CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA



COMPRENDRE ET PRÉVENIR LA FRAUDE ET LES ESCROQUERIES NUMÉRIQUES ET FINANCIÈRES AU CANADA

Rapport du Comité permanent de l'industrie et de la technologie

Ben Carr, président

NOVEMBRE 2026
45e LÉGISLATURE, 1re SESSION

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.

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 : www.noscommunes.ca

COMPRENDRE ET PRÉVENIR LA FRAUDE ET LES ESCROQUERIES NUMÉRIQUES ET FINANCIÈRES AU CANADA

Rapport du Comité permanent de l'industrie et de la technologie

Le président
Ben Carr

NOVEMBRE 2026

45e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

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

COMITÉ PERMANENT DE L'INDUSTRIE ET DE LA TECHNOLOGIE

PRÉSIDENT

Ben Carr

VICE-PRÉSIDENTS

Adam Chambers

Gabriel Ste-Marie

MEMBRES

Parm Bains

Karim Bardeesy

Doly Begum

Harb Gill

Jason Groleau

Leslyn Lewis

Michael Ma

Bienvenu-Olivier Ntumba

Dominique O'Rourke

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Xavier Barsalou-Duval

Bardish Chagger

Guillaume Deschênes-Thériault

Bruce Fanjoy

Claude Guay

Will Greaves

Lisa Hepfner

Randy Hoback

Anthony Housefather

Natilien Joseph

Tamara Kronis

Viviane Lapointe
Andrew Lawton
Chris Lewis
Chi Nguyen
William Stevenson
Tim Watchorn

GREFFIÈRE DU COMITÉ

Ariane Calvert

BIBLIOTHÈQUE DU PARLEMENT

Marie Dumont, analyste
Dana Fan, analyste
Jesse Good, analyste
Sarah Lemelin-Bellerose, analyste

LE COMITÉ PERMANENT
DE L'INDUSTRIE ET DE LA TECHNOLOGIE

a l'honneur de présenter son

SEPTIÈME RAPPORT

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

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS 1

COMPRENDRE ET PRÉVENIR LA FRAUDE ET LES ESCROQUERIES NUMÉRIQUES ET FINANCIÈRES AU CANADA 7

- Introduction 7
- Le rôle des intervenants : Les entreprises de télécommunications et les plateformes de médias sociaux 10
  - Les banques, les institutions financières et Paiements Canada 12
  - Les entreprises de télécommunications 14
  - Les plateformes de médias sociaux et les entreprises technologiques 16
- L'approche canadienne de lutte contre la fraude financière 19
  - Prévention et éducation 21
  - L'échange de données entre les secteurs 23
  - La responsabilité en matière de fraude au Canada 24
  - L'application de la loi 26
- Pratiques exemplaires : Les leçons tirées de l'Australie 28
- Conclusion 30

ANNEXE A : LISTE DES TÉMOINS 31

ANNEXE B : LISTE DES MÉMOIRES 33

DEMANDE DE RÉPONSE DU GOUVERNEMENT 35

LISTE DES RECOMMANDATIONS

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

Recommandation 1

Que le gouvernement du Canada supprime les obstacles juridiques et réglementaires inutiles qui empêchent l'échange en temps opportun de renseignements pertinents entre les institutions financières, les fournisseurs de services de télécommunications, les plateformes numériques, les organismes publics, les forces de l'ordre et les partenaires internationaux; réduise les retards nuisant à l'échange des renseignements nécessaires au recouvrement des fonds; et introduise des dispositions d'exonération protégeant les organisations qui communiquent des renseignements de bonne foi à des fins de détection, de prévention, d'enquête et de recouvrement en matière de fraude contre toute responsabilité au titre des lois applicables sur la protection des renseignements personnels et la concurrence.

Recommandation 2

Que le gouvernement du Canada élabore des protocoles normalisés d'échange de données entre les intervenants de la lutte contre la cybercriminalité et la fraude financière, tout en protégeant les renseignements personnels et en améliorant la qualité des renseignements disponibles concernant les types d'escroqueries et les caractéristiques démographiques des victimes.

Recommandation 3

Que le gouvernement du Canada accélère la mise en œuvre de la Stratégie nationale antifraude annoncée dans le budget de 2025 et la création de l'Agence contre les crimes financiers, et utilise ce cadre pour établir un régime coordonné et multisectoriel de prévention des escroqueries – qui réunirait les institutions financières, les fournisseurs de services de télécommunications, les plateformes numériques, les organismes de réglementation, les forces de l'ordre et d'autres parties prenantes concernées – afin d'échanger des renseignements, de suivre l'évolution rapide du monde de la fraude financière et d'y répondre, dans le but de fournir de la rétroaction aux gouvernements

fédéral, provinciaux et territoriaux, tout en tirant des leçons de l'approche intersectorielle coordonnée de l'Australie.

Recommandation 4

Que le gouvernement du Canada exige des entreprises de réseaux sociaux qu'elles vérifient que chaque annonceur de services financiers est une entité légitime et réglementée avant d'accepter et de publier des publicités.

Recommandation 5

Que le gouvernement du Canada exige des plateformes qu'elles suppriment immédiatement les publicités frauduleuses et les annonceurs frauduleux récidivistes dès qu'elles sont informées par des institutions financières ou des organisations légitimes faisant l'objet d'une usurpation d'identité, et qu'elles autorisent la suppression en masse plutôt que d'exiger des entreprises de technologies financières et des institutions financières qu'elles signalent chaque publicité individuellement.

Recommandation 6

Que le gouvernement du Canada veille à ce que les sanctions financières imposées par les autorités canadiennes de réglementation des valeurs mobilières pour les formes les plus graves d'inconduite sur les marchés ne soient pas annulées par une procédure de faillite, en modifiant le paragraphe 178(1) de la *Loi sur la faillite et l'insolvabilité*, de manière à ajouter la fraude, la manipulation du marché et les fausses déclarations à la liste des dettes qui ne sont pas effacées par la faillite.

Recommandation 7

Que le gouvernement du Canada continue de soutenir la Coalition canadienne antifraude et le Centre antifraude du Canada.

Recommandation 8

Que le gouvernement du Canada exige aux plateformes numériques qui gèrent des canaux publicitaires en ligne, quel que soit le volume de transactions, de divulguer publiquement leurs budgets consacrés à la prévention de la fraude, ventilés de manière générale entre les campagnes de sensibilisation du public et le développement d'outils internes.

Recommandation 9

Que le gouvernement du Canada exige que les institutions financières, les fournisseurs de services de télécommunications et les plateformes numériques mettent en œuvre des mesures documentées – y compris, sans s'y limiter, des boîtes de dialogue de confirmation explicite nécessitant un clic avant de valider une transaction ou de rediriger vers un autre site Web – afin d'alerter et de sensibiliser aux escroqueries, leurs clients et leurs utilisateurs, en temps opportun et qu'il envisage des mécanismes visant à tenir les organisations responsables des escroqueries commises au moyen de leurs canaux, y compris des sanctions financières qui imposent aux canaux ayant permis ces escroqueries le fardeau de verser des remboursements proportionnés aux victimes.

Recommandation 10

Que le gouvernement du Canada soutienne le renforcement de l'éducation et de la sensibilisation du public, adaptées aux différents types d'escroqueries et aux différentes catégories démographiques, y compris sur la manière et les lieux où signaler les fraudes et les escroqueries.

Recommandation 11

Que le gouvernement du Canada établisse un cadre national et intersectoriel de lutte contre la fraude qui définit clairement les responsabilités des institutions financières, des fournisseurs de services de télécommunications, des plateformes numériques, des organismes de réglementation et des forces de l'ordre; qu'il fasse appel dans la mesure du possible aux organismes de réglementation et autres qui sont déjà en place et qu'il demande aux entités concernées par la fraude de produire annuellement des rapports présentant des résultats mesurables, notamment sur les pertes liées à la fraude, les fonds recouvrés, le contenu frauduleux supprimé, les appels frauduleux, les messages textes bloqués et les résultats en matière d'application de la loi.

Recommandation 12

Que le gouvernement du Canada précise et, dans la mesure du possible, renforce les mesures de protection offertes par la loi pour permettre aux institutions financières, aux fournisseurs de services de télécommunications, aux plateformes numériques et aux organismes publics concernés d'échanger rapidement et de bonne foi des informations utiles signalant des fraudes sous

réserve des mesures de protection de la vie privée, dans le respect de limites établies, et mette en place un processus pour corriger la situation en cas de fausses alertes.

Recommandation 13

Que le gouvernement du Canada passe par les organismes de réglementation sectoriels pour établir des attentes raisonnables fondées sur le risque concernant les activités de fraude à risque élevé, et qu'il envisage notamment la vérification des annonceurs dans le cas de produits financiers et d'investissement; qu'il exige une action rapide lorsque l'existence d'un contenu frauduleux est confirmée, le renforcement des mesures visant à bloquer et à retracer les appels et les messages textes falsifiés ainsi que la communication d'avertissements ciblés ou des mesures de protection facultatives pour les transferts inhabituels, et ce, tout en préservant les communications légitimes, en permettant aux consommateurs de faire des choix et en offrant des recours viables.

Recommandation 14

Que le gouvernement du Canada renforce la capacité du Centre antifraude du Canada à faire appel aux structures fédérales en place, notamment en continuant à offrir des options de signalement par téléphone et en ligne, des services de triage et d'aiguillage centrés sur les victimes, en uniformisant la collecte d'information, et en ajoutant à ses publications les conclusions des rapports d'enquête sur la fraude.

Recommandation 15

Que le gouvernement du Canada collabore avec les organismes actuels de réglementation des services financiers, Paiements Canada, les institutions financières et le Centre antifraude du Canada afin d'établir rapidement des protocoles clairs en ce qui concerne la communication d'avis aux institutions destinataires, le rappel ou le gel des transferts suspects dans la mesure où la loi le permet et l'évaluation de la proportion et de la valeur des fonds de la victime qui sont recouvrés.

Recommandation 16

Que le gouvernement du Canada demande aux organismes actuels de réglementation sectoriels d'élaborer des paramètres canadiens de prévention

de la fraude pour les grandes institutions financières, les fournisseurs de services de télécommunications et les plateformes numériques, notamment en ce qui concerne la vérification du contenu frauduleux, la suppression de comptes, les délais d'intervention, le blocage des appels et des messages textes frauduleux, les fonds recouvrés, les fausses alertes et les recours, et que les résultats obtenus soient publiés périodiquement.

Recommandation 17

Que le gouvernement du Canada accorde la priorité à la lutte contre la fraude transfrontalière organisée occasionnant de fortes pertes en ce qui concerne les ressources au sein de la GRC et du Centre antifraude du Canada; améliore la formation spécialisée et l'accès à des outils d'enquête licites offerts aux services de police; renforce la coopération avec les partenaires provinciaux, territoriaux et internationaux; et produise des rapports sur les enquêtes, les accusations, les condamnations, les opérations perturbées et les fonds recouvrés.

Recommandation 18

Que le gouvernement du Canada, lors de l'élaboration de règlements qui touchent les banques et les institutions financières, maintienne la capacité des institutions financières de prévoir les périodes de retenues et les limites sur les chèques et d'autres produits papier susceptibles d'être altérés, contrefaits ou négociés de manière frauduleuse.

COMPRENDRE ET PRÉVENIR LA FRAUDE ET LES ESCROQUERIES NUMÉRIQUES ET FINANCIÈRES AU CANADA

INTRODUCTION

Imaginez un vieil homme qui reçoit un appel de son petit-fils, lequel lui raconte qu'il a été victime d'un accident de voiture et a besoin d'argent. L'homme passe à la banque pour aller chercher de l'argent et le donne à un étranger ou encore procède à un transfert électronique vers une adresse électronique qui lui semble familière. Ce n'est qu'après coup, après avoir parlé à sa famille, qu'il découvre que l'appel ne venait pas de son petit-fils, mais d'une personne utilisant la technologie pour reproduire la voix de son proche. L'argent est disparu; toute cette affaire était une arnaque. Donné par Ian Paterson, président-directeur général de Plurilock Security, cet exemple ne fait qu'illustrer le problème grandissant de la fraude financière au Canada.

Aux termes du paragraphe 380(1) du *Code criminel*, commet une fraude quiconque, « par supercherie, mensonge ou autre moyen dolosif », dépossède illégalement le public ou une personne « de quelque bien, service, argent ou valeur ». Selon le Centre antifraude du Canada, en 2025, les Canadiens ont perdu plus de 704 millions de dollars à cause de fraudes, marquant la pire année à ce jour. De plus, entre 2022 et 2026, les pertes liées à la fraude signalées par les Canadiens dépassent 2,4 milliards de dollars. Or, le montant véritable de ces pertes est sans doute beaucoup plus élevé, le Centre estimant que seulement 5 à 10 % des cas de fraude sont signalés. D'ailleurs, David Shipley, directeur général de Beauceron Security, évaluait les pertes liées à la fraude au Canada en 2025 entre 7 et 14 milliards de dollars, précisant que ces pertes avaient augmenté de 326 % depuis 2020.

Les témoins ont souligné la portée mondiale et transnationale des activités frauduleuses et des escroqueries. Jeanette Patell, directrice des Affaires gouvernementales et des politiques publiques chez Google Canada, a expliqué que :

> Les fraudes et les escroqueries financières font des victimes et minent la confiance essentielle à l'écosystème numérique. Cet enjeu de société a pris de l'ampleur et gagné en complexité, les pertes mondiales liées à la fraude étant estimées à près de 580 milliards de dollars pour 2025, selon le « Global Financial Crime Report » de Nasdaq. Ce phénomène est alimenté par des opérations criminelles transnationales sophistiquées qui combinent des méthodes en ligne et hors ligne.

Dans la même veine, Ian Paterson a indiqué que « [c]ertaines 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. » Jeanette Patell a précisé qu'« il s'agit d'une lutte sans fin. Nous avons affaire à des organisations criminelles de pointe qui s'adaptent constamment et cherchent constamment de nouvelles vulnérabilités à exploiter. » Selon Ian Paterson, le Canada doit « investir davantage dans l'aide internationale afin de contribuer à démanteler ces réseaux à la source, avant qu'ils n'atteignent les Canadiens ».

Les trois principales fraudes signalées au Canada en 2025 étaient liées à l'identité, à l'investissement et aux services, tandis que celles ayant entraîné les répercussions financières les plus importantes étaient liées à l'investissement, aux relations sentimentales et à l'emploi. Comme l'a expliqué Jennifer Quaid, directrice exécutive d'Échange canadien de menaces cybernétiques, « [l]a menace à laquelle nous faisons face ne vient pas d'amateurs opportunistes. Il s'agit de réseaux de criminels organisés, qui utilisent des technologies sophistiquées et qui suivent des modèles opérationnels professionnels. » Le Canadian Anti-Monopoly Project a fait remarquer que « [d]ans les cas de fraude où la personne donne son approbation [comme dans l'exemple ci-dessus], la victime n'a probablement aucune chance d'obtenir réparation » [TRADUCTION].

Vu l'intensification du phénomène au Canada, le 22 septembre 2025, le Comité permanent de l'industrie et de la technologie de la Chambre des communes (le Comité) a adopté la motion suivante :

> Que, conformément à l'article 108(2) du Règlement, le Comité permanent de l'industrie et de la technologie entreprenne une étude sur les fraudes financières et les escroqueries au Canada, en reconnaissant qu'il s'agit d'une menace importante et croissante pour les consommateurs et l'économie, afin d'identifier les meilleures pratiques de prévention et de renforcer le cadre canadien de lutte contre la fraude;
>
> Que l'étude examine :
>
> - le rôle des banques, des entreprises de télécommunications et des plateformes numériques dans la prévention des escroqueries et la protection des consommateurs;
>
> - les responsabilités d'Innovation, Sciences et Développement économique Canada, du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et du Centre antifraude du

Canada, ainsi que d'autres ministères et organismes fédéraux en matière d'application de la loi, de réglementation et de sensibilisation du public;

- l'adéquation des lois sur la protection des consommateurs, de la capacité d'application de la loi et de la coordination interinstitutionnelle;
- l'impact des technologies émergentes, y compris l'intelligence artificielle, sur la facilitation et la lutte contre la fraude;
- les meilleures pratiques d'autres juridictions, telles que l'Australie, pour améliorer les mesures de prévention et d'application; et
- les conséquences économiques et sociales plus larges pour les Canadiens.

Que le Comité invite la ministre de l'Industrie à comparaître pendant au moins une heure dans le cadre de cette étude, ainsi que des témoins des ministères et organismes concernés, des représentants de l'industrie et des experts;

Que le Comité tienne au moins quatre réunions sur cette étude; et

Que le Comité fasse rapport de ses conclusions et recommandations à la Chambre[1].

Au cours des cinq réunions tenues entre les 4 et 18 juin 2026, le Comité a entendu 22 témoins, y compris des représentants de banques et d'organisations de paiements, d'entreprises de technologies et de médias sociaux, d'organismes de cybersécurité, de fournisseurs de services de télécommunications, de forces de l'ordre, d'organismes de réglementation financière, de groupes de défense des intérêts des consommateurs et d'associations industrielles internationales. Il a également reçu 15 mémoires aux fins de cette étude. Le présent rapport résume les témoignages reçus, présentant les points de vue des intervenants de l'industrie, du gouvernement et du public. Il donne un aperçu des organismes canadiens, des initiatives menées par certains et des lois en place dans le contexte de la lutte contre la fraude. Il présente également ce que le Comité a appris de l'expérience de l'Australie en la matière. Il présente des recommandations à

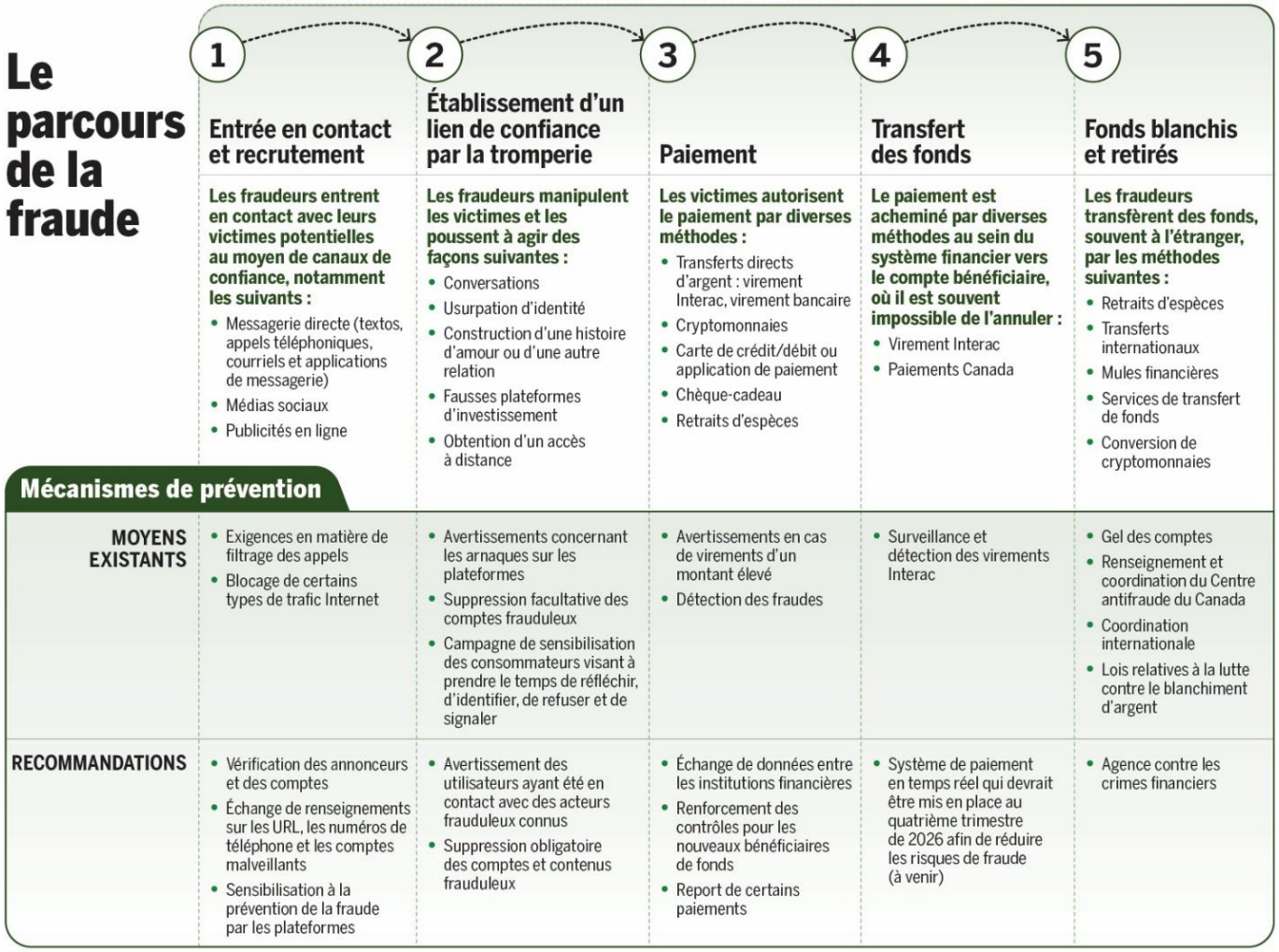
1 INDU, *Procès-verbal*, 22 septembre 2025.

l'intention du gouvernement pour l'aider à lutter contre le problème persistant et grandissant de la fraude financière.

LE RÔLE DES INTERVENANTS : LES ENTREPRISES DE TÉLÉCOMMUNICATIONS ET LES PLATEFORMES DE MÉDIAS SOCIAUX

Diverses parties, y compris les banques et les institutions financières, les entreprises de télécommunications, les médias sociaux et les plateformes numériques peuvent se retrouver à faciliter des transactions frauduleuses et des escroqueries, même si elles sont à l'avant-plan des activités de prévention. Eric Smith, vice-président principal de l'Association canadienne des télécommunications, a déclaré que la « prévention de la fraude est plus efficace lorsque les fournisseurs de services de télécommunication, les institutions financières, les plateformes numériques, les organismes gouvernementaux et les forces de l'ordre collaborent et s'échangent des renseignements ». Dans la même veine, Mark Hines, chef des produits de prévention de la fraude chez Interac Corp., a observé que « 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 ». D'ailleurs, David Pegley, directeur général, Australian Financial Crimes Exchange Ltd., a signalé que bien que le secteur bancaire collabore déjà avec les services du renseignement pour détecter les acteurs malveillants, il importe de se rappeler que les plateformes numériques et les entreprises de télécommunications sont de « solides compétiteurs », et donc « [l]'idée selon laquelle ils collaboreraient est un concept étranger ». La présente section examine le rôle de ces secteurs en matière de lutte contre la fraude et les escroqueries au Canada. La figure 1, ci-dessous, présente un exemple des étapes d'une fraude financière.

Figure 1 — Le parcours de la fraude financière



Source : Préparée par la Bibliothèque du Canada à l'aide de données du gouvernement du Canada.

Les banques, les institutions financières et Paiements Canada

Anthony Ostler, président et chef de la direction de l'Association des banquiers canadiens, a souligné que les banques canadiennes « investissent massivement dans la prévention de la fraude, la formation en cybersécurité et la sensibilisation des clients » précisant toutefois qu'« aucune organisation ni aucun secteur ne peut à lui seul endiguer efficacement cette vague ». De même, Mark Hines a présenté le point de vue d'Interac, qui estime que la fraude « touche de multiples industries et secteurs » et qu'« [a]ucune entreprise ou aucun secteur ne peut résoudre ce problème à lui seul ». Conscient de cette réalité dans le cas des banques, Tru Cooperative Bank explique dans son mémoire qu'elle « travaille également en étroite collaboration avec les prestataires de services de paiement, les partenaires du secteur, les autorités de régulation, les forces de l'ordre et des organismes tels que le Centre canadien de lutte contre la fraude et le [Centre d'analyse des opérations et déclarations financières du Canada] CANAFE afin de partager des informations et de soutenir des réponses coordonnées face aux menaces émergentes ».

Pour leur part, les banques, les institutions financières et Paiements Canada déploient des efforts pour combattre la fraude. Colin Smith, vice-président, Sciences du risque et de la décision chez Wealthsimple, a expliqué que Wealthsimple fait appel à des clés d'accès, à des emplacements de confiance et à des avertissements en temps réel pour lutter contre les fraudeurs. Par exemple, il a expliqué que « [s]i quelqu'un transfère de l'argent à l'aide de notre application [Wealthsimple] pendant qu'il est au téléphone, un avertissement s'affiche pour indiquer que l'appel ne provient pas de nos bureaux ». Ila précisé que lorsqu'« 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 ». Anthony Ostler a parlé de l'une des « plus grandes réalisations » de l'Association des banquiers canadiens, soit le lancement de la campagne de sensibilisation « Ensemble contre la fraude », qui appelle à l'action avec son slogan « Arrêtez. Vérifiez. Parlez-en ». Pour sa part, David Shipley a recommandé que les banques « propos[ent] à leurs clients des formations sur la fraude et assure[nt] un suivi ».

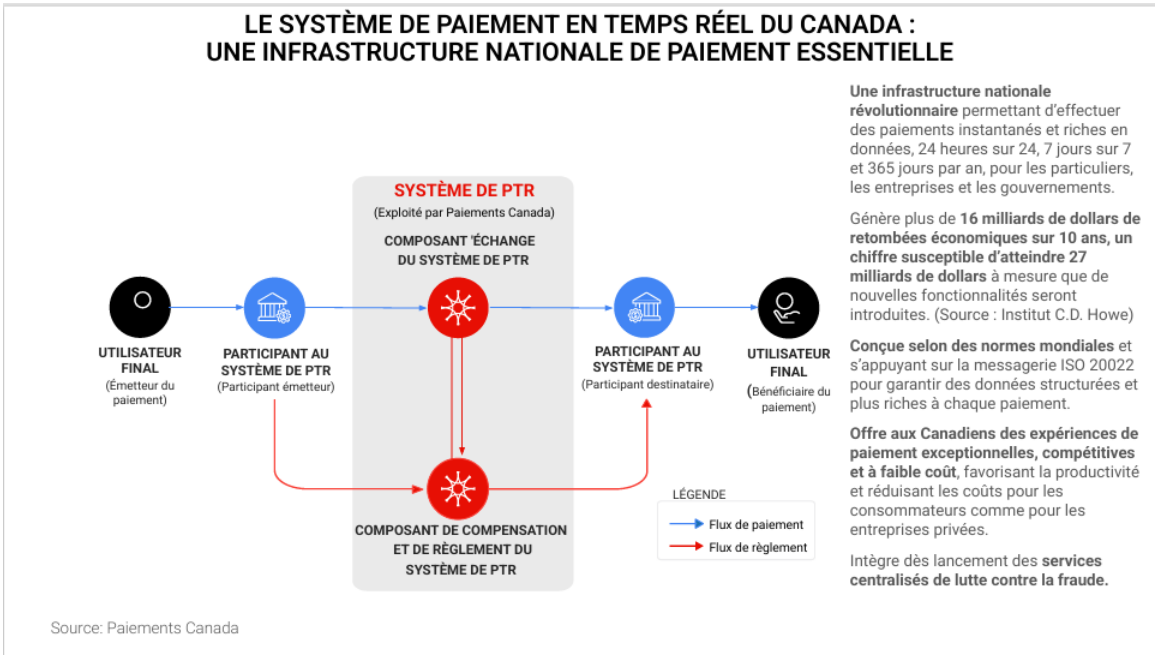
Dans son mémoire au Comité, Paiements Canada présente les observations suivantes :

> La pièce maîtresse de l'innovation financière du Canada – et la contribution la plus importante de Paiements Canada à la lutte nationale contre la fraude – est le système

de PTR[2] [qi sera lancé au quatrième trimestre de cette année], de même que les services centralisés de lutte contre la fraude. Combiné à l'élargissement de l'adhésion et à nos systèmes, le système de PTR favorisera la concurrence, l'innovation, la croissance économique et l'inclusion financière grâce aux avantages qui suivent : paiements instantanés et irrévocables, disponibilité en tout temps, messages ISO 20022[3] riches en données.

La figure 1, ci-dessous, illustre le processus de paiement du système PTR qui sera bientôt mis en place au Canada.

Figure 2 — Le système de paiements en temps réel du Canada



Source : Paiements Canada.

Colin Smith a toutefois souligné que « [l]es institutions financières et les clients peuvent travailler ensemble pour lutter contre la fraude, mais la plupart des fraudes ne proviennent pas du système financier ». Pour illustrer ce point, plusieurs institutions financières, dont Interac, ont parlé du problème des publicités frauduleuses où sont représentées leurs entreprises sur les plateformes de médias sociaux, celles de Facebook

2 Le système de paiement en temps réel (PTR) est le futur système de paiement numérique de Paiements Canada, qui permettra de régler en quelques secondes des transactions d'un montant maximal de 100 000 $. Les paiements seront définitifs et immédiats dès leur règlement.

3 La norme 20022 de l'Organisation internationale de normalisation (ISO) est une norme mondiale unique régissant l'échange de données électroniques entre les institutions financières.

et d'Instagram de Meta étant utilisées couramment pour ce genre de publicités frauduleuses. À titre d'exemple, Colin Smith a indiqué que Wealthsimple avait signalé à Meta plus de 10 000 publicités frauduleuses dans lesquelles les fraudeurs utilisaient le nom et le logo de l'entreprise. Il a ajouté qu'il s'écoulait « quatre jours […] en moyenne entre le moment du signalement à Meta et le retrait de ces publicités ». Ces exemples remettent en question la volonté de Meta de supprimer rapidement les contenus publicitaires frauduleux sur ses plateformes.

Des représentants des secteurs bancaires et financiers ont commenté les approches et l'orientation du gouvernement du Canada en matière de lutte contre la fraude financière. Par exemple, Frédéric Lapalme, directeur principal et chef délégué de l'unité Encadrement et surveillance, lutte contre la fraude et les crimes financiers au sein du Mouvement des caisses Desjardins, a indiqué que Desjardins voyait d'un bon œil les engagements du gouvernement canadien, notant qu'il « faut éviter de placer la fraude dans un cadre réglementaire trop rigide ». Il a indiqué que les institutions du Mouvement des caisses Desjardins effectuent des milliards de transactions par année et estimait qu'elles doivent « 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 ».

David Shipley a recommandé que l'on évite de créer un modèle de responsabilité qui repose uniquement sur les banques, car selon lui, les coûts liés à la fraude ne feraient alors qu'augmenter pour les consommateurs. Il a souligné que « les banques n'assument jamais ces coûts. Les coûts seront répercutés sur vos électeurs sous forme de frais de services et d'intérêts. » Anthony Quinn, président de l'Association canadienne des individus retraités, a présenté un autre point de vue, selon lequel les banques « devraient assumer une plus grande responsabilité » à l'égard des pertes découlant de manœuvres frauduleuses. Fintechs Canada a convenu que « ces risques exige[nt] une intervention plus large, à l'échelle de l'écosystème, et non seulement des solutions ponctuelles », proposant que ce « n'est qu'en harmonisant les incitatifs, en clarifiant les rôles et en permettant un partage sécurisé des données à l'échelle de cet écosystème élargi que le Canada pourra combler les lacunes exploitées par les fraudeurs ».

Les entreprises de télécommunications

Eric Smith a expliqué le rôle des entreprises de télécommunications, les décrivant comme des fournisseurs qui « acheminent l'enveloppe », mais « ne lisent pas le courrier ». Il a parlé des mesures prises par ces entreprises, par exemple :

> [L]e blocage de certains types d'appels; les outils de prévention de l'usurpation d'identité de l'appelant, comme les programmes de blocage de numéros sortants et la mise en œuvre de la norme STIR/SHAKEN[4]; les capacités de traçage des appels pour aider à trouver l'origine des appels frauduleux; l'analyse au niveau du réseau pour détecter et signaler les communications suspectes; les systèmes de signalement des pourriels; les mesures de protection de l'identité et des comptes; ainsi qu'une collaboration continue avec les forces de l'ordre et les organismes gouvernementaux.

Carey Frey, chef de la sécurité chez Telus, a souligné que malgré ces efforts, « [l]a triste réalité est qu'il est possible d'usurper l'identité de l'expéditeur d'appels téléphoniques et de SMS ». Il a indiqué que bien que l'industrie canadienne des télécommunications ait mis au point des protocoles sécurisés pour contrer l'usurpation d'identité, il faudrait que tous les pays fassent de même pour contrer efficacement la fraude. Eric Smith était d'accord avec ce point, notant que « si cette technologie n'est pas adoptée dans le pays d'où provient l'appel, par exemple, elle ne remplit pas cette fonction ». S'exprimant au nom des retraités, Anthony Quinn était d'avis 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 ». Il a demandé 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. »

Carey Frey a présenté certaines limites, soulignant que « les fournisseurs de services de télécommunication pourraient bloquer davantage de trafic frauduleux sur nos réseaux, mais aujourd'hui, le risque de responsabilité limite nos possibilités d'action ». Il a précisé que des « dispositions d'exonération protégeant ceux qui prennent de bonne foi des mesures antifraude contribueraient à protéger les Canadiens sans coût supplémentaire pour les contribuables ». Dans ce contexte, il s'agit de dispositions législatives ou réglementaires qui protégeraient les fournisseurs de services de télécommunication contre toute responsabilité s'ils bloquaient accidentellement des communications légitimes. Plus précisément, Eric Smith a indiqué que

> [l]'article 36 de la *Loi sur les télécommunications* leur interdit de bloquer de leur propre chef des communications sans autorisation expresse du Conseil de la radiodiffusion et des télécommunications canadiennes. Cette restriction est un élément fondamental du cadre canadien de neutralité du Net et vise à garantir que les mesures de lutte contre la

4 STIR (Secure Telephony Identity Revisited) et SHAKEN (Signature-based Handling of Asserted Information using toKENs) forment un ensemble de protocoles de télécommunications conçus pour empêcher l'usurpation illégale de l'identité de l'appelant sur les réseaux IP.

fraude ne bloquent pas par inadvertance le trafic légal ni n'interfèrent avec les communications essentielles.

Selon Steven Harroun, dirigeant principal de la Conformité et des enquêtes au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), « [e]n 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. »

Les plateformes de médias sociaux et les entreprises technologiques

Ce sont sur les réseaux sociaux que prennent souvent naissance de nombreux cas de fraude. Par exemple, comme l'a rapporté The Sunday Times le 6 juin 2026, la Lloyds Bank, au Royaume-Uni, a constaté que plus des deux tiers (68 %) des signalements de fraude faits par ses clients avaient pour origine une plateforme de Meta. Le Comité a entendu des représentants de plateformes de médias sociaux et d'entreprises technologiques, dont Meta et Google, qui ont présenté les efforts déployés par ces entreprises pour lutter contre la fraude et les escroqueries, et qui ont aussi répondu à des questions sur les profits tirés par leurs entreprises des publicités frauduleuses. Selon le Canadian Anti-Monopoly Project, « la responsabilité des plateformes de réseaux sociaux se situe actuellement dans une zone grise juridique » [TRADUCTION]. Les témoins ont présenté des suggestions concernant la réglementation des médias sociaux en matière de fraude.

Jon Camfield, responsable de la défense, Politique sur la sécurité, Meta Platforms Inc., a fait valoir que « Meta investit énormément dans le partage intersectionnel d'information », mentionnant FIRE, son programme d'échange réciproque du renseignement sur la fraude, qui permet un échange bidirectionnel d'information avec des institutions financières, ainsi que le projet Global Signal Exchange, une initiative menée en collaboration avec Oxford Information Labs, Google et la Global Anti-Scam Alliance. En avril 2026, le centre Échange canadien de menaces cybernétiques s'est joint à cette initiative. Jeanette Patell a déclaré que Google investit « depuis plus de 20 ans dans des technologies de pointe, des politiques robustes, des actions en justice et des équipes d'experts consacrées à la protection des utilisateurs de [ses] produits et services ». Elle a précisé qu'en 2025, Gemini, l'outil d'intelligence artificielle de Google, avait permis « d'intercepter plus de 99 % des publicités contrevenant à [ses] politiques avant même leur diffusion ».

Or, selon un article de *Reuters* datant de novembre 2025, Meta estimait que 10 % de ses revenus de 2024 proviendraient de publicités pour des escroqueries et des produits

interdits. Considérant ce chiffre comme « une fausse représentation », Jon Camfield évaluait ces revenus plutôt autour de 3 ou 4 % en 2024. Selon Meta Investor Relations, en 2024, le chiffre d'affaires total de Meta s'élevait à 164,5 milliards de dollars américains. Jon Camfield a indiqué qu'en 2025, Meta avait réussi à réduire le nombre de publicités frauduleuses signalées de plus de 50 %. Des témoins, y compris les représentants de Wealthsimple et d'Interac, ont néanmoins attiré l'attention sur l'utilisation problématique de leur entreprise dans des publicités frauduleuses affichées sur les plateformes de Meta. Wealthsimple a déclaré qu'entre octobre 2025 et janvier 2026, l'entreprise avait signalé 10 000 publicités de cette nature parues sur les plateformes de Meta, et que plus récemment, elle en avait signalé jusqu'à 1 500 par jour. Lorsqu'on lui a demandé si Meta laissait volontairement des fraudeurs accéder à son site et tenait compte des publicités frauduleuses dans le cadre de l'analyse de rentabilité du site, Rachel Curran, directrice de la Politique publique chez Meta Canada, a répondu ceci : « Je suis tout à fait en désaccord avec cela. C'est n'importe quoi. »

Dans son mémoire au Comité, Meta expliquait également qu'au cours des dix dernières années, l'entreprise avait investi, à l'échelle mondiale, plus de 30 milliards de dollars américains dans la sécurité, précisant qu'il est difficile de décrire les investissements réalisés dans un pays donné en raison de la nature transnationale des manœuvres frauduleuses et des escroqueries. Comme l'indique Meta Investor Relations, en 2025, Meta a réalisé un chiffre d'affaires de près de 201 milliards de dollars américains. Depuis qu'elle est devenue publique en 2012, l'entreprise a cumulé des revenus de plus de 1 000 milliards de dollars américains et des profits supérieurs à 328,5 milliards de dollars américains.

Colin Smith a fait valoir que le signalement des publicités au cas par cas – ce que fait actuellement Wealthsimple pour les publicités sur Meta – est « un jeu perdu d'avance », ajoutant que Meta n'offre pas de solution applicable à l'ensemble de la plateforme pour régler le problème au Canada. Selon lui, « [l]a 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 ». Reconnaissant qu'il s'agit là d'une « solution intéressante » et d'un « outil de plus », Frédéric Lapalme a ajouté que « [ç]a ne réglera 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. » Quant à Meta, Jon Camfield a expliqué que l'entreprise renforçait « la vérification des annonceurs; [son] objectif, c'est que 90 % de [ses] revenus publicitaires viennent d'annonceurs confirmés d'ici la fin de 2026, comparativement à 70 % à la fin de 2025 ».

Des membres du Comité ont demandé si Meta était prêt à partager sur sa plateforme des articles de nouvelles qui contiennent de l'information exploitable sur les moyens à prendre pour lutter contre la fraude. À cette question, Rachel Curran a offert un refus, déclarant que la « *Loi sur les nouvelles en ligne* ne nous permet pas d'afficher ne serait-ce qu'un article sur Facebook ou Instagram, à moins de nous conformer à l'ensemble du cadre établi dans ladite loi ». Parlant de la capacité de Meta, sur le plan technique, à supprimer des liens de ses sites, qu'il s'agisse d'informations ou de nouvelles frauduleuses, Rachel Curran a soutenu que l'entreprise respectait la *Loi sur les nouvelles en lignes* en éliminant le contenu lié à l'actualité de ses plateformes. Au sujet des interactions du CRTC avec Meta quant à cette capacité technique d'empêcher les articles de nouvelles d'être communiqués, Scott Hutton, dirigeant principal de la section Consommation, analytique et stratégie au CRTC, a déclaré que l'entreprise avait adopté « une approche très modérée », bloquant l'accès à des sites de nouvelles de confiance. Il a fait remarquer qu'il n'y a pas beaucoup de véritables sites de nouvelles, alors qu'il y a des centaines de milliers de sites frauduleux.

En ce qui concerne Google, Jeanette Patell a soutenu que Google a « élaboré [son] modèle d'affaires et [ses] mécanismes d'application des règles de manière à ne pas tirer profit de ce type d'activités » et que l'entreprise est « en mesure de bloquer ces publicités avant qu'elles ne soient vues par les utilisateurs afin qu'elles n'entrent pas dans [son] écosystème ». En outre, en réponse à une question à savoir si Google percevait des revenus pendant qu'une publicité frauduleuse est visible sur YouTube, Jeanette Patell a répondu ceci : « Tout dépend vraiment des circonstances; je ne peux pas vous donner une réponse précise quant au modèle de revenus applicable à une publicité en particulier. ». Elle a indiqué que les plateformes de Google, comme YouTube, ont en place un processus de vérification des annonceurs, imposant des exigences de vérification encore plus rigoureuses pour les secteurs névralgiques ou à risque élevé, comme les services financiers. De plus, de façon générale, Google ne permet pas les publicités sur la cryptomonnaie, exigeant dans les rares cas où elles sont permises, une inscription auprès du CANAFE.

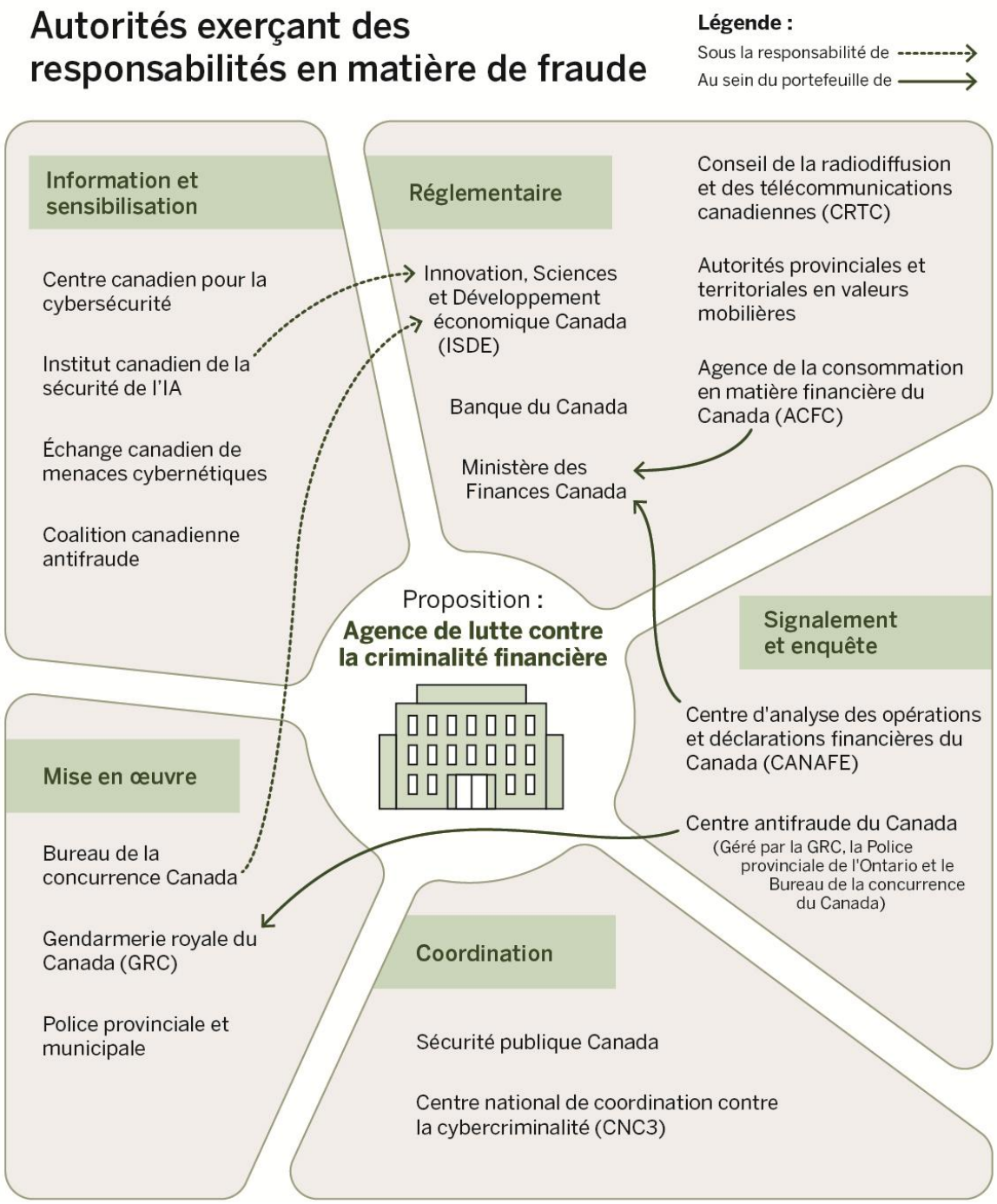
Dans un mémoire intitulé *Clickbait Cures: Unmasking the Deceptive Health Ad Infrastructure on Meta and Google*, Reset Tech s'est penché sur la publicité médicale frauduleuse diffusée sur les plateformes Meta et Google dans l'Union européenne et a constaté que ces entreprises hébergeaient des publicités frauduleuses contraires à leurs propres politiques internes. Reset Tech soulignait que « ni Facebook ni Google ne bannissent systématiquement les annonceurs problématiques; ils se concentrent plutôt sur la suppression de publicités individuelles. À moins que le problème ne soit traité au niveau du réseau en application de règles plus strictes sur les publicités liée à la santé, ces campagnes se poursuivront [TRADUCTION]. » Quant à Google et sa capacité de

supprimer les publicités frauduleuses, Jeanette Patell a expliqué que le rôle de Google « consiste à évaluer le contenu, y compris les publicités, pour déterminer s'il contrevient à [ses] politiques. Nous ne pouvons pas conclure à son caractère frauduleux. Cette responsabilité appartient aux forces de l'ordre. »

L'APPROCHE CANADIENNE DE LUTTE CONTRE LA FRAUDE FINANCIÈRE

Concernant le cadre juridique actuellement en vigueur au Canada, Carey Frey a soutenu que « [l]e Canada dispose déjà d'une grande partie de ce dont il a besoin pour lutter plus efficacement contre la fraude. Le Centre antifraude du Canada, les organismes de réglementation sectoriels, les forces de l'ordre et les coalitions du secteur privé sont déjà en place. Ce qui manque, c'est une force de coordination centrale qui veille à ce que les meilleurs outils et renseignements parviennent à ceux qui en ont besoin. » Dans son mémoire soumis à titre personnel, Kevin Cosgrove, éducateur en sécurité numérique, a avancé que le « problème réside dans le fait que les mesures actuelles destinées au public demeurent trop fragmentées, trop réactives et trop souvent axées sur la transmission d'informations plutôt que sur la capacité du public à les assimiler, à les mémoriser et à les appliquer sous pression ». Dans le même ordre d'idées, Jennifer Quaid a déclaré que « [s]i nos interventions restent fragmentées, les escrocs continueront à nous déjouer ». La section qui suit présente le cadre juridique en place au Canada, notamment les lois sur la protection des consommateurs, la capacité d'application de la loi et la coordination entre les organisations en matière de prévention, de communication d'informations, de responsabilité et de respect des règles. La figure 3 ci-dessous présente un aperçu des autorités chargées de la lutte contre la fraude au Canada.

Figure 3 — Autorités exerçant des responsabilités en matière de fraude financière au Canada



Source : Préparée par la Bibliothèque du Canada à l'aide de données du gouvernement du Canada.

Prévention et éducation

Les témoins ont parlé des initiatives et du rôle des organismes fédéraux en matière de prévention de la fraude et d'éducation du public. Chris Lynam, directeur général du Centre antifraude du Canada, qui fait partie de la Gendarmerie royale du Canada (GRC), a présenté le Centre, qui est l'agence centrale de collecte d'informations et de renseignement sur la fraude et est géré conjointement par la GRC, la Police provinciale de l'Ontario et le Bureau de la concurrence du Canada. Il a expliqué que le Centre « 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 ». Chris Lynam a admis qu'il « y a encore beaucoup à faire pour empêcher que les Canadiens soient victimes de [certaines] sollicitation[s] frauduleuse[s] ».

Steven Harroun a décrit le rôle du CRTC comme étant celui d'administrateur d'un régime de réglementation civile. Il a exposé les efforts menés par le CRTC, comme gérer la liste des numéros exclus, obliger les fournisseurs de services à bloquer les appels qui affichent des numéros qui ne pourraient normalement pas être composés et mettre en œuvre les normes STIR/SHAKEN (technologie de vérification de l'identité de l'appelant), et enfin, collaborer avec le Bureau de la concurrence et le Commissaire à la protection de la vie privée du Canada pour surveiller le respect de la *Loi canadienne anti-pourriel*. Il a informé le Comité de la *Décision de Conformité et d'Enquêtes de Télécom CRTC 2026-140*, publiée le 18 juin 2026, qui renforce la capacité des entreprises de télécommunications à bloquer l'accès au Canada par des réseaux de zombies — c'est-à-dire des réseaux d'ordinateurs, de téléphones portables ou d'autres appareils infectés par des logiciels malveillants. Cependant, puisque la compétence du CRTC découle d'un régime législatif de droit civil, Steven Harroun a reconnu que ce dernier ne peut « pas faire grand-chose contre les véritables fraudes, les vrais crimes ou les vrais comportements criminels ». Il a ajouté qu'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 ».

Les témoins ont partagé des observations quant à la place anticipée de l'éducation dans la Stratégie nationale antifraude du gouvernement du Canada, annoncée dans le budget de 2025. Jude Pinto, chef de la livraison à Paiements Canada, a indiqué que l'organisation avait fait valoir dans son mémoire soumis au gouvernement dans le cadre de consultations sur la Stratégie, qu'il fallait « une sensibilisation renforcée et collaborative des consommateurs ». De même, Jeanette Patell a indiqué que Google était d'accord avec l'idée que « des investissements dans la sensibilisation du public » devraient figurer parmi les trois grands principes au cœur de cette Stratégie. Dans son mémoire, Questrade a indiqué que l'Agence contre les crimes financiers – dont la création est annoncée dans le projet de loi C-29 –

devrait notamment avoir comme rôle d'éduquer les Canadiens et de leur prodiguer des conseils en matière de prévention.

Commentant le rôle de la prévention et l'éducation comme moyen de lutte contre la fraude, Ian Paterson a indiqué qu'il s'agissait « du premier moyen de défense ». Selon Eric Smith, « [a]ider les Canadiens à reconnaître les fraudes reste l'un des outils les plus efficaces à notre disposition ». Jennifer Quaid, quant à elle, a déclaré que « [l]a prévention doit être [l']objectif principal » de son organisme, Échange canadien de menaces cybernétiques. Enfin, David Shipley a souligné l'utilité d'enseigner ce qu'est l'intelligence émotionnelle, faisant remarquer que les arnaqueurs profitent souvent « de la solitude qui mine notre pays ».

Néanmoins, Jon Camfield a reconnu que la « sensibilisation n'est qu'une partie de la solution. Il faut vraiment beaucoup de messages diffusés au bon moment pour rejoindre les gens avant qu'ils ne s'engagent. C'est un véritable défi. » David Shipley a prévenu que : « Sans rétroaction, les programmes de sensibilisation à la fraude sont peu efficaces. D'une part — et nous l'avons montré dans notre travail d'éducation des employés —, cela incite les gens à adopter des comportements moins risqués […] C'est cela, la responsabilité partagée. » Parlant des aînés, Mark Hines a déclaré qu' : « 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. »

Anthony Quinn a apporté un autre point de vue, affirmant que pour un Canadien aîné ayant perdu toutes ses épargnes, « les programmes de sensibilisation, les discours creux des entreprises, les campagnes de relations publiques et les rappels à la prudence ne suffisent pas ». Il a réitéré que « l'éducation n'est qu'une petite partie du problème. Ce n'est manifestement pas efficace », affirmant 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. » Il a soutenu que

> la prévention de la fraude doit être une responsabilité collective, et non une simple responsabilité individuelle… 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.

Parlant de la littératie en matière de fraude, Ian Paterson a avancé que « c'est un jeu de taupe pas seulement sur le plan technologique, mais aussi sur le plan législatif ».

L'échange de données entre les secteurs

Les témoins ont évoqué l'importance de l'échange de données entre les différents secteurs de même qu'à l'échelle internationale, ainsi que le rôle de la législation en vigueur et des organismes du gouvernement du Canada à cet égard. Selon Jennifer Quaid,

> une banque, un fournisseur de services de télécommunications et une plateforme numérique peuvent chacun identifier la même activité frauduleuse, mais il n'existe aucun mécanisme efficace leur permettant de partager cette information en temps réel. C'est pourquoi chaque organisation ne voit qu'une partie du tableau, alors que les escrocs partagent des informations instantanément et exploitent les lacunes créées par le cloisonnement des systèmes et la désuétude de la réglementation.

D'ailleurs, plusieurs témoins, y compris Anthony Ostler, Mark Hines et Jon Camfield, ont souligné l'importance de la mise en place d'une approche « intersectorielle » en matière d'échange d'information. Bernard Brun, vice-président des Relations gouvernementales au sein du Mouvement des caisses Desjardins, a indiqué que « la fragmentation des données et des mécanismes de partage d'information » faisait partie des importants défis structurels. Dans la même veine, Nicholas Giurietto, responsable des politiques futures au sein d'Australian Banking Association Inc., a déclaré que son organisation demeure « plus que jamais convaincu[e] que la seule manière de réduire au minimum les préjudices dévastateurs que les escroqueries causent tous les jours aux Australiens est d'adopter une approche écosystémique coordonnée et intersectorielle dans laquelle chaque secteur de l'industrie fait sa part ».

Chris Lynam a mentionné que le Centre antifraude du Canada et le Centre national de coordination en cybercriminalité avaient organisé l'Opération Érable en 2025, réunissant à cette occasion des partenaires des secteurs public et privé. Durant cet exercice, des informations ont été échangées et transmises aux entités concernées afin qu'elles puissent prendre les mesures nécessaires. Il estimait que l'exercice avait « permis des gains d'efficacité » dans la gestion de l'échange d'informations en temps réel. Meta et Google ont signalé qu'ils avaient participé à cet exercice, qui aura lieu de nouveau en 2026.

Au sujet des lois régissant l'échange d'information, Hartland Elcock, avocat général adjoint et vice-président de l'Association des banquiers canadiens, a observé que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui est la loi fédérale sur la protection des renseignements personnels dans le secteur privé, définit les obligations des entreprises privées en matière de signalement des atteintes à la vie privée. Mark Hines a indiqué que les entreprises de technologies financières, dont Interac, accordent beaucoup d'importance au consentement et à

l'existence de motifs valables en droit de communiquer des données. Il a observé que la LPRPDE établit « une base claire pour traiter les données à des fins de lutte contre la fraude ». En revanche, dans son mémoire, Fintechs Canada a déclaré que

> [d]es lois comme la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et la *Loi sur les banques* créent de l'incertitude quant à l'échange de renseignements liés à la fraude d'une manière qui ne reflète pas le fonctionnement de la fraude moderne. Par exemple, l'absence d'une définition claire de la fraude dans la LPRPDE peut restreindre l'échange de renseignements essentiels liés aux victimes.

Entre autres, Carey Frey, Jon Camfield, Jennifer Quaid, Mark Hines, Fintechs Canada et Future of Financial Intelligence Sharing, ont attiré l'attention sur l'importance des dispositions d'exonération en matière d'échange de renseignement, lesquelles existent dans d'autres pays, notamment en Australie. Pour sa part, Mark Hines a déclaré que la « disposition d'exonération favorise le type d'échange de renseignements que nous estimons essentiel si nous voulons endiguer le problème dès son apparition ». De l'avis de Nicholas Giurietto, « [l]e rôle principal du gouvernement est de fournir le cadre politique qui permet un échange de données sécurisées conformes à la protection de la vie privée, assorti de protections de sécurité ».

En ce qui concerne le cadre juridique du Canada en matière d'échange d'informations, Carey Frey a signalé que certaines des politiques en place au Canada peuvent faciliter involontairement la fraude, faisant valoir que

> les règlements du CRTC relatifs à la confidentialité des clients restreignent l'échange de renseignements entre les différents secteurs. Un autre exemple est celui des règles du CRTC concernant le déverrouillage de dispositifs, qui facilitent la tâche des criminels souhaitant escroquer les Canadiens de leurs téléphones intelligents, les laissant avec des dettes importantes et une cote de crédit détériorée.

Dans le contexte actuel, Jennifer Quaid a soutenu que le Canada a « besoin de cadres qui brisent les cloisonnements, favorisent une véritable collaboration, allouent des ressources significatives là où elles sont nécessaires et accordent la priorité à la prévention ». Elle a souligné que la Coalition canadienne antifraude et Échange canadien de menaces cybernétiques, deux groupes à participation volontaire réunissant des intervenants du secteur privé et des gouvernements « sont prêts à bâtir cette infrastructure ».

La responsabilité en matière de fraude au Canada

Comme l'indique le mémoire du Canadian Anti-Monopoly Project, « au Canada, les cadres juridiques régissant la responsabilité en matière de fraude en ligne ne sont pas complets, et les recours dont disposent les particuliers sont limités » [TRADUCTION]. Ce mémoire

établissait une distinction entre la fraude « autorisée » et celle non autorisée, soulignant que les établissements financiers pourraient parfois être tenus responsables dans le deuxième cas. Pour cette raison, « les banques ont mis au point des techniques plus sophistiquées pour prévenir la fraude non autorisée » [TRADUCTION]. En conséquence, les fraudeurs se sont adaptés et mettent l'accent sur les escroqueries par séduction[5], dans le cadre desquelles ils gagnent la confiance de leur victime, qui leur transfère de l'argent de leur plein gré. C'est ce que l'on entend par fraude « autorisée ». Dans ce cas, « la victime n'a probablement aucune chance de récupérer son argent » [TRADUCTION]. Le mémoire du Canadian Anti-Monopoly Project a souligné les complications additionnelles liées à la montée de la cryptomonnaie, précisant que « les victimes disposent peut-être d'encore moins de recours, car les transactions en cryptomonnaies sont irréversibles et s'effectuent souvent sans l'intervention d'aucune institution financière réglementée » [TRADUCTION].

Dans un mémoire présenté par Peter Squire, un homme qui, selon *CBC News*, a perdu près de 650 000 $ à la suite d'une de ces fraudes, il est indiqué que le Canada devrait passer de la « vigilance des consommateurs » à la « responsabilité des institutions ». M. Squire recommandait d'obliger « les institutions financières à indemniser les victimes lorsque les mesures de prévention ne fonctionnent pas ou que les signes avant-coureurs passent inaperçus ». Dans le même ordre d'idées, partageant l'avis selon lequel une plateforme hébergeant une publicité frauduleuse devrait assumer une part de responsabilité, Anthony Quinn a affirmé que « [n]ous 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. »

Les témoins ont évoqué la question de la responsabilité et ont exposé leur point de vue sur les parties qui sont responsables ou qui devraient être tenues responsables en cas de fraude. Mark Hines a fait valoir qu'« 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. » Il a exposé la proposition de l'entreprise : « [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. » Selon Frédéric Lapalme, dans certains cas, « 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.

5 Une escroquerie dite « par séduction » (« pig butchery scam » en anglais) est une fraude en ligne de longue haleine qui repose sur une relation amoureuse, la victime étant comparée à un cochon engraissé par la confiance, l'amitié ou l'amour avant d'être « abattue » à des fins lucratives.

Donc, la Coalition canadienne antifraude et les autres initiatives pour rassembler tous les joueurs sont d'autant plus importantes. »

Lorsqu'on lui a demandé si Google remboursait les victimes de fraude pour les pertes qu'elles ont subies, Jeanette Patell a insisté sur la complexité de la question, soulignant que chez Google, les gens sont « conscients du coût humain que cela représente et nous reconnaissons également que les criminels doivent être tenus responsables de leurs actes ». Dans son mémoire, Google présente le point de vue de l'entreprise :

> [Nous] estimons qu'une approche équilibrée, qui met l'accent sur la sensibilisation des usagers et des usagères, les solutions technologiques, les mesures d'application de la loi visant directement les fraudeurs et le crime organisé connexes ainsi que la coopération entre les parties prenantes, comme l'industrie et les organismes gouvernementaux, sera plus efficace que l'imposition de sanctions financières aux plateformes.

Exprimant la position du Centre antifraude du Canada, Chris Lyman a tenu les propos suivants :

> [J]e 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.

L'application de la loi

Les témoins ont discuté des différents aspects liés à l'application du cadre juridique canadien régissant la fraude et les escroqueries. Or, comme l'a fait remarquer Mark Hines, « [l]application de la loi est aussi importante, mais elle intervient une fois que le mal est fait ».

En ce qui concerne le remboursement des sommes perçues auprès des fraudeurs dont la responsabilité a été établie, Sarah Corrigall-Brown, avocate générale de la British Columbia Securities Commission, a soulevé un point touchant la *Loi sur la faillite et l'insolvabilité*, qui empêche la Commission de recueillir de l'argent pour rembourser les victimes de fraude puisque ce texte de loi

> 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.

Pour cette raison, cette intervenante a recommandé que la *Loi sur la faillite et l'insolvabilité* soit modifiée afin que les dettes liées à des cas de fraude, de manipulation du marché et de fausse déclaration ne soient pas effacées en cas de faillite.

Hartland Elcock a expliqué le rôle du CANAFE en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et le contournement de sanctions : « Il ne s'agit pas des infractions principales de fraude, mais du traitement de l'argent après l'incident initial, et le rôle du CANAFE consiste à lier ces informations pour les transmettre aux autorités. » Il a expliqué que le CANAFE « est un organisme de renseignement et non un organisme d'application de la loi. Nos membres sont ceux qui signalent le plus grand nombre d'opérations suspectes au CANAFE : lorsqu'une organisation constate une activité douteuse donnant lieu à des motifs raisonnables de soupçonner le blanchiment d'argent, elle transmet cette information au CANAFE. » En ce qui a trait à l'efficacité du CANAFE et du Centre antifraude du Canada dans l'exercice de leur rôle, Frédéric Lapalme a fait l'observation suivante :

> 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.

Carey Frey a recommandé que les organismes d'application de la loi soient dotés « d'un mandat explicite et des ressources nécessaires pour appréhender efficacement les auteurs de fraudes et démanteler leurs dispositifs techniques ».

PRATIQUES EXEMPLAIRES : LES LEÇONS TIRÉES DE L'AUSTRALIE

L'Australie passe actuellement d'un régime fondé sur la coopération volontaire en matière de lutte contre les escroqueries à un cadre de prévention à caractère obligatoire qui est applicable à de multiples secteurs, conformément à la *Scams Prevention Framework Act 2025* (Loi de 2025 établissant un cadre de prévention des escroqueries), qui a reçu la sanction royale le 20 février 2025 et modifie la *Competition and Consumer Act 2010* (Loi de 2010 sur la concurrence et les consommateurs). En vertu de la Loi de 2025, la responsabilité en matière de prévention de la fraude est partagée entre les secteurs désignés. Les entités réglementées sont tenues de mettre en place des mesures visant à prévenir, à détecter, à signaler, à perturber et à combattre les manœuvres frauduleuses. Dans un premier temps, le gouvernement australien se concentre sur les services bancaires, les télécommunications et certaines plateformes numériques, puisque ces secteurs sont les principaux vecteurs utilisés par les fraudeurs. Nicholas Giurietto a indiqué que bien que la loi en question ait été adoptée, « sa mise en œuvre est encore en cours ». Il a souligné que « la composante la plus efficace est le fait qu'[elle] présente les responsabilités de chaque secteur comme étant équivalentes, mais différentes ».

Comme l'a indiqué Nicholas Giurietto,

> [l]e cadre australien de prévention des escroqueries a suscité beaucoup d'attention à l'échelle mondiale en tant que premier exemple du régime réglementaire de lutte contre les escroqueries reposant sur le principe selon lequel tous les secteurs de l'industrie doivent contribuer à la lutte contre les escroqueries.

Il a noté que d'autres secteurs concernés par les fraudes devront participer à la mise en place d'une intervention coordonnée, y compris « les échanges de cryptomonnaie, les expéditeurs non bancaires de fonds, les fournisseurs de logiciel d'accès à distance, les marchés en ligne, les fournisseurs de cartes-cadeaux et bien d'autres ». Pour sa part, Anthony Ostler a souligné que l'Australie s'attaquait à la fraude en appliquant « une approche intersectorielle public-privé », une action qu'il juge « essentielle ». Pour illustrer ce point, il a signalé que depuis 2022, les escroqueries avaient diminué de 30 % en Australie, mais augmenté de 32 % au Canada.

Anthony Ostler et Hartland Elcock ont donné un exemple du fardeau réglementaire qui pèse sur les institutions canadiennes par rapport à celles de l'Australie, expliquant que les rapports sur les opérations douteuses du CANAFE comportent 400 champs contre 30 à 50 pour leurs équivalents en Australie. D'après eux, une réduction du nombre de champs faciliterait la transmission de renseignements utiles, ce qui permettrait aux organismes d'application de la loi d'agir. Lorsqu'il y a trop de champs, les résultats tirés des nombreuses données désagrégées sont moins efficaces.

Par ailleurs, selon Anthony Ostler, les publicités frauduleuses ne sont pas éliminées aussi rapidement au Canada qu'en Australie. Nicholas Giurietto a souligné que « pour les entreprises de plateformes; si une personne veut faire la publicité d'un produit financier », on vérifie « qu'elle détient effectivement une licence australienne l'autorisant à offrir des services financiers — c'est-à-dire la licence requise pour la vente de produits d'investissement en Australie — avant de l'autoriser à faire la publicité de son produit ».

En ce qui concerne les obligations en matière de lutte contre la fraude, l'Australie se distingue du Canada en ce sens que tous les secteurs, y compris les banques, les plateformes de médias sociaux, les entreprises de télécommunications et le secteur des contrats à terme, portent leur part de responsabilité. Nicholas Giurietto a déclaré que si seules les banques sont responsables, « on finit par essayer de contenir un feu qui brûle déjà ». Il a fait remarquer que si les entreprises de télécommunications et les plateformes agissaient plus tôt, il serait possible d'intervenir plus rapidement face aux escroqueries et de diffuser des informations afin d'éviter qu'il y ait de nouvelles victimes.

En ce qui concerne l'accès légal, qui, dans le cas du Canada, permet légalement aux services de police et du renseignement de procéder à l'interception de communications ainsi qu'à la perquisition et à la saisie d'informations en vertu du *Code criminel,* de la *Loi sur le Service canadien de renseignement de sécurité* et d'autres lois, y compris la *Loi sur la concurrence*, Nicholas Giurietto a expliqué que « le système fédéral de l'Australie comporte des responsabilités policières qui se chevauchent, ce qui peut parfois compliquer les choses. Toutefois, il est très important de pouvoir échanger des renseignements et prendre des mesures, que ce soit en communiquant des renseignements ou, dans certains cas, en appuyant les organismes d'application de la loi. » Il a par ailleurs souligné que « [l]'échange de renseignements entre entités privées est tout aussi important, du fait que, parfois, le secteur privé peut se servir de ce qu'on appelle des indices de fraude qui ne satisfont pas à la norme juridique que les organismes d'application de la loi pourraient devoir respecter avant d'engager des poursuites ou de prendre d'autres mesures ». En parlant de l'échange du renseignement entre les intervenants du secteur privé et les organismes d'application de la loi étatiques et fédéraux, David Pegley a souligné que, malheureusement, la plupart des acteurs malveillants menant des activités en Australie proviennent de l'étranger.

Les témoins ont également parlé des différentes institutions de l'Australie qui combattent la fraude. David Pegley a décrit les fonctions de l'Australian Financial Crimes Exchange, une organisation indépendante à but non lucratif qui facilite le partage d'informations entre une centaine de membres issus de huit secteurs d'activité différents, notamment les médias numériques, les entreprises de télécommunications, les compagnies d'assurance, les banques et les plateformes d'échange de cryptomonnaies. Jennifer Quaid a mentionné la création, par l'Australie, du National Anti-Scam Centre. Au sujet des efforts déployés par

l'Australie pour combattre la fraude, Nicholas Giurietto a commenté qu'au « fil du temps, il devient […] plus coûteux pour les fraudeurs de prendre pour cible l'Australie plutôt qu'un autre pays, et ils pourraient donc concentrer leurs efforts ailleurs ».

CONCLUSION

L'étude du Comité sur la fraude et les escroqueries au Canada tombe à point. Selon le Centre antifraude du Canada, entre le 1er janvier et le 30 juin 2026, 9 935 personnes ont été victimes de fraude au Canada, les pertes déclarées s'élevant à 351 millions de dollars. La présente étude fait ressortir qu'on peut encore améliorer au Canada les mécanismes de prévention, de détection et de signalement des fraudes, ainsi que ceux relatifs à la responsabilité. Le Comité est toujours préoccupé par le manque apparent de responsabilité et de reddition de comptes de la part des réseaux sociaux, compte tenu de la gravité du problème de la fraude financière sur leurs plateformes. Les plateformes de médias sociaux, les banques et les entreprises de télécommunications ont toutes un rôle à jouer pour combattre le problème grandissant de la fraude au Canada. Les témoins ont recommandé la mise en place d'un organisme central de coordination et de mécanismes plus solides d'échange d'informations entre les différents secteurs. L'Australie, qui est l'un des seuls pays à avoir connu une baisse de la fraude ces dernières années, présente des solutions stratégiques pour le Canada, telles que l'adoption d'une approche publique privée de lutte contre la fraude et le partage intersectoriel de la responsabilité en cas de fraude. En présentant 18 recommandations ciblées, le Comité encourage le gouvernement à agir pour s'attaquer à ce grave problème, qui touche un grand nombre de Canadiens et Canadiennes.

ANNEXE A :
LISTE DES TÉMOINS

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

Organismes et individus	Date	Réunion
Association des banquiers canadiens	2026/06/04	42
Hartland Elcock, vice-président et avocat général adjoint		
Anthony Ostler, président et chef de la direction		
Association canadienne des télécommunications	2026/06/04	42
Eric Smith, vice-président principal		
TELUS	2026/06/04	42
Carey Frey, chef de la sécurité		
Australian Banking Association Inc.	2026/06/08	43
Nicholas Giurietto, responsable des politiques futures		
Australian Financial Crimes Exchange Ltd.	2026/06/08	43
David Pegley, directeur général		
Beauceron Security	2026/06/08	43
David Shipley, directeur général		
Échange canadien de menaces cybernétiques	2026/06/08	43
Jennifer Quaid, directrice exécutive		
Meta Platforms Inc.	2026/06/08	43
Jon Camfield, responsable de la défense, Politique sur la sécurité		
Rachel Curran, directrice, Politique publique, Meta Canada		
British Columbia Securities Commission	2026/06/11	44
Sarah Corrigall-Brown, avocate générale		
Association canadienne des individus retraités	2026/06/11	44
Anthony Quinn, président		

Organismes et individus	Date	Réunion
Paiements Canada	2026/06/11	44
Jude Pinto, chef de la mise en œuvre		
Plurilock Security Inc.	2026/06/11	44
Ian Paterson, président-directeur général		
Gendarmerie royale du Canada	2026/06/11	44
Chris Lynam, directeur général, Centre antifraude du Canada		
Wealthsimple	2026/06/11	44
Colin Smith, vice-président, Sciences du risque et de la décision		
Conseil de la radiodiffusion et des télécommunications canadiennes	2026/06/16	46
Steven Harroun, dirigeant principal, Conformité et enquêtes		
Scott Hutton, dirigeant principal, Consommation, analytique et stratégie		
Mouvement des caisses Desjardins	2026/06/16	46
Bernard Brun, vice-président, Relations gouvernementales		
Frédéric Lapalme, directeur principal et chef délégué, Encadrement et surveillance, lutte contre la fraude et les crimes financiers		
Interac Corp.	2026/06/16	46
Mark Hines, chef des produits de prévention de la fraude		
Google Canada	2026/06/18	47
Jeanette Patell, directrice, Affaires gouvernementales et des politiques publiques, Canada		

ANNEXE B :
LISTE DES MÉMOIRES

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

Canadian Gaming Association

Corporation Visa Canada

Cosgrove, Kevin

Démocratie en surveillance

Equifax Canada Co.

Fintechs Canada

Foster, Pamela

Google Canada

Questrade Inc.

Shakepay Inc.

Squire, Peter

Tru Cooperative Bank

DEMANDE DE RÉPONSE DU GOUVERNEMENT

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

Un exemplaire des *procès-verbaux* pertinents (réunions nos 42, 43, 44, 46, 47, 48 et 51) est déposé.

Respectueusement soumis,

Le président,
Ben Carr