



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

45^e LÉGISLATURE, 1^{re} SESSION

Comité permanent de l'industrie et de la technologie

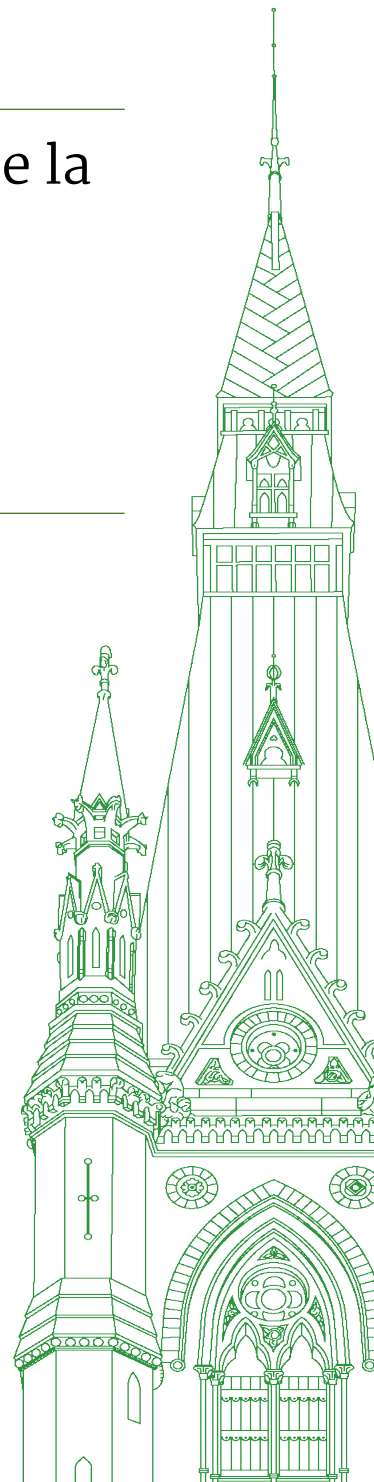
TÉMOIGNAGES

NUMÉRO 046

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le mardi 16 juin 2026

Président : Ben Carr



Comité permanent de l'industrie et de la technologie

Le mardi 16 juin 2026

• (1530)

[Français]

Le président (Ben Carr (Winnipeg-Centre-Sud, Lib.)):
J'ouvre maintenant la séance.

Bon après-midi, tout le monde.

[Traduction]

Nous poursuivons notre étude sur les fraudes. Nous tiendrons une autre réunion après celle-ci. Elle aura lieu jeudi, comme il en a été convenu lors de notre réunion d'hier.

Pour commencer, j'ai quelques questions d'ordre administratif à régler.

Je rappelle aux témoins qui sont dans la salle que si leur oreillette pour l'interprétation est branchée, mais qu'elle n'est pas dans leur oreille, il faut la placer sur l'autocollant devant eux, afin de protéger la santé et le bien-être de nos interprètes.

[Français]

Je peux confirmer que nous avons fait tous les tests pour confirmer que les appareils audiovisuels fonctionnent correctement.

[Traduction]

Chers collègues, mon calendrier indique — il se peut que ce soit erroné, selon ce qui se passe à la Chambre — qu'il est possible que la sonnerie retentisse au début de la réunion. Comme vous le savez, j'ai besoin du consentement unanime pour poursuivre les délibérations lorsque la sonnerie se fait entendre. Je m'adresserai à chaque membre du Comité si cela se produit. Je ne fais que vous prévenir pour que vous puissiez y réfléchir. Si je n'obtiens pas le consentement unanime, nous devrons suspendre la séance pendant une demi-heure. Nous devrons donc nous accommoder de cette décision. J'y reviendrai si c'est nécessaire.

Nous accueillons plusieurs témoins aujourd'hui. Tout d'abord, du Conseil de la radiodiffusion et des télécommunications canadiennes, le CRTC, nous accueillons Steven Harroun, vice-président, Conformité et enquêtes, et Scott Hutton, vice-président, Consommation, analytique et stratégie.

Messieurs, je vous souhaite la bienvenue.

Du Mouvement des caisses Desjardins, nous accueillons Bernard Brun, vice-président, Relations gouvernementales, et Frédéric Lapalme, directeur principal et chef délégué, Encadrement et surveillance, lutte contre la fraude et les crimes financiers. Ils se joignent à nous par vidéoconférence.

Mark Hines, chef de la fraude — non pas de la fraude, mais des produits de prévention de la fraude —, d'Interac Corp, se joint à nous dans la salle.

C'est probablement une distinction importante, monsieur Hines.

Pourquoi ne pas vous entendre en premier?

Mesdames et messieurs les témoins, vous disposerez de cinq minutes pour faire une déclaration préliminaire, après quoi nous passerons aux questions des députés.

Monsieur Hines, je vous cède la parole. Vous avez cinq minutes.

Mark Hines (chef des produits de prévention de la fraude, Interac Corp.): Bonjour et merci, monsieur le président et mesdames et messieurs les membres du Comité.

Comme le président l'a dit, je m'appelle Mark Hines. Je suis chef des produits de prévention de la fraude à Interac. Je vous remercie beaucoup de m'avoir invité à participer à cette étude aujourd'hui.

J'aimerais d'abord reconnaître que nous sommes réunis sur le territoire traditionnel non cédé de la nation algonquienne anishinabe et reconnaître la présence durable des Premières Nations, des Inuits et des Métis.

Interac est une entreprise canadienne de paiement et de vérification numérique. Près de 300 institutions financières se connectent à nos réseaux, et les Canadiens utilisent nos produits plus de 20 millions de fois par jour. Nous sommes au cœur des flux financiers au Canada, ce qui nous donne une vision unique, à l'échelle du système, de la fraude et de la criminalité financière en particulier. Nos équipes surveillent le réseau 24 heures sur 24 et communiquent des signalements aux institutions financières, afin qu'elles puissent intervenir en temps réel face aux activités suspectes.

J'aimerais utiliser le temps qui m'est imparti aujourd'hui pour expliquer ce qui a changé en matière de fraude, pourquoi elle est plus difficile à combattre qu'auparavant et quelles sont les meilleures façons de protéger les Canadiens.

La fraude et l'escroquerie sont des menaces graves et croissantes. Derrière chaque escroquerie, il y a une personne qui a perdu de l'argent et souvent sa confiance par la même occasion. La nature de la menace a toutefois évolué. Auparavant, les mesures de protection contre la fraude étaient axées sur l'expéditeur, car la principale menace était l'accès non autorisé à un compte. Les arnaques fonctionnent différemment parce que c'est le véritable titulaire du compte qui autorise le paiement. Cela met l'accent sur l'élément du destinataire dans le réseau, ce qui nécessite de nouvelles capacités et de nouveaux investissements à l'échelle du système. Parallèlement, l'intelligence artificielle a considérablement accéléré le rythme des tentatives d'escroquerie. Elles ne sont pas seulement plus sophistiquées et convaincantes, elles sont maintenant automatisées à grande échelle et il suffit de prendre une personne au dépourvu une seule fois pour réussir.

Le message le plus important que je souhaite faire passer au Comité, c'est que ce problème touche de multiples industries et secteurs. Interac investit massivement dans ce domaine, mais pour passer à l'étape suivante, il faut mettre en place une approche coordonnée.

Interac déploie aujourd'hui des fonctionnalités de lutte contre la fraude et l'escroquerie sur les services de virements électroniques, et nous avons beaucoup investi pour être le premier fournisseur approuvé de services de lutte contre la fraude dans le nouveau système en temps réel du Canada. Contrairement à d'autres pays, nous lancerons le paiement en temps réel avec des mesures de protection contre la fraude intégrées, dans le but de prévenir la flambée d'escroqueries que d'autres pays ont connue. Cela signifie que les Canadiens bénéficieront d'une protection accrue dès le départ.

Aucune entreprise ou aucun secteur ne peut résoudre ce problème à lui seul. La fraude ne commence pas et ne finit pas au même endroit. Elle commence souvent par un appel téléphonique, un message texte ou une escroquerie en ligne. Au moment où l'argent est transféré, c'est souvent l'institution qui effectue la transaction qui en sait le moins sur son origine. Le facteur déterminant est le temps qui s'écoule entre la détection et l'intervention. Plus un signal digne de confiance arrive rapidement au bon endroit, plus une institution peut agir avant que l'argent ne soit perdu.

Nous considérons que les efforts du gouvernement visant à élaborer une stratégie nationale de lutte contre la fraude et à établir une agence contre les crimes financiers représentent une étape importante. L'application de la loi est aussi importante, mais elle intervient une fois que le mal est fait. Elle doit être jumelée à une coordination qui permet de prévenir les préjudices en premier lieu en empêchant l'argent de quitter les comptes bancaires des Canadiens.

C'est la raison pour laquelle la mesure la plus efficace que le Canada puisse prendre consiste à faciliter un meilleur partage des données entre les secteurs, notamment les institutions financières, les fournisseurs de services de télécommunications, les plateformes numériques et les forces de l'ordre. À titre de précision, il ne s'agit pas de regrouper les données dans une seule base de données ouverte. Il s'agit de signaux ciblés et fondés sur le risque qui permettent aux institutions d'agir en fonction de renseignements exacts reçus au bon moment. Il s'agit d'une approche axée sur la prévention et c'est celle qui donnera, à notre avis, les meilleurs résultats pour le Canada.

Je vous remercie. Je me ferai un plaisir de répondre à vos questions.

● (1535)

Le président: Merci beaucoup, monsieur Hines.

Je ne sais pas exactement qui parlera au nom du CRTC. Est-ce M. Harroun?

D'accord. Vous avez la parole, monsieur.

Steven Harroun (dirigeant principal, Conformité et enquêtes, Conseil de la radiodiffusion et des télécommunications canadiennes): Bonjour.

Avant de commencer, je tiens à reconnaître que nous sommes réunis sur le territoire traditionnel non cédé du peuple algonquin anishinabe.

Je suis accompagné cet après-midi de mon collègue, Scott Hutson, vice-président, Consommation, analytique et stratégie.

Je vous remercie de me donner l'occasion de comparaître devant le Comité dans le cadre de son étude sur les fraudes financières et les escroqueries au Canada.

Comme vous le savez, le CRTC est un tribunal quasi judiciaire indépendant chargé de réglementer le secteur canadien des communications dans l'intérêt public. Nous menons des consultations publiques sur les questions de télécommunications et de radiodiffusion, et nous prenons des décisions en fonction du dossier public.

Le CRTC fait également partie d'un effort fédéral plus vaste visant à lutter contre les appels téléphoniques, les courriels et les messages textes indésirables. Dans ce contexte, nous gérons des régimes de réglementation civile. Étant donné que le CRTC n'a pas pour mandat d'évaluer ou d'enquêter sur des comportements qui pourraient être de nature criminelle, nous encourageons les Canadiens à signaler tout cas de fraude présumée aux autorités compétentes responsables de l'application de la loi. Dans certaines circonstances, nous pouvons communiquer des renseignements à ces autorités, conformément aux exigences juridiques et aux exigences en matière de protection de la vie privée en vigueur.

● (1540)

[Français]

Aujourd'hui, je parlerai de nos rôles civils en vertu des règles sur les télécommunications non sollicitées et de la Loi canadienne antipourriel. Conformément à cette législation, nous contribuons à protéger les Canadiens en établissant des règles claires, en aidant les entreprises à s'y conformer, en imposant des sanctions à ceux qui ne respectent pas les règles et en sensibilisant la population canadienne.

Pour ce qui est des appels téléphoniques indésirables, c'est le Conseil de la radiodiffusion et des télécommunications canadiennes qui gère la Liste nationale de numéros de télécommunication exclus. Les Canadiens peuvent y inscrire leur numéro de téléphone gratuitement. Ces dernières années, nous avons mis en place une stratégie solide visant à empêcher dès le départ que ces appels indésirables ne parviennent aux Canadiens.

Comme il s'agit d'un défi complexe en constante évolution, il n'existe pas de solution unique. Notre approche combine donc plutôt des mesures réglementaires et techniques.

[Traduction]

Par exemple, les fournisseurs de services de télécommunications sont tenus de bloquer les appels qui affichent des numéros qui ne pourraient normalement pas être composés, comme le 123-456-7890. Les fournisseurs offrent également des services de filtrage des appels, ce qui permet aux Canadiens de mieux gérer les communications qu'ils reçoivent.

Nous prenons également des mesures à l'égard de la falsification de l'identité de l'appelant, une pratique par laquelle l'appelant masque son numéro de téléphone à la personne qui reçoit l'appel. Pour régler ce problème, nous avons exigé que les fournisseurs de services mettent en œuvre les normes STIR/SHAKEN. Cette technologie aide à vérifier si un appel provient réellement du numéro affiché sur l'écran d'identification de l'appelant, ce qui permet aux Canadiens d'identifier plus facilement les appels dignes de confiance.

Les nouvelles technologies jouent également un rôle de plus en plus important. L'intelligence artificielle, par exemple, peut être un outil utile. En 2021, le CRTC a approuvé une demande d'un fournisseur canadien de services de télécommunications visant à mettre en œuvre une solution fondée sur l'intelligence artificielle qui peut bloquer les appels suspects dans le réseau du fournisseur avant qu'ils ne parviennent aux Canadiens. À ce jour, des milliards d'appels de ce type ont été bloqués.

Permettez-moi maintenant d'aborder le rôle du CRTC en vertu de la Loi canadienne anti-pourriel, ou la LCAP. Nous travaillons de concert avec le Bureau de la concurrence et le Commissariat à la protection de la vie privée pour promouvoir et surveiller la conformité à la LCAP. Nous faisons également de la sensibilisation pour aider les Canadiens à mieux se protéger et à réduire les effets des pourriels. Nous collaborons avec des partenaires et des intervenants dans le cadre de cet effort.

En conclusion, le CRTC continuera de travailler dans le cadre de son mandat pour aider à protéger les Canadiens contre les appels, les pourriels et les messages textes indésirables.

Nous vous remercions de nous avoir donné l'occasion de comparaître devant vous. Nous serons heureux de répondre à vos questions.

Le président: Merci beaucoup, monsieur Harroun.

[Français]

Le prochain témoin est M. Brun.

[Traduction]

Vous avez la parole. Vous avez cinq minutes.

[Français]

Bernard Brun (vice-président, Relations gouvernementales, Mouvement des caisses Desjardins): Merci, monsieur le président.

Mesdames et messieurs les membres du Comité permanent de l'industrie et de la technologie, je vous remercie de l'invitation au nom du Mouvement Desjardins.

Je m'appelle Bernard Brun et je suis vice-président aux Affaires gouvernementales pour le Mouvement des caisses Desjardins. Je suis accompagné de mon collègue Frédéric Lapalme, directeur principal et chef délégué, Encadrement et surveillance, lutte contre la fraude et les crimes financiers.

C'est un privilège de contribuer aux travaux de votre étude portant sur les fraudes financières et les escroqueries au Canada, une préoccupation de première importance pour Desjardins. À titre de rappel, Desjardins, c'est aujourd'hui plus de 524 milliards de dollars d'actifs et plus de 10 millions de membres et de clients partout au pays. Nous accompagnons près d'un demi-million d'entreprises, de la petite et moyenne entreprise aux grandes organisations, dans tous les secteurs de l'économie canadienne. Nous sommes le plus important groupe financier coopératif en Amérique du Nord et le huitième groupe financier le plus important au monde.

La fraude est aujourd'hui l'une des formes de criminalité économique les plus répandues, sophistiquées et dommageables au Canada et à l'échelle internationale. Alimentée par la numérisation de l'économie, par l'intelligence artificielle, comme mes collègues le mentionnaient précédemment, et par l'accès mondial aux plate-

formes numériques, elle évolue à un rythme tel que les institutions publiques et privées peinent à y répondre efficacement.

La fraude est devenue un crime à faible risque et à rendement élevé. Les réseaux criminels opèrent désormais avec de plus grandes capacités, sans frontières géographiques, et en exploitant les technologies numériques, les cryptoactifs, et même les capacités d'usurpation alimentées par l'intelligence artificielle.

Plusieurs défis structurants limitent actuellement l'efficacité de la lutte contre la fraude. Je vous en nomme cinq: la fragmentation des données et des mécanismes de partage d'information; la multiplication des initiatives réglementaires et des cadres de conformité; la nature transnationale des opérations criminelles; les conséquences pour les victimes; et la rapidité d'adaptation des fraudeurs et l'utilisation croissante de l'intelligence artificielle.

C'est dans ce contexte que chaque avancée en matière de sécurité entraîne rapidement l'émergence de nouvelles stratégies de contournement. Cette dynamique crée une course technologique constante et exerce une pression importante sur les gouvernements, mais aussi sur les institutions financières et les entreprises. Les répercussions dépassent largement les pertes monétaires. Les victimes rapportent fréquemment des conséquences durables: détresse psychologique, perte de confiance envers les institutions, isolement social et atteinte à la sécurité personnelle financière.

Comme groupe financier à charte québécoise, la majorité de notre encadrement relève du gouvernement et des organismes du Québec. Par contre, nous opérons à la grandeur du Canada, ce qui nous donne une expérience et une perspective sur l'importance de la coordination et de la complémentarité réglementaire pour atteindre des résultats tangibles.

Nous sommes encouragés par la volonté du gouvernement fédéral de privilégier une action concertée entre les différents acteurs afin de lutter contre la fraude financière. Il est essentiel de mobiliser les multiples intervenants travaillant à réduire les incidents de fraude. Cela va notamment dans le sens des travaux de la Coalition canadienne antifraude, dont Desjardins est un membre actif.

En avril dernier, nous avons déposé un mémoire au ministère des Finances en réponse à sa consultation sur la Stratégie nationale antifraude. C'est avec plaisir que nous le communiquerons au Comité si cela peut contribuer à vos travaux.

En conclusion, s'il fallait donner la priorité à une seule action pour lutter efficacement contre la fraude financière et les escroqueries au Canada, ce serait d'abord de faciliter une forme de partage d'information entre les organisations réglementées afin d'améliorer la prévention et la détection.

À cet égard, nous remarquons le dépôt, hier, du projet de loi C-36, visant à renforcer la protection de la vie privée et à modifier la Loi sur la protection des renseignements personnels et les documents électroniques. Le texte prévoit notamment une exception au consentement pour permettre la transmission d'informations à des fins de prévention, de détection et de réduction des activités frauduleuses. Il s'agit, à notre avis, d'un signal positif qui doit être poursuivi et analysé attentivement en vue d'être harmonisé et aussi coordonné avec les cadres législatifs provinciaux.

Je vous remercie de votre attention. Mon collègue et moi serons heureux de répondre à vos questions.

• (1545)

Le président: Merci, monsieur Brun.

[Traduction]

Chers collègues, nous entamons maintenant notre première série de questions.

Monsieur Guglielmin, vous avez la parole. Vous avez six minutes.

Michael Guglielmin (Vaughan—Woodbridge, PCC): Je vous remercie, monsieur le président.

Je remercie les témoins de leurs déclarations préliminaires.

Monsieur Hines, un récent sondage mené par Interac a révélé que 79 % des Canadiens croient que l'intelligence artificielle aide à rendre les escroqueries plus convaincantes et qu'elle permet aux fraudeurs de les créer beaucoup plus facilement. Selon vous, dans quelle mesure l'intelligence artificielle a-t-elle changé la donne au cours des deux dernières années?

Mark Hines: Je ne passerai pas trop de temps sur la question de la complexité, car je suppose que le Comité en a beaucoup entendu parler. J'aimerais plutôt insister sur la vitesse d'exécution, qui a une incidence non seulement sur la rapidité, mais aussi sur le volume d'activités suspectes qui touchent à la fois les institutions et les réseaux individuels. Cela signifie que la probabilité qu'on réussisse à prendre quelqu'un...

Un parent débordé qui ouvre la porte d'entrée voit un lien et clique dessus sans prendre les 30 secondes nécessaires pour le vérifier. Une grand-mère inquiète envoie de l'argent à un petit-enfant. Statistiquement, cela augmente simplement la probabilité que ces choses se produisent. À mon avis, c'est l'autre élément sur lequel nous ne nous concentrons pas assez. Je ne veux pas minimiser l'aspect de la complexité, car il est bien réel, mais c'est l'élément auquel nous n'accordons pas suffisamment d'attention.

• (1550)

Michael Guglielmin: Y a-t-il des escroqueries à venir qui vous préoccupent plus que d'autres?

Mark Hines: Nous catégorisons les types d'escroqueries que nous observons sur notre réseau. Je dirais que, de loin, les plus répandues sont les escroqueries en matière d'investissement. Il y en a de tous les types, des escroqueries sentimentales aux escroqueries par usurpation d'identité bancaire, mais les escroqueries en matière d'investissement sont de loin celles que nous voyons le plus fréquemment.

Michael Guglielmin: Diriez-vous qu'au Canada, nos systèmes de prévention de la fraude — qu'il s'agisse des banques, des systèmes de paiement, des plateformes de télécommunications, etc. — parviennent à suivre le rythme de cette nouvelle complexité et la vitesse à laquelle évoluent les escroqueries, ou observez-vous des lacunes à cet égard?

Mark Hines: Je constate que des sommes importantes sont investies pour tenter de suivre le rythme. À notre avis, pour tirer pleinement parti de cet investissement important, il faut mettre en place un système de partage des données entre les secteurs. Les escroqueries, par exemple, peuvent se produire entièrement en dehors du réseau que nous exploitons. Nous ne savons pas où elles ont commencé. Nous ne connaissons pas les détails de leur origine. Notre capacité de réaction est donc limitée.

Si vous me le permettez, j'aimerais mentionner un autre détail qui, selon moi, pourrait être utile au Comité. Dans le cas des escroqueries, ce n'est souvent pas le transfert initial que l'on détecte, mais plutôt le compte de la personne touchée. C'est lorsqu'on constate que des paiements sont encaissés de l'autre côté qu'on commence à se rendre compte qu'il y a un problème. Les boucles de rétroaction qui donnent une meilleure idée de l'autre côté du réseau font partie des outils qui empêcheraient de verser les fonds en premier lieu.

Michael Guglielmin: Quel type d'investissements sont effectués par Interac pour aider à prévenir certaines de ces escroqueries générées par l'intelligence artificielle?

Mark Hines: Interac est au milieu d'un cycle stratégique de trois ans au cours duquel nous investissons des sommes importantes. Ces investissements visent à mettre en place le nouveau système de paiement en temps réel. Lorsque les virements électroniques migreront vers le système de compensation et de règlements en temps réel, nous effectuerons également des mises à niveau importantes pour mettre en place des contrôles comparables.

C'est un investissement institutionnel majeur pour notre société.

Michael Guglielmin: À votre avis, dans l'ensemble de l'écosystème, c'est-à-dire les banques et les autres plateformes, les secteurs progressent-ils au même rythme ou certains d'entre eux accusent-ils un retard?

Mark Hines: Je pense qu'il y a certainement des disparités. Je pense notamment que les institutions financières et les réseaux de paiement de tous types, et pas seulement les nôtres, font des investissements parce que c'est là que se produisent les pertes financières en ce moment. Encore une fois, pour revenir à ce que je disais, nous estimons qu'il est essentiel d'élargir ce spectre et d'exiger que les autres intervenants de l'écosystème participent à ces efforts.

Michael Guglielmin: Je vous remercie beaucoup.

J'ai quelques questions pour les représentants de Desjardins.

En 2019, des données de vos membres ont été volées. On a découvert qu'elles circulaient encore sur des forums criminels clandestins pas plus tard qu'en novembre 2025, soit plus de six ans après l'atteinte. Surveillez-vous activement, pour le compte de vos membres, les données volées sur le Web clandestin?

[Français]

Frédéric Lapalme (directeur principal et chef délégué, Encadrement et surveillance, lutte contre la fraude et les crimes financiers, Mouvement des caisses Desjardins): Je vous remercie beaucoup de la question.

Je ne vais pas entrer dans les détails de l'incident survenu en 2019, puisque Desjardins l'a commenté publiquement à de multiples reprises. Cela dit, nous investissons plusieurs centaines de millions de dollars annuellement pour contrer la fraude et assurer la sécurité des données. Notre bureau de la sécurité compte 1 800 experts en sécurité.

Pour ce qui est des données qui circulent sur le Web clandestin, ce sont effectivement des éléments que nous surveillons pour nos membres. Nous avons offert plusieurs systèmes de protection depuis l'incident. Récemment, nous avons offert certaines protections pour ce qui est du Web clandestin, et elles ont été ajoutées à la portée. Nous comprenons que nos membres et nos clients ont une crainte relativement aux données présentes sur le Web clandestin. Ce sont des éléments que nous considérons de façon très ciblée.

[Traduction]

Michael Guglielmin: Lorsque vous trouvez des données, que pouvez-vous faire? Pouvez-vous les retirer du Web clandestin ou la surveillance se limite-t-elle à suivre leur propagation?

[Français]

Frédéric Lapalme: Il est extrêmement difficile de sortir des données du Web clandestin, et même d'Internet. Une fois que c'est sur Internet, c'est dans la sphère publique.

Il faut tenir compte d'un autre point. Il peut y avoir des discussions sur le nombre exact, mais il y a plusieurs centaines, voire des milliers de fuites de données. De façon générale, les citoyens canadiens et québécois ont malheureusement été victimes à plusieurs reprises de plusieurs fuites de données. Ça ne dégage pas Desjardins de sa responsabilité, par contre, et je vous assure que nous la prenons très au sérieux, mais les données sont présentes à plusieurs niveaux.

Ça peut être utile pour la fraude, surtout pour les arnaques, particulièrement les arnaques des faux représentants, dans le cadre desquelles un fraudeur se fait passer pour un agent de police ou pour un employé d'une institution financière. Le fait qu'il a accès à certaines informations va permettre de créer cette confiance chez la victime potentielle. Quand on répond au téléphone et que la personne de l'autre côté connaît déjà plusieurs informations clés, ça crée un niveau de confiance envers le faux représentant en question. Ça lui donne une certaine crédibilité. Voilà ma réponse.

• (1555)

[Traduction]

Le président: Je vous remercie, monsieur Guglielmin.

Monsieur Ma, je crois comprendre que vous partagerez peut-être votre temps avec Mme O'Rourke. Je vais vous laisser décider entre vous. Vous avez six minutes au total.

Vous avez la parole.

Michael Ma (Markham—Unionville, Lib.): Je vous remercie.

Je vous remercie, messieurs, d'être ici aujourd'hui.

Ma première question s'adresse aux représentants du CRTC.

Le gouvernement a annoncé la création d'une nouvelle agence contre les crimes financiers. Selon vous, quelles sont les occasions de renforcer la coordination entre les entreprises de télécommunications, les organismes de réglementation, les organismes d'application de la loi, les institutions financières et cette nouvelle agence, afin de démanteler le réseau de fraude?

Steven Harroun: Comme de nombreux témoins vous l'ont dit dans le cadre de cette étude, cette collaboration est essentielle. Encore aujourd'hui, tous mes collègues ont laissé entendre la même chose. Je pense que la nouvelle Agence contre les crimes financiers représentera une excellente façon de réunir les fournisseurs de services de télécommunications, les banques et d'autres intervenants pour lutter contre ces activités.

Pour le CRTC, le plus grand défi consiste à s'assurer que tous les intervenants communiquent entre eux. Je dirais que chacun fait sa part pour se tenir au courant. Cette collaboration est donc essentielle.

Michael Ma: Merci.

Avant de céder la parole à ma collègue, j'ai une question à poser au représentant d'Interac.

Monsieur Hines, vous avez parlé de l'importance du partage des données. De quel type de données s'agit-il et dans quelle mesure ce partage est-il effectué en temps voulu? Bien souvent, ce genre de processus constitue davantage une mesure après coup qu'un véritable outil de prévention de la fraude. J'aimerais savoir à quoi vous songez lorsque vous parlez du partage des données.

Mark Hines: Tout à fait. Si cela peut vous être utile, je peux vous donner un exemple de scénario avec l'élément de données.

Une arnaque apparaît sur une plateforme numérique. L'utilisateur clique dessus. Il est redirigé vers une discussion en ligne où on l'incite à faire un investissement qui s'avère être une arnaque. Si la plateforme numérique ou l'entreprise de télécommunications détermine que cette activité est suspecte, elle pourrait transmettre sur un réseau le lien et le numéro de téléphone associé à la discussion. Lorsque cela atteint un système de paiement, nous serions en mesure de déterminer qu'il s'agit d'un élément qui fait partie de notre recette secrète. Je pourrais alors vérifier si la destination de ce paiement frauduleux est liée à une arnaque qui est déjà survenue. Je bloquerais alors le paiement. Nous avertirions l'institution financière et lui dirions de ne pas envoyer le paiement, car nous pensons qu'il y a un grand risque que ce soit une arnaque.

C'est ce genre de renseignements qui peut avoir une grande incidence si nous les obtenons avant le traitement du paiement.

Michael Ma: Merci.

Je vous pose ma toute dernière question. Pensez-vous qu'il sera utile de sensibiliser et d'informer le public?

Mark Hines: C'est une excellente question.

Ce que je dirais, c'est que les arnaqueurs ciblent les personnes les plus vulnérables. Ainsi, bien qu'il soit très important d'informer les gens, il y a des limites quant à la mesure dans laquelle on peut protéger ces personnes ce faisant. C'est pourquoi Interac estime que la responsabilité va bien au-delà de cela. Elle incombe à chacun d'entre nous qui jouons un rôle dans l'exemple que je viens de donner.

Michael Ma: Merci.

Je cède la parole à ma collègue.

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

Monsieur Hines, je trouve fascinant que vous ayez affirmé que « le facteur déterminant est le temps qui s'écoule entre la détection et l'intervention ». Lorsque Wealthsimple a témoigné devant le Comité, nous avons appris que l'entreprise avait trouvé, en une seule journée, 1 500 utilisations frauduleuses de son logo et hypertrucages mettant en scène son PDG, mais qu'il avait fallu quatre jours à la plateforme Meta pour les supprimer.

Pensez-vous que les plateformes en font assez?

Mark Hines: Je pense que les plateformes doivent faire partie de la solution. La question n'est pas de savoir si elles sont capables de tout supprimer. Ce qui importe, c'est qu'en nous transmettant les renseignements à mesure qu'elles suppriment les contenus, chacun de ces éléments de données augmente considérablement nos chances d'empêcher le transfert d'argent, qui est le moment où les Canadiens subissent un préjudice.

Ce que nous préconisons, sur le plan de la responsabilité au sein de l'écosystème, c'est que chaque acteur ait des obligations clairement définies et que la responsabilité découle du respect ou du non-respect de ces obligations. Nous nous incluons nous-mêmes dans cette démarche.

• (1600)

Dominique O'Rourke: Je trouve utile que vous nous ayez dit que les arnaques liées aux investissements sont de loin les plus répandues, car on a parfois tendance à les considérer comme un problème qui touche uniquement les personnes âgées qui ne maîtrisent pas forcément les technologies. On entend dire que ces escroqueries sont de plus en plus sophistiquées. On dit également que seulement 5 à 10 % d'entre elles sont signalées. À l'évidence, les arnaques liées aux investissements sont nombreuses, tout comme les arnaques sentimentales, sans compter toutes sortes d'autres escroqueries qui ciblent les personnes âgées.

Vous avez indiqué que la mesure la plus efficace réside dans le partage des données entre les secteurs. Pouvez-vous m'expliquer quelles sont certaines des considérations relatives à la protection de la vie privée? L'Ontario a encore du mal avec la cybersanté. Pouvons-nous établir ce partage intersectoriel des données assez rapidement? De quoi avez-vous besoin sur le plan législatif, ou quelle est votre recommandation?

Mark Hines: Lorsque je parle de partage des données, je fais référence à des éléments de données bien précis qui sont échangés entre des parties bien précises. Je pense qu'il y a deux aspects juridiques sur lesquels il faut se concentrer. L'un d'entre eux a été mentionné précédemment. Il s'agit de disposer d'une base claire pour traiter les données à des fins de lutte contre la fraude. Cela existe déjà dans la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE.

D'après mon expérience dans la négociation d'ententes d'échange de données dans une institution financière, au sein d'une entreprise de technologie financière, puis aujourd'hui chez Interac, nous accordons une importance capitale au consentement, ce qui montre à nouveau combien il est essentiel de disposer de motifs valables pour traiter des données.

L'autre aspect concerne les dispositions d'exonération pour l'échange de renseignements. Elles existent dans d'autres pays pour la mise en commun de renseignements relatifs à la criminalité financière. Si je considère que c'est si important, c'est parce que, d'après l'expérience que je viens de mentionner, nos participants prennent très au sérieux leur responsabilité lorsqu'il s'agit des données et ils ne les communiqueront que s'ils estiment que le risque est faible ou acceptable. Cette disposition d'exonération favorise le type d'échange de renseignements que nous estimons essentiel si nous voulons endiguer le problème dès son apparition.

Dominique O'Rourke: Mon temps est écoulé. Merci.

Le président: Merci, madame O'Rourke.

[Français]

Monsieur Ste-Marie, c'est à votre tour. Vous avez la parole pour six minutes.

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

Je salue l'ensemble des témoins. Je les remercie de leur présence.

Mes questions seront pour les représentants du Mouvement des caisses Desjardins. J'aimerais en entendre davantage au sujet des encadrements législatifs restrictifs ou contradictoires.

Frédéric Lapalme: Je vous remercie beaucoup de la question.

Mon collègue M. Bernard Brun l'a mentionné: nous sommes présents au Québec, mais également au Canada. Donc, pour ce qui est de la protection des renseignements personnels, la différence entre la législation fédérale et la législation provinciale est un défi. Comme institution financière, nous souhaitons participer aux initiatives de lutte contre la fraude. Nos collègues sont dans des organisations de compétence fédérale, donc de législation fédérale, alors que nous sommes au provincial. Nous devons analyser et déceler des écarts pour nous assurer de participer à ce genre d'initiative de transmission d'informations dans les règles de l'art. Il y a donc beaucoup de paperasse interne et d'évaluations pour nous assurer que nous faisons ça de la bonne manière, ce qui, bien entendu, dans des cas de fraude très rapides, ne marche pas dans la chronologie précise d'une initiative de lutte contre la fraude.

Gabriel Ste-Marie: En matière de lutte contre la fraude, vous souhaitez plus de transmission d'informations entre les intervenants impliqués. Pouvez-vous nous en dire plus?

Frédéric Lapalme: C'est un point intéressant. M. Brun l'a mentionné: c'est le point clé. Le Mouvement des caisses Desjardins négocie des milliards de dollars de ses membres clients, et effectue des millions, voire des milliards de transactions par année. Nous devons donc être capables de nous transmettre ces informations avec Interac et nos collègues des banques, donc de nous assurer d'utiliser ces données à bon escient pour lutter contre la fraude. Comme les transactions se font en millisecondes maintenant, étant donné l'arrivée des transactions en temps réel, nous serons limités. Nous devons donc être capables d'utiliser ces données tant à l'interne qu'avec nos collègues, pour être capables de mettre en place les bonnes balises et les bons garde-fous, afin de protéger nos membres clients.

• (1605)

Gabriel Ste-Marie: Je passe à ma prochaine question, qui est une question double.

J'aimerais entendre vos commentaires au sujet de votre expérience des interactions entre les différents intervenants gouvernementaux liés à la fraude. On peut penser au Centre d'analyse des opérations et déclarations financières du Canada, ou CANAFE, au Centre antifraude du Canada et à la Gendarmerie royale du Canada, ou GRC.

De plus, quel rôle voyez-vous pour la future Agence contre les crimes financiers, étant donné qu'il y a déjà des institutions présentes?

Frédéric Lapalme: Ces institutions ont leur rôle à jouer, tant le CANAFE que le Centre antifraude du Canada. Ce sont des corps policiers. Desjardins interagit avec les deux au quotidien. Les corps policiers peuvent nous envoyer des demandes pour mener des enquêtes. Selon les seuils de déclaration, nous allons fournir au CANAFE les informations sur plusieurs centaines de milliers de transactions par année. Malheureusement, bien souvent, il est possible que nous envoyions des choses au CANAFE, donc des déclarations, et qu'un corps policier qui est en train d'enquêter nous fasse directement une demande sur le même cas. Donc, il y a un avantage à tirer pour les organisations qui se trouvent des deux côtés de l'information qui est envoyée.

Pour ce qui est de l'Agence, ce que nous aimerions voir, ce sont les arrestations découlant des enquêtes. C'est aligné avec les recommandations du Groupe d'action financière, publiées il y a cinq ans, et probablement le prochain rapport qui sera déposé. Nous voulons nous assurer de l'efficacité du régime, tant sur le plan de la fraude que du crime financier — parce que les choses se recoupent éventuellement —, pour obtenir un résultat concret: une arrestation et une condamnation. La prévention est utile, mais il y a un certain point de non-retour, qui nécessite des enquêtes et, malheureusement, des accusations formelles.

Donc, c'est là que nous souhaiterions éventuellement voir l'Agence ou un autre organisme prendre la place, parce qu'il y a une expertise nécessaire aux enquêtes sur les crimes financiers qui n'est pas donnée à n'importe quel corps policier au Canada.

Gabriel Ste-Marie: J'aimerais revenir sur le Régime canadien de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes. S'il y avait une amélioration à y apporter pour mieux lutter contre la fraude, qu'est-ce que ça serait?

Frédéric Lapalme: J'ai déjà mentionné la transmission d'informations et les arrestations.

J'irais dans ce sens, vers une approche basée sur le risque. Nous le faisons pour la fraude. Les institutions financières n'aiment pas perdre de l'argent, bien entendu, et ne souhaitent vraiment pas que leurs membres clients soient touchés par les fraudes. Donc, il faut nous laisser cette marge de manœuvre pour gérer les risques, gérer la fraude et arriver aux résultats souhaités.

Nous faisons partie de la dynamique. Nous saluons l'initiative d'aujourd'hui et la consultation nationale. Nous soutenons de tout cœur la volonté du gouvernement de lutter contre la fraude. Il faut éviter de placer la fraude dans un cadre réglementaire trop rigide. Ça serait la recommandation, tant pour ce qui est de la fraude que du crime financier.

Gabriel Ste-Marie: Il me reste une minute. Je vais poser une dernière question.

Un témoin est venu nous dire qu'il y a d'autres pays où la loi est telle qu'elle exige que les plateformes numériques vérifient l'identité des personnes qui achètent des publicités et qui prétendent vendre des produits financiers, incluant les cryptomonnaies, avant de les publier. Le témoin nous disait que, dans ces pays, les plateformes ont obtenu, et on aurait vu une baisse des escroqueries.

Est-ce que vous pensez que c'est une avenue que le Canada devrait emprunter?

Frédéric Lapalme: C'est une solution intéressante. C'est un outil de plus dans le coffre à outils du Canada et des institutions. Ça ne règlera pas tout, mais le principe est tel que, plus les choses sont anonymes, plus la fraude est présente. Donc, il est sûr et certain qu'une exigence de transparence pour permettre de comprendre qui agit, qui paie et qui finance les publicités ou fait d'autres actions sur d'autres plateformes, ce n'est pas perdu.

Gabriel Ste-Marie: Je vous remercie beaucoup.

Le président: Merci, monsieur Ste-Marie.

[Traduction]

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

Raquel Dancho (Kildonan—St. Paul, PCC): Merci beaucoup.

Merci aux témoins de leur présence.

Ma première question s'adresse à M. Harroun.

J'ai remarqué que des progrès avaient été réalisés ces dernières années et je pense que c'est peut-être grâce au CRTC et à son travail sur l'usurpation d'identité et les problèmes d'affichage de l'appelant. La dernière fois que vous étiez ici — je crois que c'était en septembre —, j'ai mentionné que mon bureau de circonscription avait reçu un appel de la RBC qui, en réalité, ne provenait pas du service bancaire en ligne de la RBC. Heureusement, j'avais dans mon équipe une personne très avisée qui s'en est rendu compte et qui y a mis fin.

J'ai remarqué récemment que je reçois désormais des messages textes similaires de la part d'une banque avec laquelle je fais affaire. On me rappelle, par exemple, de régler ma facture de carte de crédit — c'est un message légitime.

J'en ai reçu un similaire...

Le président: Madame Dancho, je suis vraiment désolé de vous interrompre.

Je constate que la sonnerie se fait entendre. Je vais vous demander de faire une petite pause. Je vais arrêter le chronomètre, mais je vous laisserai reprendre depuis le début pour que tout le monde puisse suivre le fil de votre intervention.

Raquel Dancho: Bien sûr. Je crois que je m'égarais un peu de toute façon. J'ai tellement de choses à dire.

Le président: Eh bien, vous aurez l'occasion de recommencer.

Chers collègues, je constate que la sonnerie se fait entendre. La télévision n'est pas allumée, mais je suppose qu'un vote a été demandé. J'ai besoin du consentement unanime pour poursuivre. Étant donné qu'il s'agit d'une question de privilège, je vais demander à chaque député de me faire signe qu'il accepte.

Des députés: D'accord.

Le président: Madame Dancho, je vous laisse reprendre votre intervention. Vous disposez de cinq minutes.

● (1610)

Raquel Dancho: Je pense qu'il y a eu des progrès sur le plan de l'identification de l'appelant et cela tient peut-être au travail du CRTC et à vos initiatives... Je ne sais pas si vous avez demandé aux entreprises de télécommunications de lutter contre l'usurpation d'identité à l'aide de la technologie STIR/SHAKEN.

Que pouvons-nous faire contre les textos frauduleux? Ils semblent de plus en plus sophistiqués. L'autre jour, j'ai failli me faire piéger par un message qui ressemblait énormément à un message légitime. Je reçois des rappels par texto de ma banque, ce qui est très pratique. Cet autre message que j'ai reçu était très similaire et j'ai failli tomber dans le panneau. Y a-t-il quelque chose que vous puissiez faire pour inciter les entreprises de télécommunications à s'attaquer à ce problème?

Steven Harroun: Je vous remercie de la question. Vous avez bien fait une belle transition pour moi.

Du côté de la téléphonie, nous avons mis en place des mesures comme le blocage universel des appels provenant de numéros tels que le 123-456-7890, dont j'ai déjà parlé, mais aussi STIR/SHAKEN, qui est en réalité ce système de vérification des appels. Est-ce votre banque qui vous appelle? Le système peut au moins vous indiquer un « X » ou « potentiellement frauduleux », ou vous indiquer si vous pouvez faire confiance à l'appel.

En ce qui concerne les messages textes, votre question tombe à point nommé, car l'année dernière, nous avons mis en place un cadre permettant aux fournisseurs de services de télécommunications de bloquer les courriels et les messages textes qu'ils savent frauduleux. Je vais être honnête: je m'occupe des politiques, mais il y a toute une série d'aspects techniques derrière cela qui leur permettent de déterminer si un message texte est valide ou si un courriel contient une pièce jointe sur laquelle il ne faut pas cliquer, etc.

Dans les semaines à venir, nous allons publier une décision qui renforcera encore davantage ce cadre et qui permettra aux entreprises de télécommunications d'aller plus loin, en ce sens qu'elles pourront empêcher de tels messages textes d'arriver sur votre téléphone.

Raquel Dancho: C'est une excellente nouvelle.

La technologie pour le faire existe et il semble que vous allez leur permettre de l'utiliser. Est-ce exact?

Steven Harroun: Tout à fait. Selon les dispositions de la Loi sur les télécommunications, les fournisseurs de services de télécommunications doivent obtenir l'autorisation du CRTC pour intervenir sur tout type de trafic. Lorsque je parle de ces questions, je dis souvent que si je ne peux pas faire appliquer quelque chose, je m'occuperai de la réglementation, ce qui correspond à cet aspect de la politique, et que si je ne peux pas, en fait, m'occuper de la réglementation, alors j'informerai les Canadiens.

Raquel Dancho: Merci.

C'est un excellent travail et je me réjouis que ces mesures soient mises en place.

Je voudrais comprendre comment les choses vont fonctionner. Si je cliquais sur le lien et que j'effectuais un virement électronique, l'argent serait prélevé sur mon compte bancaire. Imaginons que je sois cliente chez Desjardins. L'argent serait prélevé, puis acheminé vers l'escroc par le réseau de paiement Interac. Quelle est la part de responsabilité de chacun d'entre vous?

Je pose la question à M. Hines.

Si j'effectuais un virement électronique destiné à l'escroc, quelle serait votre responsabilité, légalement, pour empêcher cet escroc d'agir? J'essaie simplement de comprendre quelle est la responsabilité de Desjardins, quelle est la vôtre, et où chacune s'arrête. Pouvez-vous m'expliquer la différence? Comment collaboreriez-vous avec Desjardins au sujet de cette arnaque?

Mark Hines: Actuellement?

Raquel Dancho: Oui.

Mark Hines: Actuellement, en tant que réseau intermédiaire, Interac ne joue pas de rôle direct dans l'indemnisation des victimes d'escroqueries. C'est géré par nos participants, généralement une institution financière. Ce que nous proposons, cependant, c'est que chaque acteur de la chaîne — la plateforme, nous-mêmes, la banque et l'individu — ait des obligations précises. Si nous ne les

respectons pas, nous devrions alors assumer une certaine part de responsabilité.

Raquel Dancho: Quelles sont vos capacités par rapport à celles de Desjardins, par exemple, lorsqu'il s'agit de bloquer un virement électronique? Je m'adresserai ensuite aux représentants de Desjardins pour obtenir une réponse. Quelle est la différence entre vous deux? Qui devrait bloquer le virement?

Mark Hines: Chacun d'entre nous a un rôle à jouer. Le rôle essentiel que nous jouons... Notre principal atout réside dans la vision globale que nous avons du réseau. Qu'est-ce que cela signifie? C'est que je peux voir certains renseignements sur le destinataire que l'institution expéditrice ne peut pas voir par elle-même, qu'il s'agisse de la plus grande institution financière du pays ou d'une petite institution. Obtenir ces renseignements du côté du destinataire, ce qui est vraiment essentiel notamment pour lutter contre les escroqueries, est ce sur quoi nous concentrons nos efforts, car c'est ce que nous sommes les seuls à pouvoir faire.

Raquel Dancho: D'accord.

[Français]

Je m'adresse à vous, les témoins de Desjardins. Est-ce que vous avez des suggestions de lois qu'on peut adopter ou de quelque chose qu'on peut faire en lien avec la réponse de M. Hines?

Frédéric Lapalme: Oui. Ce que nous aimerions mentionner, c'est que ça démontre l'importance de la Coalition canadienne anti-fraude, qui a été lancée, et des discussions que nous avons aujourd'hui. Donc, c'est une chaîne complète.

Dans la situation qui a été mentionnée, l'institution financière serait grandement responsable de la compensation ou non de la victime, mais, comme nous avons pu le démontrer aujourd'hui, c'est une chaîne complète d'intervenants qui ont tous une responsabilité. Donc, la Coalition canadienne antifraude et les autres initiatives pour rassembler tous les joueurs sont d'autant plus importantes.

• (1615)

[Traduction]

Raquel Dancho: Enfin, ma dernière question s'adresse aux représentants du CRTC. Quel est selon vous le rôle des entreprises de télécommunications? Était-ce leur responsabilité d'empêcher l'envoi de ce message texte à la base? Je ne dis pas cela par méchanceté, mais j'ai parfois l'impression qu'on se renvoie un peu la balle: « Oui, c'est un peu de notre faute, mais c'est aussi un peu la leur et nous n'allons pas en assumer les coûts. C'est à eux de le faire, mais nous aurions pu l'empêcher. » Bref, je pense que vous voyez où je veux en venir.

Quel rôle les entreprises de télécommunications jouent-elles pour mettre fin à cela?

Le président: Si possible, veuillez répondre en 30 secondes environ, monsieur Harroun.

Steven Harroun: En fin de compte, le rôle des entreprises de télécommunications dans ce scénario consiste à acheminer le message texte, l'appel ou le courriel jusqu'à votre boîte de réception. Elles constituent le canal qui vous le transmet. Heureusement, comme elles sont très engagées dans la lutte contre ce type de fraude et ce genre d'activité, elles s'adressent souvent à moi pour demander des autorisations: « Pouvons-nous bloquer ce type de trafic? Pouvons-nous empêcher ce genre de choses? » C'est tout simplement leur rôle. Elles souhaitent assurer la sécurité du réseau autant que n'importe qui d'autre, mais, en fin de compte, leur rôle est d'acheminer les communications si elles sont censées le faire, si elles transitent par leur réseau.

Le président: Merci, madame Dancho.

[Français]

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

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

Je vais commencer par vous, monsieur Hines.

Il est vrai qu'Interac n'est pas une institution financière à part entière. Vous travaillez avec les banques pour, je dirais, effectuer les transactions financières à l'interne.

Je vais aller sur le sujet de l'humain. Je vais parler des aînés, de nos parents et de nos grands-parents. Certains ont des téléphones cellulaires et font parfois des virements Interac. Il arrive qu'ils maî-trisent mal une transaction et qu'ensuite la banque dise que ce sont eux les responsables. Nous, comme jeunes parents, nous n'avons pas été outillés pour former nos grands-parents sur la manière dont Interac fonctionne. Si je suis au travail, je ne peux pas aller m'asseoir pour montrer à mon grand-père et à ma belle-mère comment Interac s'utilise.

À quel moment l'institution est-elle responsable de donner aux aînés une bonne littératie financière pour éviter la fraude?

[Traduction]

Mark Hines: Comme je l'ai déjà mentionné, il est essentiel d'informer les gens, en particulier les groupes vulnérables. Les personnes âgées en font évidemment partie. J'ai entendu des témoignages de personnes qui ont des difficultés d'apprentissage et qui ont été victimes d'escroqueries sentimentales graves. Ce sont des histoires tragiques.

Chez Interac, nous estimons que le consommateur ne devrait pas avoir à supporter seul le poids de ces escroqueries. C'est pourquoi notre approche consiste à définir une démarche intersectorielle, à déterminer ce que chacun doit faire et à répartir les responsabilités en conséquence.

Informé en est un élément essentiel. Malheureusement, pour ce qui est plus particulièrement des personnes âgées — et ce n'est qu'une observation personnelle —, j'ai constaté que cela pouvait les empêcher de faire ce qu'ils auraient vraiment besoin de faire en ligne. Informer les gens est un élément essentiel, mais nous avons également un rôle à jouer pour veiller à leur ériger une sorte de rempart afin de les protéger.

[Français]

Bienvenu-Olivier Ntumba: Merci, monsieur Hines.

Je vais rapidement poser la même question aux représentants de Desjardins avant de passer la parole à ma collègue.

Monsieur Lapalme, vous pouvez répondre.

Frédéric Lapalme: Je vous remercie de la question.

Ma réponse va ressembler beaucoup à celle de M. Hines. Nous l'avons mentionné aussi: les aînés ne sont plus les seules victimes. Les jeunes sont des victimes sur le plan des investissements. Les gens qui ne sont pas des jeunes ni des aînés sont victimes d'autres types d'arnaques. En fait, les gens les plus susceptibles d'être visés par des arnaques sont des gens qui, malheureusement, ne songent pas au fait qu'ils sont potentiellement des victimes, et pensent que les autres le sont. C'est dans la rapidité d'exécution des transactions et des fraudes dans la vie quotidienne des citoyens et des membres clients que se passent les arnaques. Je pense que ça a été mentionné par un autre témoin: un faux pas momentané peut mener à être victime de fraude.

Donc, la technologie est de plus en plus implantée et, malheureusement, nous ne pouvons pas remettre le génie dans la bouteille. Nous allons devoir évoluer.

[Traduction]

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

Merci à vous tous d'être ici aujourd'hui.

Je voudrais reprendre là où Mme Dancho s'est arrêtée. Cela vous surprendra peut-être, mais j'ai le sentiment qu'au sein de notre comité, c'est sur ce point que nos positions convergent et que nous sommes tous très préoccupés par la situation. Notre étude revêt désormais une importance toute particulière pour trouver un moyen de protéger les Canadiens.

Je commencerai par Interac.

Monsieur Hines, vous avez parlé de certaines mesures. Pour revenir à ce dont parlait Mme Dancho, pourriez-vous nous expliquer comment les différents acteurs collaborent? Nous avons eu des discussions avec des représentants de plateformes, en gros avec tous les différents acteurs. Nous sommes tous ici. Pouvons-nous au moins trouver une solution ou un modèle qui nous permette de comprendre ce que nous pouvons améliorer?

● (1620)

Mark Hines: Il existe aujourd'hui des cadres et des structures — on n'a pas à les inventer — tant au Canada qu'à l'étranger. Ici, il y a essentiellement une structure semblable en matière de cybersécurité, dans laquelle les organisations s'échangent des informations. Ce genre d'approche pourrait être adoptée pour les données sur la fraude.

L'Australie est un bon exemple. Je pense que le Comité a reçu un délégué de l'Australie. C'est un marché qui a choisi une telle approche. On essaie d'apprendre de l'expérience d'autres pays, de l'Australie, en particulier, du Royaume-Uni dans une certaine mesure, et de Singapour également. Il y a des normes sur la façon de structurer les choses pour minimiser les atteintes à la vie privée, tout en garantissant l'intégrité et la sécurité, évidemment. Je citerais ces exemples comme des modèles concrets que l'on pourrait adopter sans avoir à partir de zéro.

Si vous me permettez de prendre encore 15 secondes pour donner un exemple du fonctionnement d'un élément dans un tel scénario, parmi les nouvelles fonctionnalités que l'on déploie en matière de PTR et de virement électronique est ce qu'on appelle une liste de risques, qui contient certaines données qui ont déjà été associées à la fraude. Si l'on sait qu'un numéro de téléphone a déjà été associé à une fraude et que l'on peut réinjecter cette information dans le système, cela peut permettre à un FST de filtrer ces acteurs malveillants. Je parle toujours des informations qui nous parviennent, mais il existe également des moyens pour nous de les partager en retour.

Doly Begum: Si vous me le permettez, j'aimerais poser la même question à M. Harroun.

Le président: Madame Begum, je crains que l'on ait largement dépassé le temps imparti, alors on devra peut-être y revenir plus tard.

Quelle coïncidence. Je viens de jeter un coup d'œil, l'espace d'un instant, à un courriel de FIFA World qui se lit comme suit: « 4 millions de dollars ont été accordés jusqu'à présent, Ben Carr. Cliquez ici pour votre récompense exclusive. » Lorsque j'ai cliqué sur le lien de FIFA World, disons que cela avait l'air frauduleux. Je suis content d'avoir été bien informé sur le sujet, mais ça tombe vraiment à pic.

Je n'y vois aucun de vos logos, alors tout le monde est en sécurité pour le moment.

[Français]

Monsieur Ste-Marie, vous avez la parole pour deux minutes et trente secondes.

Gabriel Ste-Marie: Je vous félicite pour votre vigilance, monsieur le président.

Je vais encore continuer de discuter avec vous, les représentants du Mouvement des caisses Desjardins.

J'aimerais entendre vos commentaires au sujet du rôle de l'intelligence artificielle dans la fraude, mais aussi dans la prévention.

Frédéric Lapalme: L'intelligence artificielle est la nouveauté. Elle est la saveur du mois et probablement des prochaines décennies. Les fraudeurs l'utilisent dès maintenant. Par exemple, au Québec, on a vu l'utilisation de la langue française qui a augmenté. Avant, c'était une barrière qui nous protégeait un petit peu au Québec. Malheureusement, ce n'est plus le cas pour ce qui est des textos et des courriels. Un agent conversationnel est capable d'écrire un très bon courriel.

Pour ce qui est de la prévention et de la détection, en tant qu'institution financière, nous devons utiliser ces outils. On en revient encore aux éléments de la protection des renseignements personnels. C'est important, mais, pour être capables d'utiliser l'intelligence artificielle, nous avons besoin de données. Les institutions financières ont plein de données qui peuvent servir à protéger leurs clients, leurs membres. Ma réponse serait donc dans cette même veine.

Gabriel Ste-Marie: Passons maintenant à un autre sujet: le système bancaire ouvert.

Actuellement, en cas de fraude où quelqu'un fait une transaction non autorisée, l'institution financière doit payer, mais, avec le système bancaire ouvert, il y a un risque que l'institution et la plateforme d'échanges se renvoient la balle, ou encore que les entre-

prises de technologie financière n'aient même pas les moyens de payer.

Comment peut-on s'assurer que le consommateur ne soit pas perdant?

Bernard Brun: C'est une très bonne question. On entre dans une autre dimension, où on parle plus de portabilité des données. Le système bancaire ouvert va également amener des transactions plus fréquentes.

Il est important de voir que ce système existe déjà, mais qu'il prend la forme de grattage d'écran. La première chose que je mentionnerais, c'est qu'il serait excellent de mettre en place un cadre réglementaire, parce que ça va vraiment permettre de délimiter et de départager des responsabilités.

Cela dit, on met vraiment le doigt sur le défi, c'est-à-dire toute la coordination qui doit être effectuée. Il doit y avoir une coordination très claire entre les territoires de compétence, que ce soit le Québec ou d'autres provinces et le fédéral, pour déterminer qui est responsable et à quel point, surtout dans le contexte du système bancaire ouvert et des services aux consommateurs, étant donné l'accélération des transactions.

• (1625)

Gabriel Ste-Marie: D'accord. Je vous remercie beaucoup.

Monsieur le président, je vous laisse les quelques secondes qu'il me reste. Merci.

The Chair: Merci, monsieur Ste-Marie.

[Traduction]

Monsieur Falk, vous avez la parole pour cinq minutes.

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

Je remercie les témoins de leur présence au Comité aujourd'hui.

Monsieur Hines, j'aimerais commencer par vous.

Des représentants de Paiements Canada étaient ici il y a quelques réunions, et ils ont parlé du PTR, le système de paiement en temps réel, qui sera mis en place plus tard cet automne et qui permettra d'accélérer les transactions.

Pour l'instant, on ne dispose pas de ce système. On utilise un système plus lent. À quel point est-il plus lent? Quelle est la durée habituelle du traitement d'un paiement?

Mark Hines: Le système de virement électronique tel qu'il existe aujourd'hui est en fait composé de plusieurs éléments, y compris des éléments en temps réel. La majorité des paiements d'entreprise et une partie des paiements de détail s'effectuent en effet en temps réel, tandis que la majeure partie de notre système comporte des délais entre le paiement effectué par l'utilisateur et le transfert effectif des fonds. Cette pratique existe principalement à des fins de prévention de la fraude. La durée exacte du délai est principalement fixée par les institutions financières et peut varier de quelques minutes à une demi-heure. Les transactions en temps réel s'effectuent généralement en quelques secondes, et le plus souvent en moins d'une minute.

Ted Falk: Il y a aujourd'hui un léger décalage entre le moment où un virement est effectué et celui où il est reçu. Lorsqu'un virement est effectué, il transite par le système Interac.

Je vais aborder ici un cas précis. Il a été évoqué lors d'une réunion précédente du Comité.

Peter Squire, un agent immobilier de Winnipeg, a été victime de fraude au téléphone en octobre 2022. En novembre de la même année, il a fait un virement dans le compte du fraudeur, dans une succursale de la RBC à Toronto, et y a par la suite effectué un autre transfert plus important, pour un total d'environ 650 000 \$. Quelque part en cours de route, le fraudeur a pu ouvrir un compte à la RBC et, de là, il a transféré l'argent à la Citibank, à Hong Kong.

Vous jouez tous dans le même bac à sable. N'y a-t-il pas de recours pour les cas comme celui de Peter Squire?

Mark Hines: Une fois l'argent transféré, il est perdu. C'est précisément la raison pour laquelle j'ai mis l'accent, dans ma déclaration préliminaire et à quelques reprises aujourd'hui, sur la nécessité de se concentrer sur le partage des renseignements à des fins de prévention. Une fois que l'argent a été transféré et que l'on en est au stade des recours, il est possible d'optimiser les mesures du côté du destinataire.

Je ne veux pas minimiser le problème, mais à mon avis, rendu là, on est déjà passé à côté de l'essentiel. Pour éviter ce genre de situation, il faut empêcher que l'argent ne quitte le compte, car pour chacune de ces histoires horribles, même celles qui se terminent plus ou moins bien, le temps qu'il faut pour les régler a un effet démesuré sur les gens.

C'est précisément pour cette raison que l'on préconise de mettre l'accent sur la prévention. Il faut s'inspirer des modèles d'autres pays qui ont trouvé la bonne approche et qui en récoltent les fruits.

Ted Falk: Est-ce qu'Interac signale aux institutions financières certaines transactions comme étant potentiellement frauduleuses?

Mark Hines: Oui.

Ted Falk: À quelle fréquence?

Mark Hines: On attribue une note à chaque transaction par virement électronique et on la transmet à l'institution financière. Elle s'en sert pour décider si elle traitera ou non la transaction, si elle l'effectuera vraiment. Voilà ce que l'on fait pour l'instant.

En ce qui concerne le PTR et le système amélioré de virements électroniques, lorsque le PTR sera en service, il comportera quatre éléments principaux. On continuera d'attribuer une note. L'un des facteurs pris en compte dans cette note est ce que j'ai appelé la liste des risques, c'est-à-dire le répertoire des fraudes précédemment identifiées. Un élément clé pour le PTR est que celui-ci et le système de virement électronique partageront leur liste des risques. Ce partage des données constitue une première étape pour tenter de prévenir les fraudes. Ensuite, il y a ce qu'on appelle la confirmation du bénéficiaire, qui consiste à vérifier si le destinataire correspond bien à celui auquel on souhaite envoyer l'argent. Enfin, il y a les rapports, qui sont des renseignements *post facto*.

• (1630)

Ted Falk: Vous communiquez avec les deux parties participant à la transaction.

Mark Hines: Oui.

Ted Falk: Trouvez-vous que vos échanges sont utiles? Avez-vous connu un certain succès avec ces échanges, que vous avez documenté?

Mark Hines: Oui. Comprenez-moi bien. Il y a beaucoup de place à l'amélioration, mais aujourd'hui, on empêche déjà beaucoup de fraudes. En 2025, on a bloqué 99,8 millions de dollars de fraude sur notre réseau. Notre indicateur principal est mesuré en points de base, et il s'est établi à 3,89 pour l'exercice 2025, ce qui est compa-

rable à celui d'autres réseaux mondiaux, comme Zelle. On veut améliorer ce résultat. Ce n'est pas le meilleur de tous les réseaux, mais on parvient déjà à prévenir beaucoup de fraudes. Ce que l'on essaie de faire, c'est de renforcer encore notre capacité de réaction afin de réduire les répercussions sur les Canadiens.

Le président: Merci, monsieur Falk.

Monsieur Bardeesy, vous avez la parole pour cinq minutes.

Karim Bardeesy (Taiaiaako'n—Parkdale—High Park, Lib.): Je vais partager mon temps avec M. Bains.

J'ai quelques questions pour M. Hines.

Votre marque est très connue, tout comme votre service de virement électronique. Dans quelle mesure les fraudeurs les utilisent-ils ou détournent-ils votre marque et votre logo, par exemple sur les réseaux sociaux, notamment sur les plateformes de Meta, pour usurper votre identité dans le cadre de leurs escroqueries? Quelle est généralement votre réaction face à ce genre de situation?

Mark Hines: La confiance est notre plus grand atout. Les gens utilisent Interac parce qu'ils nous font confiance, et c'est pourquoi la fraude est un enjeu crucial pour nous. Cela peut sembler très banal, mais d'un point de vue purement commercial, si les gens ne se sentent pas à l'aise d'utiliser notre plateforme, ils ne l'utiliseront pas autant.

Avec le PTR, la concurrence nous talonne davantage que par le passé, c'est pourquoi cela revêt une importance particulière. La possibilité de cibler l'utilisation non autorisée de nos marques sur toute plateforme fait partie intégrante de la raison pour laquelle nous encourageons le partage de données; il nous permet de combattre plus efficacement la fraude.

Pour nous, ce n'est pas différent de l'exemple de Wealhtsimple, qui est, encore là, une autre marque de confiance. On rencontre les mêmes difficultés, et l'échange d'information est vraiment ce qu'il nous faut afin de pouvoir mieux cibler le problème.

Karim Bardeesy: J'ai une question pour le CRTC.

Nous avons entendu plus tôt des témoignages selon lesquels Meta bloque des articles de presse, des liens vers des nouvelles, dans le cadre de sa réponse à la Loi sur les nouvelles en ligne. Dans quelle mesure la mise en œuvre du blocage des nouvelles démontre-t-elle leur capacité technique à réagir rapidement à des liens suspects qu'ils peuvent identifier avec une certaine précision? Que pensez-vous de leur incapacité à rétablir l'accès aux liens vers des nouvelles, y compris ceux qui pourraient contribuer à lutter contre la fraude?

Scott Hutton (dirigeant principal, Consommation, analytique et stratégie, Conseil de la radiodiffusion et des télécommunications canadiennes): Nous discutons avec Meta au sujet des nouvelles depuis un certain nombre d'années, et il y a actuellement une instance ouverte devant le CRTC. Lorsque nous leur avons posé des questions, d'après ce que nous avons compris, ils ont adopté une approche très modérée. Ils examinent les sites d'information dignes de confiance, et c'est l'accès à ces sites qu'ils bloquent. Leur approche est très limitée.

Il est certain qu'ils s'efforcent, pour leurs propres raisons, de ne pas diffuser ces nouvelles, et c'est ce qu'ils font. Ils identifient un nombre limité de fraudeurs, soit des centaines plutôt que des centaines de milliers.

Karim Bardeesy: Merci.

Je vais peut-être faire un commentaire plutôt que poser une question, puis je céderai la parole à M. Bains.

L'un des outils dont disposent les députés pour communiquer avec le public, ce sont les bulletins parlementaires mensuels et les bulletins d'information. Parfois, les publications imprimées constituent une ressource inexploitée dans la lutte contre des phénomènes comme la fraude et pour informer les électeurs, en particulier ceux qui maîtrisent moins bien les technologies. Peut-être faudrait-il envisager d'inclure dans nos bulletins parlementaires des informations provenant de vos sources les plus fiables.

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

Merci, monsieur le président.

Je remercie nos témoins de s'être joints à nous aujourd'hui.

Je reviens à un témoin précédent qui est venu ici représenter l'Association canadienne des individus retraités. Comme on le sait, cette communauté est probablement l'une des plus vulnérables. Ce sont des Canadiens qui, en fin de compte, ont bâti notre pays, et l'on doit s'assurer de les protéger.

Dans leurs interventions, ils ont beaucoup parlé du fait que le CRTC pourrait en faire plus en matière de protection. Je sais que vous vous êtes occupés du blocage des appels et avez pris d'autres mesures, mais ils nous ont parlé de lacunes. J'aimerais savoir ceci. Dans le cadre de votre travail, en ce qui a trait aux mesures de protection, constatez-vous des lacunes que vous pourriez combler et sur lesquelles vous tentez d'agir? Vous pourriez peut-être nous en parler un peu.

• (1635)

Steven Harroun: De toute évidence, j'apporte un point de vue différent à cette table. Je suis responsable d'un régime législatif de droit civil. Je ne peux pas faire grand-chose contre les véritables fraudes, les vrais crimes ou les vrais comportements criminels. Dans mon domaine et au sein du service chargé de veiller au respect des règles au CRTC, j'ai adopté une approche qui place la conformité au premier plan, c'est-à-dire veiller à ce que les entreprises légitimes se conforment aux règles de télémarketing, aux règles anti-pourriel, etc.

Dans le même ordre d'idées, si je ne peux pas régler le problème au moyen d'une mesure de conformité, il y a des outils à ma disposition, en tant qu'organisme de réglementation des communications, qui me permettent de demander aux FST de faire certaines choses. C'est là qu'interviennent les mesures stratégiques dont je vous ai parlé. L'un des exemples que j'ai donnés, c'est que des milliards d'appels ont été bloqués grâce à l'intelligence artificielle pour détec-

ter les appels frauduleux. Ainsi, le téléphone ne sonne même pas, les Canadiens ne répondent pas à ces appels et ne sont pas victimes de ces arnaques, ce qui est formidable.

L'une des choses que j'ai mentionnées plus tôt, c'est l'éducation. Je ne sous-estimerai pas le pouvoir de l'éducation, surtout lorsqu'il s'agit de nos aînés et nos communautés vulnérables, comme les nouveaux immigrants qui n'ont ni l'anglais ni le français comme langue maternelle ou les personnes à faible revenu. L'éducation vise à les aider à comprendre les escroqueries, ce qui est tout ce que je peux faire dans un régime civil. Je peux les informer de l'existence de ces escroqueries, leur indiquer les signes à repérer et leur expliquer comment se protéger. Prenez le temps de réfléchir et demandez-vous si ça semble être légitime: est-ce trop beau pour être vrai? Est-ce trop grave pour être vrai? Vérifiez avant de cliquer sur un lien pour réclamer vos 4 millions de dollars. Cette étape de vérification est cruciale.

À mes yeux, en tant qu'organisme de réglementation dans un régime civil, l'éducation est essentielle, car plus les Canadiens sont au courant des arnaques, moins ils sont susceptibles d'en être victimes.

Le président: Merci beaucoup, monsieur Bains.

Chers collègues, c'est tout le temps que l'on a. Le vote aura lieu dans environ deux minutes. Je vais suspendre la séance pour permettre à chacun de voter. Si tout le monde reste dans la salle, ne s'éloigne pas trop et confirme avoir voté, on pourra passer directement aux autres travaux qui nous attendent. Il reste deux heures pour accomplir nos tâches, mais plus vite on s'y mettra, plus vite on pourra partir d'ici.

Je tiens à remercier nos témoins de s'être rendus disponibles aujourd'hui. Cette étude a été très importante et révélatrice.

Comme Mme Begum l'a mentionné plus tôt, l'une des choses que j'apprécie toujours dans ce genre d'étude, c'est d'aller au-delà des lignes partisans. Il y a une volonté de la part de tous les députés de tous les partis, qui représentent les Canadiens de partout au pays, de s'attaquer à cet enjeu. C'est un problème dont tous nos électeurs sont victimes et qui nous préoccupe à juste titre, et l'on ne pourrait pas s'en occuper sans les conseils et l'expertise qu'apportent des personnes comme vous.

Sur ce, je tiens à vous remercier d'être venus nous voir.

Chers collègues, je vais suspendre la séance. Ce sera à vos équipes de s'assurer que vous votez. On se revoit dans quelques minutes.

[La séance se poursuit à huis clos.]

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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