nous allons communiquer avec l'institution financière, le fournisseur de services de télécommunications et ainsi de suite, et nous allons dire: « Écoutez, nous croyons que cela contrevient à vos modalités de service et c'est à vous de décider si vous voulez agir. »

De plus en plus, nous essayons de faire cela à grande échelle, presque en temps réel. J'ai parlé de l'Opération Érable qui a réuni tous ces partenaires en personne pour faire ce travail. Cela a permis des gains d'efficacité dans nos mesures d'intervention.

Parallèlement, s'il y a une victime ou si une enquête est lancée, les organismes d'application de la loi travailleront en étroite collaboration avec les institutions financières, les fournisseurs de services de télécommunications et d'autres entités dans le cadre de l'enquête. Le niveau de collaboration opérationnelle a considérablement augmenté ces dernières années.

• (1250)

Michael Ma: Merci.

Quels sont les plus importants obstacles opérationnels à la coordination des efforts de lutte contre la fraude à l'échelle des secteurs et des administrations? Par exemple, le problème tient-il à l'échange de données ou à la fragmentation des compétences? Ces obstacles tiennent-ils aussi à des acteurs internationaux?

Chris Lynam: Ces obstacles ou défis existent aux niveaux tant national qu'international, dans une certaine mesure. L'échange de données entre les secteurs public et privé est toujours un défi, et ainsi de suite. La culture joue aussi un rôle. On se demande: « Est-ce que je vais prendre le risque de diffuser cette information dans l'intérêt du public? » Toutefois, il y a eu de grandes améliorations à cet égard.

Vous avez parlé de la question du découpage des compétences. C'est effectivement un défi. Notre approche repose encore en grande partie sur des critères géographiques, aux niveaux national et international, c'est donc là que nous avons besoin d'une coordination très solide. C'est ce que fait mon centre, tous les jours, on essaie de réunir les parties prenantes et de déterminer comment tirer le meilleur parti des ressources policières pour réduire au maximum la cybercriminalité et la fraude.

Michael Ma: Merci.

Nous avons brièvement parlé du recouvrement des fonds et ainsi de suite. Dans quelle mesure la rapidité de l'échange d'informations entre les institutions et les organismes d'application de la loi est-elle importante pour éviter que les criminels fassent de nouvelles victimes ou pour récupérer les fonds?

Chris Lynam: La rapidité est impérative. J'ai dit qu'il y avait un certain laps de temps — par exemple, pour un virement électronique ou tout autre type de virement d'argent —, avant que ce soit finalisé. Parallèlement, parfois, certaines transactions ont déjà été finalisées, et il est donc impossible de récupérer les fonds.

Ces deux ou trois dernières années, j'ai vu les banques et les entreprises de télécommunications discuter de la manière d'échanger ces données pour éviter qu'il y ait de nouvelles victimes. Ensuite, la Coalition canadienne antifraude a été mise sur pied, et nous en sommes membres. C'est une excellente initiative qui réunit toutes

les parties pour trouver un moyen holistique de partager l'information ou de régler le problème.

Michael Ma: Merci. Merci du travail que vous faites.

Pendant le Mois de la prévention de la fraude, le centre a souligné l'importance de mettre en lumière les crimes cachés. Pourquoi la fraude est-elle encore largement sous-déclarée au Canada, et en quoi cela influe-t-il sur les efforts de prévention?

Chris Lynam: C'est une excellente question.

J'ai dit que nous croyons que seulement 5 à 10 % des victimes signalent les fraudes. Il y a encore beaucoup de honte associée à cela. Les gens ont l'impression d'avoir fait quelque chose de mal. Les aînés, en particulier, s'inquiètent parce qu'ils ont perdu des sommes importantes. La honte joue un rôle important, c'est pourquoi nous passons beaucoup de temps à essayer de les rassurer en leur disant: « C'est vous, la victime. » C'est un élément important de notre message. Je supervise des gens hautement qualifiés, et quand ils parlent au téléphone avec des victimes, ils adoptent une approche axée sur les victimes. Toutefois, nous avons encore du pain sur la planche. Les campagnes de sensibilisation du public se poursuivent pour encourager les gens à signaler la fraude.

Pour finir, j'ai dit dans ma déclaration préliminaire que nous avons lancé un nouveau site public de signalement. Nous recevons toujours des appels téléphoniques, mais, avec le nouveau site, nous recevons maintenant deux fois et demie plus de signalements en ligne qu'auparavant. Nous faisons des progrès en ce qui concerne le signalement.

Michael Ma: Je suis content de l'entendre. Merci beaucoup.

Le président: Merci, monsieur Ma.

[Français]

Comme je l'ai mentionné au début, je dois réduire le temps alloué pour les trois prochaines questions. M. Ste-Marie aura une minute, Mme Kronis en aura deux et demie, puis pour les libéraux, Mme Begum en aura deux et demie.

Monsieur Ste-Marie, vous avez la parole pour une minute.

Gabriel Ste-Marie: Merci, monsieur le président.

Monsieur Lynam, j'aimerais avoir votre opinion pour ce qui est de la responsabilité civile. Quelqu'un qui se fait frauder et qui a des motifs raisonnables de croire que la plateforme a été négligente devrait-il être tenu coresponsable, selon vous, parce qu'on parle de crime ici? À partir de quel pourcentage de ces publicités étant de la fraude une organisation devrait-elle être désignée organisation criminelle? Merci.

[Traduction]

Chris Lynam: Malheureusement, je ne suis pas bien placé pour donner des avis juridiques en matière civile sur la question de la responsabilité civile de l'utilisateur de la plateforme et ainsi de suite. Comme je l'ai dit aujourd'hui, les plateformes numériques ont certainement un rôle à jouer et devraient s'assurer de recevoir rapidement des informations que nous leur transmettons, de nous envoyer des informations et d'effectuer des recherches sur leurs plateformes. Je pense qu'il reste beaucoup à faire à ce chapitre.

• (1255)

[Français]

Gabriel Ste-Marie: Merci, monsieur le président.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Madame Kronis, allez-y, vous avez deux minutes et demie.

Tamara Kronis (Nanaimo—Ladysmith, PCC): Merci beaucoup.

Nous essayons d'aller aussi vite que l'Internet.

Vous avez souligné l'importance de la prévention et décrit les entreprises de télécommunications, les banques et les institutions financières comme... Peut-on dire qu'elles sont coopératives et réceptives, mais surtout réactives?

Chris Lynam: En ce qui concerne la prévention?

Tamara Kronis: Non, désolée. En ce qui concerne l'intervention quand une escroquerie se produit.

Chris Lynam: Je ne suis pas sûr de bien...

Tamara Kronis: Permettez-moi de vous poser une question.

Y a-t-il un moyen d'empêcher que les gens reçoivent un texto ou un appel frauduleux?

Chris Lynam: Tout à fait; les entreprises de télécommunications le peuvent, et on peut trouver d'autres moyens d'interrompre ces activités, selon le propriétaire du type de chaîne. Cela se fait tous les jours. Nous devons intensifier nos efforts dans ce sens. Nous devons définir des cadres pour renforcer cela.

Tamara Kronis: Est-ce volontaire ou est-ce réglementé?

Chris Lynam: Je ne suis pas bien placé pour dire si cela est soumis à une réglementation ou si cela est fait de manière volontaire, du côté des entreprises de télécommunications. D'après les discussions que nous avons avec ces secteurs, ils veulent vraiment en faire plus pour lutter contre la cybercriminalité et la fraude.

Tamara Kronis: Y a-t-il quelque chose qui oblige les entreprises de télécommunications à signaler les fraudes en temps réel ou le volume de stratagèmes frauduleux qui circulent sur leurs réseaux?

Chris Lynam: Non, mais je sais qu'ils ont des protocoles, comme le protocole STIR/SHAKEN, pour vérifier les appels et s'assurer qu'ils sont légitimes. Je n'ai pas de réponse générale à la première partie de votre question.

Tamara Kronis: Y a-t-il des lacunes?

Chris Lynam: Il y a encore beaucoup à faire pour empêcher que les Canadiens soient victimes de sollicitation frauduleuse.

Tamara Kronis: Que recommanderiez-vous au gouvernement fédéral de faire, en tirant profit de notre pouvoir en matière de télécommunications, du côté des mesures positives et concrètes que nous n'avons pas encore adoptées?

Chris Lynam: Je connais assez bien le fonctionnement et les cadres des entreprises de télécommunications, mais, malheureusement, je ne suis pas expert en réglementation des télécommunications et je ne peux donc pas vous donner une réponse éclairée.

Tamara Kronis: Dans ce cas, pourriez-vous profiter des dernières secondes qui nous restent pour donner quelques conseils aux gens de ma circonscription, qui craignent d'être des victimes? Quels sont les signes avant-coureurs et que doivent-ils faire en premier?

Chris Lynam: C'est très simple. C'est l'approche « cinq minutes ». Il y a trois choses à faire: détecter, contrer et signaler la fraude. C'est comme l'approche « arrêter, se jeter par terre et rouler » de ma génération. Nous devons utiliser des termes très simples pour encourager les gens. Prenez seulement cinq minutes pour réfléchir, vous éviterez ainsi la plupart des escroqueries.

Tamara Kronis: Merci beaucoup.

Le président: Merci, madame Kronis.

Madame Begum, vous avez deux minutes et demie.

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

Merci beaucoup, monsieur Lynam, d'être ici. Je vais faire de mon mieux pour aller à la vitesse de la lumière ou de l'Internet.

Au cours des 10 dernières années, des personnes, surtout des personnes âgées, ont signalé des incidents d'escroquerie au porte-à-porte. Que ce soit sous prétexte d'inspecter leur chauffe-eau ou quelque chose d'autre dans leur maison, les victimes se sont retrouvées avec un privilège de 15 000 ou 20 000 \$ sur leur maison. Je sais qu'il y a encore des aînés, aujourd'hui, qui ne s'en sont pas vraiment remis, qui ont dû payer ou qui n'ont pas pu vendre leur propriété à cause de cette fraude.

Premièrement, existe-t-il des mécanismes ou y a-t-il quelque chose que nous pouvons faire pour soutenir les victimes de cette arnaque?

Je vais poser ma deuxième question, parce que je n'ai pas beaucoup de temps. Parallèlement, j'ai l'impression que les jeunes sont aussi ciblés par des types de fraudes similaires, qui ne se font pas au porte-à-porte, mais plutôt sur leurs téléphones. Par exemple, ils reçoivent un message de Starbucks leur proposant un café gratuit et ils cliquent sur « J'accepte ».

J'ai récemment écouté un exposé de Booshra Ahmed, une scientifique des données, qui parlait du coût caché lorsque l'on clique sur « J'accepte ». C'est essentiellement l'avenir de l'intelligence artificielle; comprendre ce qui se passe, comment vos données sont largement partagées et ce que cela implique pour vous.

Que pouvons-nous faire pour soutenir les jeunes au cours des décennies à venir, et comment pouvons-nous éviter d'être victimes de situations semblables?

Merci beaucoup.

Chris Lynam: Je vais aborder la question sous deux angles différents. Je vais commencer par la première partie de votre question.

Bon nombre d'aînés sont parfois victimes de ces escroqueries au porte-à-porte. Et devinez qui a vraiment le tour pour sensibiliser les aînés à la fraude et à la cybercriminalité? Les autres aînés. Nous menons un programme avec des aînés bénévoles que nous formons. Ils animent des présentations en personne. Parfois, nous parlons aux victimes au téléphone et nous leur expliquons comment éviter de se faire escroquer à nouveau. Dans certains cas, elles sont en train d'être victimes d'une escroquerie et elles devraient tout arrêter. Cela revient à ce que je disais sur l'adaptation des campagnes de prévention en fonction du public cible.

En ce qui concerne les jeunes, nous devons adopter une approche sociétale. Cela doit se faire à l'école. Nous devons les rejoindre en ligne. C'est là qu'ils sont, dans une certaine mesure. Les parents doivent expliquer à leurs enfants comment reconnaître une escroquerie ou les dangers auxquels ils s'exposent s'ils envoient des photos à caractère intime. Il faut leur dire: « S'il te plaît, ne fait pas cela, tu vas gâcher ta vie. » J'utilise cet exemple, mais il n'y aura pas d'approche universelle en matière de prévention. Elle doit être adaptée à des publics spécifiques.

• (1300)

Doly Begum: Merci beaucoup.

Le président: Merci beaucoup.

Monsieur Lynam, merci beaucoup d'être ici aujourd'hui. Merci à vous et à la GRC de votre travail constant et de tout ce que vous faites pour mettre fin à la fraude et limiter les risques qui y sont associés. Nous attendons avec impatience toute autre contribution de l'organisation concernant l'élaboration des politiques du gouvernement fédéral.

Chers collègues, je vais suspendre brièvement la séance avant d'accueillir le prochain groupe de témoins. Je tiens à vous dire, pour que les partis puissent en discuter à l'avance, que nous n'aurons pas le temps d'entendre le troisième intervenant dans la prochaine heure. Cela veut dire qu'il y aura deux intervenants du côté des conservateurs et deux intervenants du côté des libéraux. Le temps de M. Ste-Marie sera réduit. Profitez des prochaines minutes pour décider de la façon dont vous voulez procéder.

Encore une fois, monsieur Lynam, merci beaucoup, et bonne journée.

Nous allons brièvement suspendre la séance.

• (1300)

(Pause)

• (1310)

Le président: Nous reprenons nos travaux.

Chers collègues, nous sommes à la troisième et dernière heure de la réunion d'aujourd'hui. Nous accueillons deux nouveaux témoins, un par vidéoconférence et un en personne.

Nous accueillons par vidéoconférence M. Anthony Quinn, président de l'Association canadienne des individus retraités. Nous accueillons en personne M. Colin Smith, vice-président, Sciences du risque et de la décision, de Wealthsimple.

Messieurs, vous aurez au plus cinq minutes pour faire votre déclaration préliminaire, après quoi les membres des partis reconnus assis à la table vous poseront des questions.

Monsieur Quinn, allez-y. Vous avez cinq minutes.

Anthony Quinn (président, Association canadienne des individus retraités): Merci au président et aux membres du Comité de m'avoir invité à comparaître aujourd'hui.

Je m'appelle Anthony Quinn, et je suis président de l'Association canadienne des individus retraités, l'ACIR. Nous représentons plus de 250 000 membres à l'échelle du Canada et défendons les intérêts des aînés canadiens, y compris en matière de sécurité financière, de santé et de protection contre la discrimination fondée sur l'âge.

La fraude peut bouleverser la vie des aînés canadiens. Quand un aîné perd de l'argent à cause d'une escroquerie, il perd souvent toute l'épargne accumulée pour sa retraite au fil des décennies. Le risque particulier auquel sont exposés les aînés victimes de fraude tient au fait qu'il est très difficile, voire impossible, pour eux de réintégrer le marché du travail pour regagner l'argent perdu. Pour la grande majorité des Canadiens âgés, les conséquences de la fraude sont irréversibles.

L'ACIR a récemment sondé nos membres, et plus de 8 000 ont répondu. Plus de 82 % des répondants ont déclaré avoir été ciblés par un fraudeur et près d'un répondant sur cinq a dit avoir perdu de

l'argent en raison d'une fraude. Selon toutes les sources accessibles et fiables, de 5 à 10 % seulement des fraudes sont signalées. Nous croyons donc que l'ampleur réelle du problème est bien plus importante que ce que révèlent nos propres sondages.

Depuis au moins 10 ans, on dit aux Canadiens d'être plus prudents, et les aînés ont reçu le message. Ils ont assisté à des séminaires, écouté les messages d'intérêt public, lu les brochures des banques et appris à se méfier des textos, des appels et des courriels non sollicités.

Les banques, les entreprises de télécommunications, les plateformes numériques, les gouvernements et les organisations de défense des droits, comme la nôtre, ont encouragé les Canadiens à demeurer vigilants, mais les pertes liées à la fraude ne cessent d'augmenter. À un moment donné, le Parlement doit se demander si le fardeau de la prévention n'est pas trop lourd pour les victimes et trop léger pour les institutions par l'intermédiaire desquelles ces escroqueries sont menées.

Du point de vue d'un aîné canadien qui a perdu les économies d'une vie, les programmes de sensibilisation, les discours creux des entreprises, les campagnes de relations publiques et les rappels à la prudence ne suffisent pas. Notre message, pour le Comité, c'est que la prévention de la fraude doit être une responsabilité collective, et non une simple responsabilité individuelle. Cela veut dire que les entreprises de télécommunications doivent en faire plus pour authentifier les appels, prévenir la mystification et bloquer les textos frauduleux avant que les Canadiens les reçoivent. Les plateformes numériques doivent aussi être tenues davantage responsables des publicités frauduleuses, des comptes usurpant l'identité d'une personne, des publicités de faux investissements et des autres escroqueries utilisant leurs systèmes. Peut-être plus important encore, les institutions financières doivent renforcer leurs mécanismes de détection et d'interventions en matière de fraude avant que l'argent ne soit prélevé sur le compte des clients.

Dans le cas qui nous occupe, le Parlement devrait se demander si les mesures de prévention incitatives sont bien adaptées.

Je vais vous donner l'exemple d'un membre de l'ACIR. Peter Squire a 70 ans, et il est un analyste du marché à la retraite, de Winnipeg. Il n'est ni inexpérimenté ni novice en matière de finances. M. Squire a reçu ce qui semblait être un appel légitime de la part d'un expert en investissements. Les documents qui lui ont été envoyés portaient le logo de la banque. Le numéro de téléphone semblait authentique. La proposition semblait légitime. Il a demandé l'aide d'institutions financières reconnues et a fait ce qu'il pensait être un investissement financier sûr. Au lieu de cela, près de 650 000 \$ ont disparu de son fonds de retraite, à la suite d'une fraude sophistiquée.

Ce qui m'a marqué dans l'histoire de Peter, c'est qu'il a fait bon nombre des choses que nous disons aux Canadiens de faire — il a posé des questions, il a fait affaire avec des institutions reconnues et il a demandé l'aide de professionnels —, mais il est tout de même tombé dans le panneau. C'est pourquoi l'ACIR croit que la prévention de la fraude ne peut pas reposer principalement sur la vigilance individuelle. Les systèmes qu'utilisent les escrocs doivent aussi en faire davantage pour empêcher dès le départ qu'ils ne parviennent à leurs fins.

Il y a aussi un autre contraste que de nombreux aînés ont de la difficulté à comprendre. Quand approximativement 20 millions de dollars d'or ont été volés à l'aéroport Pearson de Toronto, la réponse a été collective et immédiate. Les services de police ont été mobilisés. Les autorités fédérales sont intervenues. Les compagnies d'assurance ont lancé des procédures de recouvrement des fonds. Des experts en sécurité ont été mobilisés. Des enquêtes internationales ont été financées et menées. Les autorités canadiennes ont travaillé avec les services de police et des partenaires aux États-Unis, en Inde et dans d'autres pays. L'incident a dominé l'actualité nationale. Des ressources ont été allouées. On a demandé des comptes. Récupérer l'argent volé était une priorité.

Toutefois, quand un aîné perd 650 000 \$ de son épargne-retraite à cause d'une fraude, la réaction peut être très différente. On dit souvent à la victime d'appeler sa banque, puis la police, puis le Centre antifraude du Canada, et, même si on compatit avec sa situation, on lui dit habituellement: « Je suis désolé, mais nous ne pouvons pas faire grand-chose pour vous aider. »

• (1315)

Les aînés canadiens se demandent pourquoi le Canada peut mener des interventions coordonnées au niveau national et international, quand des actifs institutionnels sont détournés, mais que, quand des Canadiens ordinaires perdent des milliards au total, on ne fait pas grand-chose. Du point de vue de la victime, les conséquences sont beaucoup plus dévastatrices. Quand les institutions assument le coût d'une perte, elles ont tendance à adopter une approche plus coordonnée et plus internationale. L'ACIR croit que la prévention, la responsabilisation et la protection des consommateurs doivent être intégrées au système, plutôt que de reposer principalement sur la vigilance individuelle.

J'aimerais ajouter que l'ACIR mène une initiative distincte, mais connexe, sur la concurrence, la transparence et la qualité des conseils en investissement proposés aux Canadiens par l'entremise des canaux d'investissement des succursales. L'année dernière, nous avons directement fait part de nos préoccupations aux banques, aux organismes de réglementation, au Bureau de la concurrence et aux fonctionnaires du ministère des Finances. Nous avons apprécié les discussions constructives que nous avons eues avec le bureau du ministre des Finances. Même si cela est distinct de la discussion d'aujourd'hui sur la fraude et les escroqueries, le principe sous-jacent est semblable. Les Canadiens doivent avoir l'assurance que leur système financier agit dans leur intérêt, que les conflits sont gérés de manière appropriée et que les consommateurs bénéficient d'un traitement équitable et d'une protection digne de ce nom.

Après une décennie où les fraudes et les pertes ne cessent d'augmenter et où les occasions d'agir sont manquées, les aînés canadiens demandent des mesures de protection et une reddition de comptes. Ils demandent des systèmes financiers et des systèmes de communication qui s'efforcent tout autant de prévenir la fraude visant des consommateurs que de prévenir les pertes subies par les institutions elles-mêmes.

Merci. Je suis prêt à répondre à vos questions.

Le président: Merci beaucoup, monsieur Quinn.

Monsieur Smith, vous avez la parole pour cinq minutes.

Colin Smith (vice-président, Sciences du risque et de la décision, Wealthsimple): Merci, monsieur le président.

Merci aux membres du Comité de m'avoir invité aujourd'hui.

Wealthsimple est le plus grand innovateur financier du Canada. Plus de quatre millions de Canadiens nous font confiance, et nous détenons plus de 150 milliards d'actifs. Il est essentiel pour nous de protéger la confiance des Canadiens à notre égard.

À quoi ressemble la fraude aujourd'hui? Nous avons passé des années à renforcer nos systèmes contre les attaques directes, mais les attaques touchent de moins en moins nos systèmes et de plus en plus les gens qui s'en servent. Les clients de toutes les institutions financières se retrouvent en première ligne.

Les attaques qui causent le plus de dommages sont aussi les plus difficiles à détecter, parce que les fraudeurs ne touchent jamais à nos systèmes. Ils incitent plutôt le client à transférer lui-même l'argent, et le client, quant à lui, croit souvent qu'on l'aide. Ce sont de vieilles tactiques, mais ce qui est nouveau, c'est la vitesse. Les fraudeurs clonent à l'aide de l'IA une voix connue ou créent de toutes pièces un document qui a l'air bien réel à l'aide d'outils que n'importe qui peut télécharger, et font en quelques minutes ce qui aurait autrefois pris des semaines.

Cela a modifié la façon dont nous luttons contre la fraude. Nous avons réalisé que la prévention fonctionne mieux quand les gens travaillent avec la technologie. Tout ce que nous faisons en coulisse pour détecter la fraude est jumelé à des outils bien réels qui permettent aux clients de participer à la lutte.

Par exemple, une clé d'accès est une mesure de sécurité plus simple, qui vous permet d'accéder à votre compte à l'aide des données biométriques ou du NIP de votre appareil. Contrairement au mot de passe traditionnel, les clés d'accès sont seulement liées à votre appareil personnel et à Wealthsimple, ce qui veut dire qu'elles ne fonctionneront pas sur de faux sites ou des sites frauduleux. Quand nous avons lancé les clés d'accès, au cours du premier trimestre de l'année, nos clients se sont empressés de protéger plus de 10 milliards de dollars à l'aide de ces clés d'accès.

Un autre nouvel outil, ce sont les emplacements de confiance. Les clients peuvent désigner des endroits, comme le domicile ou le travail, comme étant des emplacements de confiance. Si vous décidez de transférer de l'argent de n'importe quel autre endroit, vous devrez vous soumettre à des vérifications, selon des modalités supplémentaires qui auront été établies. Plus de 500 000 transactions de nos clients ont été vérifiées de cette façon.

Nous protégeons aussi nos clients en communiquant avec eux en temps réel. Si quelqu'un transfère de l'argent à l'aide de notre application pendant qu'il est au téléphone, un avertissement s'affiche pour indiquer que l'appel ne provient pas de nos bureaux. Quand un client semble être victime d'une arnaque, une équipe formée précisément à cette fin, le *spell breakers group*, ou groupe des briseurs de charmes, communique avec lui pour lui parler avant que l'argent ne disparaisse.

Les institutions financières et les clients peuvent travailler ensemble pour lutter contre la fraude, mais la plupart des fraudes ne proviennent pas du système financier. Les institutions financières, les fournisseurs de services de télécommunications et les plateformes de médias sociaux doivent travailler ensemble pour prévenir les fraudes, surtout depuis que l'IA accélère ces arnaques.

De nombreuses tentatives de fraude contre nos clients commencent sur les médias sociaux, où les fraudeurs se servent de notre nom et de notre logo pour afficher des publicités frauduleuses qui entraînent des Canadiens dans des arnaques comme le stratagème de manipulation des cours boursiers. Entre octobre 2025 et janvier 2026, nous avons signalé plus de 10 000 publicités de ce genre sur les plateformes Meta. Durant cette période, quatre jours se sont écoulés en moyenne entre le moment du signalement à Meta et le retrait de ces publicités.

Récemment, nous avons relevé et signalé 1 500 publicités frauduleuses en un seul jour. Nous faisons ce que nous pouvons pour protéger nos clients de ces arnaques. Nous avons construit un système fondé sur l'IA pour identifier, en temps réel, les actions qui font peut-être partie d'un stratagème de manipulation des cours boursiers et qui avise automatiquement nos clients qui pourraient s'approprier à les acheter.

Signaler les publicités l'une après l'autre, c'est un jeu perdu d'avance. Les plateformes ne semblent pas encore avoir réglé le problème, et Meta ne semble pas non plus avoir adopté de politiques pour régler le problème. La solution durable est de demander aux entreprises de médias sociaux de vérifier que tous les annonceurs de services financiers sont des entités légitimes et réglementées, comme le font déjà les États-Unis, le Royaume-Uni, l'Australie, Hong Kong et six autres pays. C'est la recommandation centrale du mémoire que nous avons présenté à propos de la Stratégie nationale antifraude du gouvernement.

Nous saluons l'engagement du gouvernement et de votre comité à vouloir protéger les Canadiens. La fraude ne ralentira pas.

Ce qui me donne espoir, c'est que nos clients ont montré qu'ils voulaient eux-mêmes être des partenaires actifs de leur propre protection, et c'est avec ce type de partenariats que nous pourrions protéger les Canadiens.

Merci. J'ai hâte de répondre à vos questions.

• (1320)

Le président: Merci beaucoup, monsieur Smith.

Je vais profiter de cette rare occasion pour poser une question, parce que vous avez piqué mon intérêt en parlant d'un sujet qui a été abordé plus tôt cette semaine dans un témoignage.

Combien de jours avez-vous dit que Meta a pris pour retirer une publicité frauduleuse que vous lui avez signalée?

Colin Smith: Durant cette période, c'était en moyenne quatre jours.

Le président: Est-ce que Meta a reconnu d'emblée qu'il s'agissait d'une fraude ou l'entreprise s'est-elle justifiée en disant qu'elle n'était pas certaine qu'il s'agissait d'une fraude?

Colin Smith: Nous avons demandé à ce que des publicités fassent l'objet d'une vérification, et ce processus de vérification — qui se fait à l'interne et vise à déterminer si une publicité est frauduleuse — prenait quatre jours.

Le président: D'accord.

Je suis convaincu que d'autres députés auront des questions de suivi à cet égard. Sinon, je pourrais y revenir à la toute fin.

Sur ce, madame Borrelli, vous avez la parole pour six minutes.

Kathy Borrelli: Bienvenue à nos témoins. Merci d'être ici aujourd'hui pour cette étude importante.

Ma première question s'adresse à M. Quinn.

De nombreux aînés sont ciblés par des arnaques mettant en scène par du faux personnel de soutien technique ou de faux représentants d'une banque, qui convainquent la victime d'installer un logiciel d'accès à distance. Une fois que c'est fait, l'arnaqueur peut inciter la victime à se départir de toutes ses économies.

Les banques ou les plateformes de paiement devraient-elles ajouter des mesures de vérification supplémentaires ou retenir temporairement l'argent quand on tente d'effectuer des paiements à risque élevé à partir d'un appareil auquel on semble avoir accédé à distance?

Anthony Quinn: Merci de la question.

Je crois effectivement que les banques devraient assumer une plus grande responsabilité au regard de ces pertes. Habituellement, les arnaques ne supposent pas que l'argent soit remis en main propre. Les arnaqueurs doivent se servir des systèmes électroniques détenus et exploités par les banques. L'argent est habituellement transféré d'une institution à une autre à l'aide de leurs systèmes. Nos membres croient que les institutions financières devraient assumer une plus grande responsabilité. Sinon, l'éducation à elle seule — malgré les efforts communs — ne sera pas suffisante pour prévenir les fraudes et les arnaques, et nous n'avons aucun moyen de récupérer l'argent.

Kathy Borrelli: Merci, monsieur Quinn.

L'un des enjeux, c'est que nous devons protéger les aînés de la fraude, mais sans les traiter comme s'ils étaient incapables de gérer leur propre argent. La solution, quelle qu'elle soit, doit protéger l'indépendance tout en freinant la manipulation à risque élevé.

Quel genre de mesures de sécurité vos membres accepteraient-ils? Je pense à des personnes de confiance, des limites de transactions optionnelles, l'imposition d'un délai sur les transferts inhabituels ou ce genre de choses.

• (1325)

Anthony Quinn: Nous voulons toujours éviter d'avoir une attitude paternaliste envers les personnes âgées et de leur donner l'impression de leur retirer le contrôle de leurs propres décisions financières. Nous devons trouver un équilibre entre cela et les pressions exercées par les fraudeurs pour encourager les victimes à prendre rapidement une décision concernant une offre limitée ou dans une situation d'urgence, comme dans l'arnaque des grands-parents, où le petit-enfant a des problèmes avec la loi ou des problèmes de santé.

Je crois que nos membres accepteraient volontiers de perdre un peu de ce contrôle en échange d'un délai de transfert si cela veut dire qu'ils sont protégés par les banques et qu'ils peuvent s'assurer que le transfert est légitime.

Kathy Borrelli: Pensez-vous que l'on devrait mettre en place, avec les banques, les plateformes, les services de télécommunications et la police, un service de première ligne bien précis pour les aînés victimes de fraude, comme un centre à qui elles pourraient s'adresser lorsqu'elles se font voler de l'argent?

Anthony Quinn: Nous avons parlé au Centre antifraude du Canada. Il nous dit qu'il ne peut pas répondre à la plupart des appels téléphoniques entrants. Il demande aux personnes victimes d'arnaques de remplir les formulaires en ligne. Elles sont arnaquées en ligne. Elles essaient de communiquer avec la GRC et d'autres forces de police, qui leur disent de remplir des formulaires en ligne. Nous avons besoin d'une réaction immédiate des banques, si elles sont en mesure de récupérer l'argent.

Il est beaucoup plus important de s'assurer que les banques essaient d'empêcher la fraude, au départ, que de mettre en place un service où les aînés peuvent signaler une fraude après coup. Le problème, à l'heure actuelle, c'est qu'il est trop tard, et tout le monde compatit. Les gens ont l'impression que le système ne les protège pas vraiment.

Kathy Borrelli: Au cours de la dernière heure, nous avons discuté avec Chris Lynam, du Centre antifraude du Canada. Il nous a dit que le Centre antifraude avait créé un programme où les aînés s'aidaient les uns les autres. Connaissez-vous ce programme? Savez-vous s'il donne des résultats?

Anthony Quinn: Il s'agit sans doute seulement d'un programme de prévention de la fraude parmi des milliers d'autres mis en œuvre au Canada. Ce que nous voulons faire comprendre aujourd'hui, c'est que l'éducation n'est qu'une petite partie du problème. Ce n'est manifestement pas efficace. Même ceux qui sont informés finissent par être victimes de fraude. Les institutions doivent jouer un rôle plus important pour protéger les aînés de ces fraudes.

Kathy Borrelli: Je reçois beaucoup de demandes d'information. Je reçois beaucoup de courriels et d'appels de personnes âgées victimes de ces fraudeurs. Vers qui devrions-nous les orienter? Comment puis-je les aider?

Anthony Quinn: J'aimerais pouvoir vous répondre, madame.

Nous demandons au Parlement de prendre les choses en main, d'encourager et peut-être d'obliger les institutions à jouer un rôle plus important, d'investir dans l'application de la loi et d'augmenter les amendes et les peines dans notre pays afin de dissuader les fraudeurs.

Kathy Borrelli: Qu'est-ce qui est le plus important selon vous? Que demandez-vous le plus au gouvernement?

Anthony Quinn: Ma demande la plus importante, c'est que les institutions, surtout les banques et les services de télécommunications, aient une plus grande part de responsabilité dans ce dossier, et qu'elles fassent partie de la solution pour prévenir les fraudes. Je crois que si elles étaient comptables d'une partie de ces pertes, cela les inciterait davantage à prendre les mesures qui s'imposent.

Kathy Borrelli: Merci, monsieur Quinn.

Anthony Quinn: Merci.

Le président: Merci beaucoup, madame Borrelli.

Je crois que c'est maintenant au tour de M. Fanjoy qui partagera son temps avec M. Bains. Je vais vous laisser départager le temps entre vous.

Vous avez la parole pour six minutes, monsieur Fanjoy.

Bruce Fanjoy (Carleton, Lib.): Merci, monsieur le président.

Je suis très heureux de voir que l'Association canadienne des individus retraités est présente. Je suis convaincu que tout le monde autour de la table a dans sa famille des personnes vieillissantes, qui deviennent plus vulnérables aux crimes financiers complexes. Nous

souhaitons tous les protéger tout en respectant leur indépendance et leur autonomie.

J'aimerais savoir ce que nous pourrions faire, selon vous, pour nous assurer de ne pas leur enlever leur indépendance tout en les protégeant activement, sachant que certains aînés souffrent de démence, sans avoir reçu de diagnostic, ce qui les rend particulièrement vulnérables.

● (1330)

Anthony Quinn: Merci beaucoup.

Les fraudeurs se servent d'astuces et de pièges psychologiques de plus en plus convaincants pour entraîner les Canadiens dans leurs arnaques. Ce n'est pas nécessairement lié à des problèmes cognitifs. C'est sans doute davantage lié à une surestimation de nos connaissances et de notre capacité d'interpréter nos décisions financières. Je pense que nous devons examiner ce qu'ont fait d'autres pays qui ont fourni plus d'efforts pour protéger leurs aînés, outre l'éducation, comme les États-Unis et le Royaume-Uni, et vraiment encourager...

Encore une fois, estimés parlementaires, il faut demander aux institutions, surtout aux banques et aux services de télécommunications, de jouer un rôle plus important dans la protection des Canadiens, et il ne faut pas oublier que les aînés sont ceux qui se font voler le plus d'argent. Il faut fixer des exigences et les rendre responsables des pertes financières si elles ne prennent pas ces dispositions et qu'elles ne mettent pas en place ces mesures de protection pour prévenir les fraudes. Si on exige cela d'elles, elles seront sans doute plus encouragées et disposées à protéger davantage les Canadiens.

Bruce Fanjoy: Merci.

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

Parm Bains: Merci, monsieur Fanjoy.

Merci aux témoins de s'être joints à nous. Je vais essayer de poser mes questions rapidement.

Monsieur Quinn, je suis originaire de Richmond, en Colombie-Britannique. L'espérance de vie dans cette région est la plus longue au Canada, et beaucoup d'aînés y vivent.

Je sais que vous avez parlé des services de télécommunications. D'autres témoins nous ont parlé aujourd'hui de la complexité des stratagèmes de fraude et d'arnaque. Vous avez parlé de l'aspect émotif des choses et avez souligné que les fraudeurs sont de plus en plus habiles. Nous avons aussi entendu parler de la solitude. Les fraudeurs ciblent les gens seuls. Pourriez-vous nous parler de quelques lacunes précises et formuler des recommandations pour aider notre agence contre les crimes financiers à l'avenir? Lui avez-vous présenté des observations?

Aussi, quand un appel semble être frauduleux, les services de télécommunications le signalent. Aimerez-vous que le système bancaire soit doté, d'une façon ou d'une autre, d'un système d'alerte?

Anthony Quinn: Je pense que tout ce que vous avez dit est vrai, monsieur.

Nous n'essayons pas de dire que les banques et les services de télécommunications ne font rien, mais ils pourraient certainement en faire plus. Nos téléphones affichent une alerte indiquant qu'il pourrait s'agir d'un appel frauduleux, mais ce système d'alerte laisse tout de même passer beaucoup d'appels. Pour ce qui est des médias sociaux, comme mon collègue de Wealthisimple l'a mentionné, il y a littéralement un déluge de publicités fausses et trompeuses sur les médias sociaux, et beaucoup d'ânés consultent ces plateformes pour obtenir de l'information et passer le temps.

Pour ce qui est des lacunes, je dirais que j'aimerais que les parlementaires adoptent une approche énergique pour réglementer les institutions, par le truchement du CRTC et du contrôle que vous exercez sur les institutions financières, pour les amener à jouer un rôle plus important.

Nous ne pouvons pas demander aux victimes, les ânés et les jeunes Canadiens, d'être des experts dans tous ces domaines en développement, mais nous devrions exiger que ces grandes institutions nationales, qui n'ont aucune concurrence et qui gagnent des milliards de dollars de revenus par année grâce aux Canadiens, soient de vrais partenaires et nous protègent des fraudeurs.

Parm Bains: Merci. Je crois que mon temps est écoulé.

Le président: Merci beaucoup, monsieur Fanjoy et monsieur Bains.

[Français]

Monsieur Ste-Marie, c'est à vous pour six minutes.

Gabriel Ste-Marie: Oui, merci, monsieur le président.

Je remercie les deux témoins de leur présence.

Monsieur Smith, vous nous dites que d'autres pays imposent aux plateformes numériques, comme celles de Meta, de vérifier l'authenticité des entreprises qui offrent des services financiers via leurs publicités, et vous demandez que ce soit fait ici aussi. Est-ce que c'est bien ça?

• (1335)

[Traduction]

Colin Smith: Oui, c'est cela. Vous pouvez consulter sur le site de Meta la liste des pays qui exigent une vérification supplémentaire des publicités qui concernent un certain nombre de secteurs, y compris les services financiers. Meta a la capacité technique de le faire, mais l'entreprise a décidé de ne pas faire cela au Canada.

[Français]

Gabriel Ste-Marie: Je suis estomaqué.

Est-ce que vous savez si les autres pays qui ont ces vérifications plus sévères ont vu ce type de fraude diminuer auprès de leur population?

[Traduction]

Colin Smith: À ma connaissance, oui. Je ne connais pas très bien les statistiques des autres pays, mais cette étape de vérification est assurément importante. Dans les cas où on a usurpé l'identité de Wealthisimple, on parle de situations extrêmes où des hypertrucages ont mis en scène notre PDG qui proposait des actions aux Canadiens. C'est clairement du matériel frauduleux qui se sert de notre marque.

[Français]

Gabriel Ste-Marie: C'est vraiment préoccupant. Merci beaucoup.

Est-ce que vous savez pourquoi Meta n'offre pas ce processus de vérification supplémentaire au Canada? Est-ce que, dans les autres pays, ça a dû passer par l'adoption d'une loi ou d'un règlement, ce que le gouvernement n'a pas encore fait ici?

Est-ce que vous estimez que le fait que ce processus ne soit pas mis en place ici constitue une forme de laxisme de la part des plateformes numériques?

[Traduction]

Colin Smith: Oui, je crois que, si cela n'a pas été mis en place ici, c'est parce que cela complexifie le processus d'affichage de publicités sur la plateforme. Je crois réellement que le gouvernement pourrait faire quelque chose à cet égard.

[Français]

Gabriel Ste-Marie: Je vous remercie beaucoup.

Monsieur Quinn, je vous remercie beaucoup de votre présence aussi.

On entend trop d'histoires d'horreur comme celle à laquelle vous avez fait référence et où des ânés se retrouvent avec des comptes vidés des économies d'une vie, sans que rien soit fait. Ça doit changer. Il y a beaucoup de cas dans les médias au Québec, dans les émissions d'affaires publiques, qui relatent les stratagèmes qui ont eu lieu. Ça fait déjà quelques années. Ça bouge très lentement.

De votre intervention, j'ai bien retenu qu'il faut davantage tenir de façon responsable les entreprises de télécommunications, les institutions financières et les plateformes numériques. À ce sujet, j'aimerais avoir votre avis sur la question de responsabilité civile. Si quelqu'un s'est fait frauder et qu'il y a des motifs raisonnables de croire que la plateforme où la publicité a été affichée a été négligente, est-ce que la plateforme devrait être tenue coresponsable?

[Traduction]

Anthony Quinn: Je ne crois pas pouvoir dire le contraire, monsieur.

Nous sommes rendus à un point au Canada où nous reprochons aux victimes de ne pas s'être renseignées suffisamment ou de ne pas être suffisamment au courant. Je pense que nous devons renverser les rôles pour protéger les Canadiens. Et s'il faut demander aux plateformes elles-mêmes, aux services de télécommunications, aux fournisseurs de services numériques ou aux institutions financières, de rendre des comptes, je ne crois pas que nos membres s'y opposeraient.

[Français]

Gabriel Ste-Marie: Je vous remercie. Évidemment, on parle de crimes ici: c'est criminel, ce qui est fait et ces vols.

Plus tôt cette semaine, Meta est venue nous dire qu'elle faisait beaucoup d'efforts pour réduire les publicités frauduleuses, même s'il faut quatre jours en moyenne pour les retirer une fois signalées. En plus, comme vous l'avez dit, il y a un déluge de fausses publicités sur ces plateformes. On a aussi entendu dire que peut-être 10 % des publicités sont frauduleuses, mais que Meta en tire un revenu.

Selon vous, à partir de quel pourcentage de publicités considérées comme frauduleuses une organisation devrait-elle être désignée comme une organisation criminelle?

• (1340)

[Traduction]

Anthony Quinn: Il me serait difficile de parler du pourcentage, mais, quand nous savons que la majorité de ces crimes sont commis par l'entremise de Meta et d'organisations similaires, je pense que nous devons leur imposer des normes plus élevées, leur demander de faire partie de la solution et les empêcher de servir d'entonnoir par où passent ces criminels nationaux et internationaux.

[Français]

Gabriel Ste-Marie: Je vous remercie.

Monsieur le président, je vous cède les 10 secondes de temps de parole qui me restent.

Le président: Il vous restait environ 15 secondes. Comme toujours, je vous remercie de votre générosité, monsieur St-Marie.

[Traduction]

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

Tamara Kronis: Merci beaucoup.

Monsieur Smith, je vais vous poser quelques questions.

J'ai trouvé votre explication excellente, lorsque vous avez dit que le système s'en prend désormais aux utilisateurs — et non aux systèmes eux-mêmes —, en amenant les clients à transférer leur argent. Bien entendu, ce qui pose le plus problème, ici, c'est que cela se produit à la vitesse d'Internet. On fait beaucoup d'efforts pour obtenir les données, après les faits, mais à ce stade, la prévention est généralement réactive. C'est bien cela?

Colin Smith: Pour remédier à ce problème, Wealthisimple songe à intégrer des éléments de sécurité directement dans l'expérience client, dans notre application, pour qu'ils fassent partie des interactions entre nos clients et Wealthisimple. Nous ne gérons pas uniquement des règles et des modèles relatifs à la fraude à l'arrière-plan.

Tamara Kronis: Bien entendu, le plus difficile pour vous, c'est que les institutions financières sont au premier plan dans tout cela. Lorsqu'une personne s'aperçoit qu'elle a été victime d'une escroquerie, c'est d'abord son institution financière qu'elle appelle. Dans de nombreux cas d'investissements frauduleux, une fois que l'argent a été envoyé, surtout s'il s'agit de cryptomonnaie ou d'un type de plateforme à l'étranger, il est virtuellement impossible de le récupérer, n'est-ce pas?

Colin Smith: C'est généralement vrai. Nous essayons de le récupérer au nom de nos clients, dans des cas de fraude, mais cela risque évidemment d'être compliqué.

Tamara Kronis: En ce qui concerne les systèmes, vous essayez vraiment d'être proactifs, mais, du point de vue de la loi, le système lui-même dépend toujours vraiment du signalement fait par la victime de fraude après les faits. C'est bien cela?

Colin Smith: Je ne pense pas que ce soit tout à fait juste. Nous prenons beaucoup de mesures proactives au nom de nos clients. Nous plaçons, par exemple, des avertissements sur l'application, lorsque nous remarquons quelque chose de suspect avant que le client n'effectue une transaction. Par exemple, lorsqu'un client essaie d'envoyer de la cryptomonnaie pour la première fois, un écran d'attente impossible à ignorer s'affiche et met en garde contre les

types de fraudes les plus courantes liées aux cryptoactifs, et le client doit l'accepter avant de poursuivre.

Nous réfléchissons certainement à la manière dont nous pouvons être davantage proactifs, malgré la loi que vous avez mentionnée.

Tamara Kronis: C'est très utile de le savoir.

En tant qu'institution financière, avez-vous un moyen quelconque de surveiller des choses comme les annonces d'investissements considérables, à part demander à quelqu'un d'agir comme un utilisateur?

Colin Smith: En ce qui concerne les publicités elles-mêmes, nous en signalons tous les jours. Il s'agit d'un processus incroyablement manuel et chronophage, où nous recherchons de nouvelles publicités utilisant notre marque de commerce ou notre nom de marque, et nous les signalons aux plateformes de médias sociaux. Nous avons donc été obligés de bâtir une infrastructure plus sophistiquée dans la partie interne.

Vu que nous ne pouvons pas empêcher les publicités d'apparaître, nous nous intéressons plutôt aux clients qui réalisent des investissements sur nos plateformes et à la manière dont les gens parlent de ces actions sur les réseaux sociaux ou dans les nouvelles, car c'est cela que nous pouvons contrôler. En combinant ces différents signaux, nous pouvons avertir les clients avant qu'ils n'investissent dans quelque chose qui pourrait être une fraude.

Tamara Kronis: Lorsque vous parlez des choses que vous pouvez contrôler, y a-t-il quelqu'un qui a un contrôle sur ces publicités frauduleuses et qui sait si elles vont apparaître? Est-ce que ce sont les entreprises de télécommunications? Qui est le mieux placé pour empêcher cela?

Colin Smith: Ce sont les plateformes de médias sociaux.

Tamara Kronis: Selon vous, quel serait le moyen le plus efficace pour nous, étant le pouvoir du fédéral sur les télécommunications, de réunir toutes les parties et de les obliger à régler certains des problèmes que M. Quinn a mentionnés et à trouver des solutions en cas de pertes?

• (1345)

Colin Smith: Avant tout, il faudrait obliger les plateformes de médias sociaux à confirmer que tous les annonceurs de services financiers sont légitimes et vérifiés, ce serait très utile. Ce qui se passe, c'est que ces publicités sont très rapidement affichées sur une foule de comptes, et tous les annonceurs, sans exception, utilisent quelque chose comme le logo ou le nom de marque de Wealthisimple, alors qu'ils ne sont aucunement associés à nous.

Tamara Kronis: Pour essayer de régler certains des problèmes en ligne, le gouvernement propose des mesures dans un certain nombre de projets de loi, ce qui est parfois difficile à suivre. Y a-t-il quoi que ce soit dans une loi en vigueur qui permet vraiment d'aller au cœur du problème?

Colin Smith: Pas que je sache, non.

Tamara Kronis: Merci beaucoup.

Le président: Merci beaucoup, monsieur Kronis.

Madame O'Rourke, il me semble que vous vouliez partager un peu de votre temps avec M. Ma, donc je vais vous laisser voir cela entre vous.

La parole est à vous deux, et vous avez cinq minutes.

Dominique O'Rourke: Merci, monsieur le président.

Monsieur Smith, quel plaisir d'entendre parler de votre équipe de rompeurs de charmes et de vos mesures proactives.

J'aimerais revenir en arrière. Vous dites avoir détecté 1 500 publicités d'investissements frauduleuses en un seul jour, sur la même plateforme. Vous les avez signalées, et les éliminer prend, en moyenne, quatre jours. C'est étonnant, car Meta peut bloquer la publication de n'importe quelle nouvelle, donc c'est assez choquant à entendre pour le Comité.

Vous êtes une entreprise de technologie financière légitime et réglementée. Avant tout, vous êtes numérique, donc je suppose que vous devez prouver que vous êtes une plateforme légitime avant d'y faire de la publicité. Quel seuil serait approprié pour que les annonceurs prouvent leur légitimité?

Colin Smith: Il devrait être identique à celui des autres publicités vérifiées affichées sur les autres plateformes, c'est-à-dire que, pour n'importe quelle plateforme publicitaire, vous savez qui paie, et cela doit correspondre au nom de la marque apparaissant dans la publicité, en particulier dans des secteurs comme les services financiers.

Dominique O'Rourke: Une entreprise d'une taille industrielle comme celle-ci devrait-elle avoir les outils pour cela?

Colin Smith: C'est ce qu'elles font dans les autres pays, oui.

Dominique O'Rourke: C'est formidable. Merci.

Je cède mon temps à M. Ma.

Michael Ma: Merci beaucoup.

Monsieur Smith, vous avez parlé tout à l'heure du fait que les plateformes devaient vérifier les publicités, et vous avez également mentionné que cela se faisait au moyen des paiements, entre autres.

Pourquoi pensez-vous que les plateformes comme Meta prennent quatre jours pour les supprimer, alors que cela leur prend à peu près une heure pour supprimer des articles de nouvelles?

Colin Smith: Mon hypothèse, c'est que ces publicités génèrent un revenu. C'est comme n'importe quoi sur cet espace. Vous devez en tenir compte.

Michael Ma: Merci.

Ma prochaine question s'adresse à M. Quinn.

Vous avez mentionné, dans vos déclarations liminaires, que les institutions financières devaient en faire plus au chapitre de la prévention de la fraude. Pourriez-vous également parler des rôles que les plateformes de médias sociaux devraient jouer plus souvent pour mieux prévenir la fraude?

Anthony Quinn: J'ai mis l'accent sur les institutions financières en particulier, car c'est à par elles que l'argent est transféré. Le premier contact avec la fraude se passe probablement par l'entremise d'une publicité sur Facebook, où quelqu'un se fait passer pour un représentant de Wealthisimple ou pour le premier ministre et fait l'éloge d'une occasion d'investissement « trop belle pour être vraie ». Au moment de la transaction financière, comme dans le cas de nos membres, l'argent, qui est confié à une institution financière fiable, est prélevé du compte en banque de la personne ou de l'ainé et transféré aux frais de la banque.

C'est pour cela que je me suis davantage focalisé sur les institutions financières, plutôt que sur les annonceurs ou les diffuseurs du message, mais ces derniers nous préoccupent autant que les institutions financières.

Michael Ma: Merci.

À ce propos, pourriez-vous nous parler de l'importance de la sensibilisation du public, comme le représentant de la GRC l'a mentionné tout à l'heure, à la lutte contre la fraude financière et les escroqueries visant, en particulier, les aînés et les retraités?

Anthony Quinn: Il ne fait aucun doute que la sensibilisation et l'éducation sont importantes et probablement les plus faciles à faire. C'est pour cela que le Canada a surtout misé sur l'éducation, ces 10 dernières années, mais les fraudes et les arnaques n'ont cessé d'augmenter, même à mesure que l'éducation a augmenté. L'Association canadienne des individus retraités pense que nous devons maintenant nous focaliser sur les institutions financières et les entreprises de télécommunications en les obligeant à assumer une responsabilité plus grande, de façon qu'elles feront tout ce qui est en leur pouvoir — et avec un peu de chance, le Parlement fera également pression — pour protéger les Canadiens contre les fraudes et les arnaques.

● (1350)

Michael Ma: Merci.

À ce propos, monsieur Quinn, l'ACIR a envoyé au gouvernement une lettre pour demander une meilleure coordination fédérale, une application plus stricte de la loi, et des mesures plus efficaces pour demander des comptes aux banques. En quoi les mesures à venir visant à combattre la fraude financière, comme la stratégie antifraude, les modifications à la Loi sur les banques et l'Agence contre les crimes financiers, démontrent-elles un progrès considérable dans la protection des aînés et des personnes retraitées contre la fraude financière et les escroqueries?

Anthony Quinn: Je dirais que ces mesures sont un signe que le gouvernement commence à y accorder plus d'attention et à agir, mais nous devons encore voir le fruit de bon nombre de ces programmes embryonnaires. Je voudrais qu'ils aient plus de poids dans les poursuites. De nombreux criminels s'en tirent à bon compte, sous prétexte qu'ils ont volé moins de 5 000 \$ ou que les crimes qu'ils ont commis sont moins graves, alors qu'ils continuent de voler des millions de dollars chaque année. L'Association demande au gouvernement d'agir en sévissant contre les criminels et en imposant des mesures de protection aux institutions.

La troisième chose que j'ajouterais, c'est que la police ne peut pas aller d'une province à l'autre pour pourchasser ces criminels à l'intérieur du pays. Nous savons à quel point il est difficile de traverser les frontières internationales, mais, même à l'intérieur du Canada, la police et les victimes nous disent qu'un criminel à Vancouver vole de l'argent à une victime à Saint John. Or, la police ne peut pas agir, même si elle sait qui, où et pourquoi le crime a été commis.

Michael Ma: Merci, monsieur le président.

Le président: Merci, monsieur Ma.

[Français]

Monsieur Ste-Marie, je vous donne la parole pour une minute et trente secondes.

Gabriel Ste-Marie: Merci, monsieur le président.

Monsieur Smith, actuellement, en cas de fraude où quelqu'un fait une transaction non autorisée, c'est l'institution financière qui devrait payer.

Dans le contexte d'un système bancaire ouvert, il y a un risque que l'institution financière et la plateforme d'échange se relancent la balle, ou encore que l'entreprise de finance technologique n'ait pas les moyens de payer. Comment alors s'assurer que le consommateur n'est pas perdant?

[Traduction]

Colin Smith: Dans le monde du système bancaire ouvert, je pense que les consommateurs profiteront beaucoup de la liberté de communiquer leurs renseignements à plusieurs institutions d'avantage qu'à l'heure actuelle, grâce, entre autres, à la liaison bancaire, ce qui dans certains cas posera un plus gros problème pour la sécurité du compte. D'après moi, je ne pense pas qu'il serait risqué de modifier la responsabilité ou les paiements en cas de fraude, comme vous le demandez. Nous nous attendons à ce que les choses restent généralement inchangées et que toutes les institutions financières réglementées faisant partie du système bancaire ouvert continuent de se plier aux mêmes obligations.

[Français]

Gabriel Ste-Marie: Nous pourrions en discuter à un autre moment.

Merci, monsieur le président.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

Je prendrai une minute pour poser deux questions très brèves, ici.

La première s'adresse à vous, monsieur Smith. Cela fait maintenant plusieurs fois que, pendant la séance, puisque vous l'avez mentionné dans vos déclarations liminaires, que l'on fait référence à la réaction tardive de Meta quand une fraude lui est signalée par votre organisation. Pourriez-vous nous faire part publiquement du contenu d'une conversation que vous auriez eue avec des organismes financiers similaires qui auraient constaté le même type de retard, dans ce type de fraude?

Colin Smith: Je pense que nous pourrions faire un suivi de cette question par écrit, avec des discussions similaires. Effectivement, c'est certainement quelque chose dont nous avons discuté au sein de l'industrie.

Le président: C'est apprécié. Je vous encouragerais, dans la limite du raisonnable, à peut-être réunir certains de vos collègues qui occupent des postes similaires afin de discuter de leurs expériences, et si vous le désirez, de fournir au Comité un rapport plus détaillé sur votre expérience collective avec Facebook, en particulier, par rapport à cela. Ce serait très apprécié.

Ma dernière question s'adresse à vous, monsieur Quinn.

Encore une fois, en ce qui concerne Meta, vos membres vous ont-ils fait part de leurs expériences, lorsqu'ils voient une fraude sur Facebook? Prennent-ils contact avec Facebook? Facebook leur envoie-t-il un message pour dire: « Nous souhaitons vous informer qu'il se peut que vous soyez victime d'une fraude »? Vos membres demandent-ils du soutien ou une orientation à Facebook, et si oui, Facebook leur répond-il d'une manière ou d'une autre?

Pourriez-vous brièvement nous donner un aperçu de la relation qui existe entre les aînés du Canada et Facebook, selon vous, quant aux activités frauduleuses qui émanent de sa plateforme?

Merci, monsieur Quinn.

• (1355)

Anthony Quinn: Merci, monsieur le président.

Ni Facebook ni Meta n'ont fait d'efforts délibérés pour communiquer avec les aînés.

La majorité de nos membres qui interagissent avec nous le font par l'entremise de Facebook. Chaque publication que nous mettons sur Facebook est ciblée par les escrocs, car ils savent que les aînés se réunissent sur notre page Facebook, et les fraudes suivent directement la piste de nos publications et des discussions de nos membres. Des arnaques amoureuses aux occasions financières en passant par les offres d'emploi, tout est une escroquerie qui se retrouve directement dans les discussions de nos membres.

Je ne pense pas que Facebook ou Meta agissent proactivement pour protéger les aînés du Canada.

Le président: Monsieur Quinn, j'ai une dernière question de suivi.

Verriez-vous un intérêt à utiliser le témoignage que vous avez fourni aujourd'hui, avec celui de M. Smith et les questions que les membres du Comité vous ont posées, pour publier quelque chose de votre organisation sur Facebook, au cours de la prochaine semaine ou de la semaine suivante, en demandant à Facebook de faire suivre le message, au moyen de ses algorithmes et capacités complexes, et en le mettant au défi pour voir s'il est prêt à le faire? Est-ce quelque chose que vous seriez prêt à faire?

Anthony Quinn: Je suis certainement disposé à faire cela, monsieur le président. Je demanderais l'appui de vos gentils bureaux et, peut-être, de quelques experts. Nous ne sommes pas des experts technologiques à ce chapitre, mais nous sommes prêts à faire tout ce que nous pouvons pour discuter avec Facebook et l'encourager à prendre des mesures proactives. Nous serions ravis de participer.

Le président: Monsieur Quinn, je vous donne ma parole — je ne peux pas parler au nom des autres députés ici présents — que, si je vois que l'Association canadienne des individus retraités publie, dans les prochains jours ou les prochaines semaines, quoi que ce soit pour demander directement que Facebook prenne plus de responsabilités pour lutter contre les fraudes qui sévissent sur sa plateforme, et si je vois que vous ou vos membres lancez un appel à l'action, je me ferai un plaisir et un point d'honneur d'utiliser mes réseaux sociaux pour faire passer le message.

Sur ce, monsieur Smith et monsieur Quinn, merci beaucoup de votre présence aujourd'hui. Vous nous avez aidés à mieux comprendre l'étendue du problème auquel nous sommes confrontés. Continuer d'entendre ces histoires est assez tragique. L'histoire la plus tragique, justement, est celle de la vie détruite d'une personne qui a travaillé pendant des décennies pour construire un nid pour sa famille et elle afin de profiter du temps qu'il lui reste dans notre pays. Nous ferons de notre mieux pour agir, et vos conseils nous seront d'une très grande utilité, à ce chapitre.

Sur ce, merci, messieurs.

Chers collègues, je vous rappelle rapidement que, lundi prochain, le ministre Solomon sera des nôtres pour parler de notre stratégie relative à l'IA. Mardi, nous finaliserons le rapport sur les fabricants de moules sur lequel nous avons travaillé, je l'espère, et nous entendrons les deux ou dernières heures de témoignages liés à cette étude.

Sur ce, je vous souhaite à toutes et à tous une belle fin de semaine. La séance est levée.

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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