

Commentaires présentés
au ministère des Finances du Canada



Stratégie nationale antifraude : Vers une responsabilisation de tous les acteurs

28 avril 2026

Table des matières

| | |
|--|-----------|
| L'intervenante | 3 |
| 1. La grande oubliée : la responsabilité des organisations | 4 |
| 1.1. Pour un régime de responsabilisation des banques en matière de fraude..... | 4 |
| 1.1.1. Les justifications à la responsabilisation..... | 6 |
| 1.1.2. Rectifier les faits sur l'impact de la responsabilisation des banques | 7 |
| 1.2. Responsabiliser les sociétés de télécommunications et les plateformes numériques..... | 9 |
| 2. Réponses aux questions de la consultation | 12 |
| 2.1. Commentaires généraux sur le cadre proposé | 12 |
| 2.1.1. Pour un niveau de protection élevé et contraignant | 12 |
| 2.1.2. Pour une approche multisectorielle et collaborative (questions 1 à 4)..... | 13 |
| 2.1.3. Pour un échange de renseignements entre organisations (questions 5 à 11)..... | 14 |
| 2.2. Commentaires sur les principes du cadre proposé | 15 |
| 2.2.1. Prévention (questions 12 à 17)..... | 15 |
| 2.2.2. Détection (questions 18 à 30) | 17 |
| 2.2.3. Perturbation (questions 31 à 35)..... | 18 |
| 2.2.4. Réponse (questions 36 à 45)..... | 19 |
| 2.3. Autres aspects (questions 46 à 50) | 21 |
| Sommaire des principales recommandations | 23 |

L'intervenante

Créée en 1983, Option consommateurs est une association à but non lucratif qui a pour mission d'aider les consommateurs et de défendre leurs droits.

Parmi ses activités, notre organisation offre une aide directe à des milliers de consommateurs via son service d'information juridique et son service d'aide budgétaire. En tant qu'intervenante reconnue en consommation, son expertise est souvent sollicitée lors de consultations publiques ou par les médias dans divers domaines, tels que les finances personnelles, les pratiques commerciales, les services financiers, la protection de la vie privée, l'énergie et l'accès à la justice. Option consommateurs réalise également des rapports de recherche sur de nouveaux enjeux de consommation et, lorsque nécessaire, intente des actions collectives contre des commerçants.

La présente consultation interpelle tout particulièrement Option consommateurs. Au cours des dernières années, nous avons reçu des centaines d'appels de consommateurs victimes de fraude dont l'institution financière refusait tout remboursement. Étant en première ligne pour constater les ravages de la fraude sur les Canadiens, notre organisation est donc bien placée pour commenter la présente consultation.

Pour en faciliter la lecture et le repérage, les rubriques de notre intervention indiqueront, le cas échéant, les questions pertinentes de la consultation auxquelles elles répondent. Certaines questions, qui ne font pas partie du champ d'expertise d'Option consommateurs, ont été omises.

1. La grande oubliée : la responsabilité des organisations

1.1. Pour un régime de responsabilisation des banques en matière de fraude

Option consommateurs regrette que le document de consultation du ministère ne propose pas d'emblée d'élargir les obligations des banques relatives au remboursement des consommateurs victimes de fraude¹. Afin que la Stratégie nationale antifraude ait un impact concret pour les consommateurs, nous estimons incontournable d'exiger que les banques remboursent leurs clients victimes de fraude – à moins bien sûr que ceux-ci aient commis une négligence grave dans le cadre de la fraude.

Comme nous l'avons mentionné lors de diverses consultations précédentes², les contrats bancaires comportent des clauses qui permettent aisément aux banques de se dégager de toute responsabilité en cas de fraude et de faire reposer la perte sur les épaules de leurs clients. Par exemple, il n'est pas rare que la banque prétende que, puisque la victime a donné « volontairement » ses identifiants bancaires au fraudeur, il s'agit d'une transaction qu'elle a « autorisée » au sens du contrat et qu'elle doit en assumer la perte. Ou encore, la banque peut invoquer divers manquements à des clauses relatives à des obligations de sécurité que doit respecter le consommateur pour refuser de l'indemniser.

Pourtant, les victimes de fraude qui nous contactent ne sont pas des personnes négligentes ou insouciantes. Les victimes de fraude sont des citoyens prudents et diligents qui ont été manipulés par des criminels ayant recours à des stratagèmes très sophistiqués et crédibles. Or, même si n'importe qui aurait pu tomber dans le piège tendu par les fraudeurs, les banques les tiennent responsables des pertes subies en invoquant divers manquements contractuels.

À l'heure actuelle, la loi n'offre guère de rempart pour faire échec à ces stipulations contractuelles. Tel que le mentionne le document de consultation, la *Loi sur les*

¹ <https://www.canada.ca/fr/ministere-finances/programmes/consultations/2026/strategie-nationale-antifraude-document-de-consultation.html>

² Voir notamment notre réponse aux consultations du ministère sur les propositions en vue de renforcer le secteur financier canadien de 2024 : <https://option-consommateurs.org/revendications/consultation-renforcement-secteur-financier-canadien>

banques prévoit une protection contre les transactions non autorisées sur carte de crédit³; le *Code de pratique canadien des services de cartes de débit* en fait autant à l'égard des opérations par carte de débit avec NIP⁴. Toutefois, ces normes se montrent aujourd'hui caduques face aux nouveaux types de fraude dits « autorisés » faisant appel au piratage psychologique qui sévissent au Canada, telles que la fraude du faux représentant bancaire ou les fraudes d'investissement en ligne.

En l'absence de normes qui obligent le remboursement des consommateurs, nous voyons souvent des victimes qui ont perdu des dizaines, voire des centaines de milliers de dollars dans des arnaques, et qui se retrouvent sans recours contre leur banque. Selon le dernier Baromètre d'Option consommateurs et du Consortium de recherche empirique en droit interdisciplinaire numérique et financier (CREDI-NF), près de la moitié des Canadiens victimes de fraude bancaire n'ont pas été en mesure de récupérer la totalité des sommes perdues⁵. Un reportage de *La Facture* montrait qu'en 2023, seuls 17 % des cas de fraude portés devant l'Ombudsman des services bancaires et d'investissement (OSBI) étaient résolus en faveur du consommateur⁶.

Il ne s'agit pas seulement de statistiques. Les témoignages que nous recevons des consommateurs montrent que les conséquences de ces fraudes sont majeures. De nombreuses victimes peuvent avoir perdu l'ensemble de leurs économies, ce qui les place dans une situation de précarité financière qui les empêche de participer pleinement à la vie économique; dans certains cas, les victimes peuvent même se retrouver endettées⁷. C'est sans compter les impacts psychologiques et sociaux considérables qui résultent souvent de la fraude, tels que l'isolement, les sentiments

³ *Loi sur les banques*, LC 1991, c 46, art. 627.33. Au Québec, la loi prévoit également une protection similaire : *Loi sur la protection du consommateur*, RLRQ c P-40.1, art. 123-123.1.

⁴ *Code de pratique canadien des services de cartes de débit*, préparé par le Groupe de travail sur le transfert électronique de fonds de travail sur le transfert électronique de fonds, révision 2004, <https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/industrie/loisreglements/code-canadien-cartes-debit.html>

⁵ OPTION CONSOMMATEURS et CONSORTIUM DE RECHERCHE EMPIRIQUE EN DROIT INTERDISCIPLINAIRE NUMÉRIQUE ET FINANCIER, *Baromètre de confiance*, Étude réalisée auprès de la population canadienne par Léger, 2026 [à paraître].

⁶ Mélissa PELLETIER, *Fraudés et laissés pour compte par leur banque*, Radio-Canada, 29 octobre 2024, <https://ici.radio-canada.ca/nouvelle/2114907/fraudes-compte-banque-remboursement-ombudsman-protection>

⁷ Selon les données de la Clinique de cyber-criminologie de l'Université de Montréal, plus d'un tiers des victimes s'adressant à cet organisme rapportent un endettement lié à la fraude. Voir : CLINIQUE DE CYBER-CRIMINOLOGIE DE L'UNIVERSITÉ DE MONTRÉAL, Rapport annuel 2025/2026, mars 2026, https://www.clinique-cybercriminologie.ca/_files/ugd/9dc3da_b694ec772c38468191c439a7753fb0b0.pdf, p. 7.

de honte, de culpabilité ou de crainte, et qui persistent longtemps après l'acte criminel.

Face à l'ampleur de la crise, il est grand temps d'élargir les normes de remboursement des consommateurs victimes de fraude. À cet égard, nous proposons au ministère de s'inspirer de ce qui a été fait récemment dans d'autres juridictions :

- Au Royaume-Uni, le gouvernement a récemment élargi la protection contre la fraude. Selon les nouvelles règles du *Payment Services Regulator*, un consommateur victime d'une fraude dite « *APP scam*⁸ », soit une arnaque où la victime se fait convaincre par le malfaiteur d'effectuer un paiement, devra être remboursé à moins d'une négligence grossière de sa part⁹.
- Au Québec, la *Loi sur la protection du consommateur* a récemment été modifiée pour imposer aux institutions financières des obligations de remboursement en cas de fraude dans le compte bancaire du consommateur¹⁰. Ces modifications ne sont pas encore en vigueur et le deviendront suivant la publication d'un décret.

1.1.1. Les justifications à la responsabilisation

Nous estimons qu'une approche fondée sur une plus grande responsabilisation des banques permettra non seulement à des milliers de Canadiens victimes de fraude de récupérer leur argent, mais elle permettra aussi de diminuer l'occurrence de ces fraudes. En effet, en faisant porter une responsabilité plus grande aux banques, le régime législatif créerait un véritable incitatif pour ces entreprises à déployer des mesures adéquates de prévention pour limiter leurs pertes.

Rappelons également que la banque est l'acteur qui a la capacité économique de supporter les pertes. Entreprises hautement profitables, les banques canadiennes sont en mesure d'absorber les pertes découlant des fraudes dans leurs coûts

⁸ Acronyme de « *authorised push payment scam* ».

⁹ PAYMENT SYSTEMS REGULATOR, *PS23/4: APP scams reimbursement policy statement*, 19 décembre 2023, <https://www.psr.org.uk/publications/policy-statements/ps234-app-scams-reimbursement-policy-statement/>

¹⁰ *Loi protégeant les consommateurs contre les pratiques commerciales abusives et offrant une meilleure transparence en matière de prix et de crédit*, LQ 2024, c 32, art. 12 (introduisant les nouveaux articles 65.1 et 65.2 de la *Loi sur la protection du consommateur*).

d'opération bien plus aisément que le consommateur individuel, pour qui cette perte économique est parfois irrécupérable et peut représenter les économies d'une vie.

Soulignons enfin que, considérant la concentration du secteur bancaire au Canada, la concurrence peut difficilement jouer pour amener les banques à développer des politiques de remboursement plus généreuses, d'autant plus que les statistiques sur les fraudes dans les diverses institutions financières ne sont pas rendues publiques.

1.1.2. Rectifier les faits sur l'impact de la responsabilisation des banques

Contrairement à des informations qui ont circulé au Canada, la responsabilisation des institutions financières en matière de fraude, par le truchement d'obligations de remboursement, n'a pas eu pour effet d'augmenter les occurrences de fraude dans les pays qui ont implanté une telle mesure. Bien au contraire, l'exemple du Royaume-Uni montre que les normes de remboursement peuvent avoir un effet positif :

- Selon le *Payment Systems Regulator*, après l'entrée en vigueur du nouveau cadre de protection des consommateurs, le nombre de réclamations pour les fraudes de type « *APP scam* » transitant via le *Faster Payments System*, qui font l'objet de la nouvelle obligation de remboursement, a diminué d'environ 15 % entre octobre 2024 et juin 2025, par rapport à la même période d'octobre 2023 à juin 2024¹¹.
- Il est vrai que, selon le *Half Year Fraud Report 2025* du ministère des Finances du Royaume-Uni¹², l'ensemble des cas de fraude au Royaume-Uni a effectivement augmenté de 17 % par rapport à la même période en 2024. Cependant, ce même rapport montre que les cas de fraude APP ont quant à eux diminué de 8 %¹³. Il n'est donc pas fondé de conclure que les normes de

¹¹ PAYMENT SYSTEMS REGULATOR, *APP scams reimbursement dashboard for Q3 2025*, mise à jour du 30 janvier 2026, <https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/>

¹² UK FINANCE, *Half Year Fraud Report 2025*, 2025, p. 6, <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025>

¹³ *Ibid*, p. 19.

remboursement élargies ont accru les cas de fraude, puisqu'on observe une diminution des cas couverts par ces normes¹⁴.

- Le récent document de consultation *Fraud Strategy 2026-2029* du Home Office du Royaume-Uni réfère à ces statistiques et mentionne l'importance de consacrer des efforts sur la fraude dite « non autorisée »¹⁵. Rien n'indique dans cette consultation que le gouvernement britannique souhaite retirer les nouvelles obligations de remboursement. Au contraire, le document certifie que « *the Government remains committed to maintaining mandatory reimbursement*¹⁶ ».

En outre, il n'apparaît pas fondé, au regard de l'expérience britannique, d'invoquer que les consommateurs deviennent plus négligents du fait qu'ils sont protégés par des normes de remboursement (*moral hazard*). Selon le *Payment Systems Regulator* britannique, aucune observation n'a été faite en ce sens après l'entrée en vigueur des nouvelles obligations de remboursement¹⁷. En toute logique, le fait d'être assuré contre un risque n'est pas un incitatif pour un consommateur à faire preuve d'insouciance quant à ce risque.

En somme, bien qu'Option consommateurs admette que la responsabilisation des banques doit être complétée par diverses autres normes de lutte contre la fraude et la responsabilisation d'autres acteurs, nous estimons qu'il est bien mal fondé de considérer qu'une telle mesure est inefficace ou se montre contre-productive. Au contraire, l'indemnisation des consommateurs est un élément primordial et incontournable d'un cadre antifraude efficace.

¹⁴ Notons toutefois que la valeur des fraudes dites « autorisées » a augmenté de 12 %. Le ministère des Finances britannique suggère que cette hausse pourrait être attribuable à l'augmentation de la proportion des cas de fraudes d'investissement, dont les pertes sont plus importantes. Voir : *Ibid.*, p. 7.

¹⁵ UK GOVERNMENT, *Fraud Strategy 2026-2029: Disrupting crime, supporting economic resilience and delivering justice*, presented to Parliament by the Secretary of State for the Home Department by Command of His Majesty, March 2026, par. 61-63, <https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf>

¹⁶ *Ibid.*, par. 104.

¹⁷ PAYMENT SYSTEMS REGULATOR, *APP scams reimbursement dashboard for Q3 2025*, mise à jour du 30 janvier 2026, <https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/>

1.2. Responsabiliser les sociétés de télécommunications et les plateformes numériques

Nous estimons que l'obligation de remboursement des consommateurs ne devrait pas reposer uniquement sur les seules épaules du secteur financier. D'autres acteurs, lorsqu'ils jouent un rôle contributif dans la fraude, devraient en supporter la responsabilité :

- D'abord, les services des sociétés de télécommunications servent souvent à initier des arnaques. Les appels et les messages textes frauduleux sont l'amorce de nombreuses fraudes par lesquelles les consommateurs sont ciblés. Par exemple, au cours des dernières années, nous avons été contactés par des dizaines de consommateurs victimes de fraudes du faux représentant bancaire initiées par un appel téléphonique dont l'identité de l'appelant avait été mystifiée (aussi connu sous le nom de « *spoofing* »). Grâce à cette tactique, les fraudeurs pouvaient aisément convaincre leurs victimes qu'ils étaient des employés de leur institution bancaire puisque leur afficheur indiquait que l'appel provenait de leur banque.
- Ensuite, les plateformes en ligne comme YouTube ou Facebook permettent aux criminels de piéger facilement un grand nombre d'internautes, notamment grâce à de fausses annonces diffusées sur leurs réseaux publicitaires. Ces publicités peuvent, au moyen d'un hypertrucage, mettre en scène des personnalités publiques pour attirer l'attention des victimes. Parmi les arnaques ciblant les consommateurs, citons les fraudes à l'investissement, où les consommateurs sont encouragés à transférer des fonds sur des plateformes d'investissement en leur promettant des rendements mirobolants.

Les fraudes réalisées par l'intermédiaire de ces acteurs causent des pertes considérables aux Canadiens. Par exemple, en 2024, le Centre antifraude du Canada rapportait que la fraude à l'investissement avait engendré 310,6 millions de dollars de pertes¹⁸, ce qui en fait la plus importante au pays en termes de pertes financières. Chez Option consommateurs, nous avons reçu des témoignages de consommateurs qui disent avoir perdu plusieurs centaines de milliers de dollars dans de telles fraudes¹⁹. La situation est d'autant plus préoccupante que les grandes plateformes

¹⁸ <https://antifraudcentre-centreantifraude.ca/features-vedette/2025/02/month-prevention-mois-fra.htm>

¹⁹ Plus encore, ces personnes peuvent être à nouveau la cible de fraudeurs, qui les contactent à nouveau en leur promettant de pouvoir récupérer leur argent perdu.

tirent elles-mêmes profit de ce phénomène. Selon un article de *Reuters*, Facebook projetait que 10 % de ses revenus publicitaires en 2024, soit 7 milliards de dollars, proviendraient d'annonces liées à des escroqueries ou à des produits interdits²⁰.

Nous estimons donc que ces organisations devraient partager les coûts d'indemnisation des consommateurs victimes de fraude²¹. En ce sens, nous proposons que les plateformes numériques et les sociétés de télécommunications qui manquent à détecter et à bloquer les contenus frauduleux aient l'obligation de rembourser les victimes des arnaques qui ont trouvé leur point d'entrée via leurs services. De même, nous proposons que les institutions financières qui ont indemnisé un client victime de fraude puissent ensuite porter leur réclamation contre les sociétés de télécommunications et les plateformes numériques qui ont permis la réalisation de l'arnaque. Une telle approche s'accorderait d'ailleurs avec des initiatives récemment développées dans d'autres juridictions :

- En Europe, les nouvelles normes sur les services de paiement prévoient que les plateformes en ligne sont responsables envers un fournisseur de services de paiement qui a indemnisé une victime de fraude, dès lors qu'elles ont été informées d'un contenu frauduleux et qu'elles ne l'ont pas retiré²².
- Au Québec, un nouveau projet de loi propose que les plateformes en ligne soient tenues responsables des contenus frauduleux utilisant sans consentement l'image d'une personne et qu'elles puissent faire l'objet d'ordonnances afin de retirer ces contenus²³.
- En France, la loi impose aux opérateurs téléphoniques des obligations d'authentification des appels dans un effort de limiter les appels mystifiés²⁴. En raison d'un manquement à ces obligations, le Tribunal judiciaire de Paris a récemment condamné une entreprise de télécommunications à rembourser à

²⁰ Jeff HORWITZ, *Meta is earning a fortune on a deluge of fraudulent ads, documents*, Reuters, 6 novembre 2025, <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06>

²¹ Mentionnons qu'au Québec, une action collective cherchant à établir la responsabilité de la plateforme Facebook dans la diffusion de publicités frauduleuses a été autorisée : *Gauthier c. Facebook Canada Ltd.*, 2025 QCCS 1794.

²² <https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees>

²³ *Loi protégeant le consommateur contre l'utilisation trompeuse ou frauduleuse de l'identité ou de l'image d'une personne*, projet de loi n° 24 (2026), 2^e sess., 43^e légis. (Qc).

²⁴ *Code des postes et des communications électroniques*, art. L44, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000051830329

l'institution financière la compensation que cette dernière devait verser à une consommatrice victime d'une fraude du faux représentant²⁵.

²⁵ Tribunal judiciaire de Paris RG n° 24/04856, 15 janvier 2026, <https://www.courdecassation.fr/decision/696943cfdc6046d4770c741>

2. Réponses aux questions de la consultation

2.1. Commentaires généraux sur le cadre proposé

2.1.1. Pour un niveau de protection élevé et contraignant

De manière générale, nous accueillons favorablement l'approche multisectorielle proposée par le ministère, dans laquelle les institutions financières, les sociétés de télécommunications et les plateformes numériques sont visées. Reprenant essentiellement l'approche développée récemment en Australie²⁶, nous observons que le ministère propose de créer un cadre global, puis des obligations spécifiques pour chaque secteur, qui s'articuleront autour de grands principes de prévention, détection, perturbation et réponse à la fraude.

Si nous adhérons à l'orientation générale du cadre proposé par le ministère, nous nous questionnons néanmoins sur les obligations exactes qui en résulteront.

D'emblée, Option consommateurs s'interroge quant à savoir si le cadre proposé apportera véritablement un rehaussement des obligations existantes pour les banques. Une vaste jurisprudence, au Québec, a reconnu aux institutions financières un devoir de diligence raisonnable envers leurs clients et leur a fait porter la responsabilité en cas de manquement²⁷. Ainsi, en vertu du droit civil québécois, les institutions financières sont *déjà* tenues à des obligations de prévention, de détection et de perturbation des fraudes. **Nous considérons donc que le cadre envisagé devra nécessairement imposer des obligations qui rehaussent le seuil actuel de protection, et non simplement réitérer des obligations déjà existantes pour les banques** – sans quoi nous doutons de sa véritable pertinence.

En outre, il va de soi que **l'ensemble du cadre doit être contraignant pour tous les secteurs visés**. À notre avis, les codes volontaires ou autres normes facultatives donnent des résultats peu probants. La mise en œuvre des normes du cadre doit donc être assurée par des sanctions pénales importantes pour les contrevenants, en plus d'offrir des recours civils aux consommateurs en cas de manquement. De plus,

²⁶ *Scams Prevention Framework Act 2025*, Act No. 15, 2025 (introduisant notamment la nouvelle Partie IVF dans le *Competition and Consumer Act 2010*).

²⁷ Voir notamment : *Alfagomma Inc. c. HSBC Bank Canada*, 2022 QCCS 3655; *Banque CIBC c. Dubois*, 2019 QCCS 3730; *Elbaz Chocron c. Banque Royale du Canada*, 2017 QCCQ 4669; *Airmax Industries inc. c. Banque de Montréal*, 2012 QCCS 4466.

l'organisme chargé de son application devrait disposer des pleins pouvoirs pour accomplir sa mission, notamment la capacité d'émettre des injonctions. Mentionnons d'ailleurs que le cadre australien, duquel s'inspire la présente Stratégie, prévoit de telles mesures²⁸.

2.1.2. Pour une approche multisectorielle et collaborative (questions 1 à 4)

Option consommateurs appuie l'approche proposée par le ministère visant à couvrir initialement les secteurs des banques, des sociétés de télécommunications et des plateformes en ligne. Tel qu'énoncé à la section 1, ces secteurs correspondent aux entreprises qui sont généralement mises à partie dans les cas de fraude que nous rapportent les consommateurs.

Nous estimons toutefois que le gouvernement devrait se réserver la possibilité d'élargir le cadre à d'autres secteurs qui pourraient eux aussi bénéficier d'un rehaussement de leurs pratiques en matière de fraude. À titre non exhaustif, nous attirons l'attention du ministère sur les secteurs suivants :

- les services postaux, considérant que les fraudeurs peuvent détourner le courrier des consommateurs²⁹;
- les fournisseurs de guichets de cryptomonnaies, qu'on peut notamment trouver dans les dépanneurs, et qui peuvent être exploités par les fraudeurs pour transférer de l'argent sans laisser de traces³⁰;
- le secteur des cartes prépayées, qui sont parfois utilisées par les fraudeurs comme instrument pour détourner l'argent des consommateurs.

Option consommateurs appuie également la proposition qu'un organisme central soit chargé de la surveillance et de la mise en œuvre des obligations du cadre, tout en laissant le soin à des organismes déjà établis de compléter ce cadre avec des normes sectorielles. Cependant, nous estimons que le gouvernement devrait s'assurer qu'une telle structure ne cause pas d'obstacles d'ordre bureaucratique qui

²⁸ Voir à cet effet : *Competition and Consumer Act 2010* (Australie), art. 58FA à 58FZQ.

²⁹ Francis PILON, *Boîtes postales collées et sabotées: enquête sur les fraudes de cartes de crédit ouverte à la Banque TD*, Journal de Montréal, 25 mars 2026, <https://www.journaldemontreal.com/2026/03/25/boites-postales-collees-et-sabotees-enquete-ouverte-a-la-banque-td-sur-les-fraudes-de-cartes-de-credit>

³⁰ Hugo JONCAS, *Couche-Tard en cour pour des fraudes dans ses magasins*, La presse, 17 décembre 2025, <https://www.lapresse.ca/affaires/entreprises/2025-12-17/quichets-de-bitcoin-depot-aux-etats-unis/couche-tard-en-cour-pour-des-fraudes-dans-ses-magasins.php>

limiteraient inutilement sa capacité d'agir, en mettant en œuvre une approche collaborative et efficace entre ces organisations.

2.1.3. Pour un échange de renseignements entre organisations (questions 5 à 11)

Un partage efficace de renseignements entre organisations concernant la fraude nous apparaît indispensable pour que la Stratégie puisse obtenir des résultats tangibles. Dans d'autres juridictions, les stratégies antifraudes prévoient également la centralisation et le partage de l'information en matière de fraude pour faire en sorte que tous les acteurs impliqués puissent réagir rapidement à l'évolution des fraudes.

L'information échangée ne devrait pas se limiter à de grandes tendances. Elle devrait inclure aussi de l'information précise pour bloquer immédiatement l'action des fraudeurs. Par exemple, une plateforme numérique qui identifie un utilisateur publiant des annonces menant à des contenus frauduleux devrait automatiquement en informer les autres acteurs, qui pourraient ensuite agir pour bloquer ses comptes bancaires ou ses services de télécommunications.

En outre, nous rappelons que les lois sur la protection des renseignements personnels permettent déjà aux organisations d'utiliser ou de communiquer des renseignements personnels à des fins de détection ou de prévention de la fraude³¹. Si les entreprises canadiennes sont en mesure d'identifier clairement et concrètement comment ces obligations légales constituent un obstacle à la lutte contre la fraude, il pourrait être opportun d'envisager le développement d'ententes multisectorielles ou de lignes directrices permettant de leur offrir plus de prévisibilité juridique.

Cela dit, tout cadre d'échange de renseignements personnels en matière de fraude devrait offrir des garanties sérieuses aux consommateurs :

- D'abord, le partage de renseignements personnels ne devrait s'effectuer qu'aux strictes fins de lutter contre la fraude. Aucun autre type d'utilisation de ces renseignements, par exemple à des fins de marketing, ne devrait être autorisé.

³¹ *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art. 7(3) d.2), annexe 1, principe 4.3. Au Québec, voir : *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 12 al. 2 (3°).

- Ensuite, il est incontournable de prévoir un mécanisme efficace et rapide pour rectifier l'information erronée qui pourrait avoir été communiquée dans le cadre du partage de renseignements, et ce, auprès de toutes les organisations concernées. Autrement, un consommateur honnête qui aurait malencontreusement fait l'objet d'un faux positif se trouverait indûment pénalisé par l'erreur.

Enfin, un partage d'information implique également une transparence avec le public. Afin d'informer les consommateurs sur les efforts de lutte à la fraude chez les organisations, nous proposons que le gouvernement s'inspire du Royaume-Uni où des données sur la fraude dans chaque institution financière ont été rendues publiques³². Notons également qu'en Europe, les plateformes en ligne sont tenues de produire des rapports de transparence concernant, entre autres, le contenu illégal identifié et le nombre d'injonctions émises par les États de l'Union européenne, par type de contenu illicite³³.

2.2. Commentaires sur les principes du cadre proposé

2.2.1. Prévention (questions 12 à 17)

Option consommateurs appuie les grandes orientations proposées par le ministère en matière de prévention, notamment les obligations générales liées à la gouvernance, à la formation du personnel, à la connaissance du client, ainsi qu'à la sensibilisation des consommateurs.

Sans prétention d'exhaustivité, nous portons à l'attention du ministère quelques préoccupations quant au principe de prévention tel qu'exposé dans le document de consultation :

- **Les organisations devraient être tenues d'informer clairement leurs clients lorsqu'elles font l'objet d'une hausse de cas de fraude.** Au cours des dernières années, nous avons observé des vagues de fraude qui ont ciblé certaines institutions financières. Or, les victimes clientes de ces institutions financières déplorent ne pas avoir été averties adéquatement du danger qui

³² Voir par exemple : PAYMENT SYSTEMS REGULATOR, *2024 APP scam performance data – before the reimbursement requirement was implemented*, 26 février 2026, p. 7
<https://www.psr.org.uk/media/b50p3mlm/psr-2024-app-scam-performance-data-february-2026.pdf>

³³ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, JO L 277 du 27.10.2022, p. 1-102 (ci-après « Règlement sur les services numériques »), art. 15.

les guettait, alors même que la banque ne pouvait pourtant pas ignorer être la cible de fraude.

- **Les méthodes pour mettre en garde les consommateurs ou pour les authentifier devraient être adaptées aux besoins de chaque type de clientèle.** Par exemple, des personnes âgées moins familières avec les technologies numériques nous ont rapporté qu'un appel téléphonique par un humain est plus susceptible de les mettre en garde contre un risque de fraude qu'un simple texto visant à les aviser ou les authentifier. En conséquence, les stratégies de communication, d'avis ou d'authentification des banques devraient être adaptées aux publics cibles, notamment en tenant compte de leur niveau de littératie numérique.
- **L'obligation de mettre en œuvre des méthodes d'authentification à deux facteurs ne devrait pas uniquement viser le secteur financier**, mais devrait plutôt s'appliquer à tous les secteurs visés par le cadre, pour l'ensemble des opérations pouvant comporter des risques pour les consommateurs. Par exemple, en Australie, la loi impose l'authentification multi facteurs en cas de demande de remplacement de la carte SIM afin de lutter contre les fraudes par carte SIM (*SIM swapping*)³⁴.

Concernant les plateformes numériques, nous appuyons fortement la proposition du ministère de contraindre les acteurs à la vérification des utilisateurs publiant de la publicité et au filtrage des contenus. Rappelons qu'en Europe, le *Règlement sur les services numériques* prévoit maintenant que les plateformes en ligne doivent adopter des mesures garantissant l'authenticité de la publicité, notamment l'identité de la personne physique ou morale qui la finance et le destinataire auquel celle-ci est présentée³⁵. Elles doivent également mettre à la disposition du public un registre afin de renforcer la transparence de la publicité en ligne, incluant qui paie pour la publicité et qui la reçoit³⁶.

³⁴ *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*, art. 6(1) High risk transaction et 10(5); <https://www.acma.gov.au/combating-phone-scams>

³⁵ *Règlement sur les services numériques*, art. 26.

³⁶ *Ibid.*, art. 39.

2.2.2. Détection (questions 18 à 30)

Option consommateurs appuie les grandes orientations proposées par le ministère en matière de détection, notamment l'obligation de repérer les activités frauduleuses et d'enquêter sur celles-ci, de prévenir les préjudices futurs, ainsi que d'échanger de l'information avec d'autres organisations.

Bien que nous appuyions ces grandes orientations, nous craignons que les **obligations de détection prévues dans un cadre éventuel ne soient pas assez rigoureuses**. Selon notre expérience, les capacités de détection des activités frauduleuses par les entreprises se sont en effet souvent montrées insuffisantes, et ce, dans chaque secteur :

- Dans le secteur financier, nous avons souvent observé que des banques ont autorisé des transactions frauduleuses tout à fait inhabituelles dans les comptes de leurs clients, sans intervenir pour y mettre fin. Par exemple, il pouvait s'agir de virements internationaux, de transferts Interac successifs tout juste en deçà du montant limite autorisé, de transactions depuis une marge de crédit inactive depuis des années, ou diverses autres transactions atypiques eu égard au profil du consommateur, par exemple en raison de leur montant, de leur fréquence ou du moment de la journée où elles surviennent. En outre, nous avons reçu plusieurs témoignages de transactions au comptoir où le consommateur a retiré des montants importants en argent comptant dans des circonstances manifestement suspectes, sans que le personnel de la banque n'intervienne pour investiguer davantage la situation.
- Dans le secteur des plateformes en ligne, il est reconnu que les géants du numérique ont fait preuve d'une inertie importante face aux publicités frauduleuses qui y sont diffusées³⁷. Ces publicités, souvent générées à l'aide de l'IA, circulent quasi librement sur leurs réseaux publicitaires et sont une porte d'entrée fréquente pour diverses arnaques. Pourtant, des mesures simples pourraient être mises en œuvre par les plateformes pour vérifier et détecter ces annonces, d'autant plus que les fraudeurs doivent payer pour les diffuser.

³⁷ Jeff HORWITZ, *Meta is earning a fortune on a deluge of fraudulent ads, documents*, Reuters, 6 novembre 2025, <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06>

- Dans le secteur des télécommunications, le CRTC a déjà déployé des mesures visant à limiter la mystification d'appels³⁸. Cependant, malgré ces efforts, force est de constater que les fraudes s'appuyant sur les télécommunications ont continué de sévir au Canada³⁹. Encore ici, nous considérons que des mesures de filtrage des appels additionnelles pourraient être déployées, en s'inspirant pour ce faire des meilleures pratiques développées à l'étranger⁴⁰.

En somme, il ne suffit pas d'énoncer un principe de détection : encore faut-il que les obligations sous-jacentes à ce principe soient suffisamment élevées.

2.2.3. Perturbation (questions 31 à 35)

Option consommateurs appuie les grandes orientations proposées par le ministère en matière de perturbation, notamment les obligations générales liées au retrait de l'accès aux fraudeurs connus, à la suspension des activités suspectes et à la mise en garde des utilisateurs.

Cependant, les obligations proposées nous apparaissent tout à fait incomplètes à l'égard des institutions financières. En effet, **les obligations de perturbation spécifiques pour les banques devraient être bien plus larges que la seule fermeture de comptes bancaires appartenant à des fraudeurs**⁴¹ :

- **Les banques doivent avoir l'obligation expresse de bloquer les transactions suspectées d'être frauduleuses.** Lorsqu'elles détectent une activité

³⁸ La *Politique réglementaire de Conformité et Enquêtes et de Télécom CRTC 2018-484* exige ainsi la mise en œuvre à l'échelle du réseau téléphonique du service de blocage universel d'appels comportant une mystification manifestement illicite de l'identité de l'appelant. De même, la *Décision de Conformité et Enquêtes et de Télécom CRTC 2021-123* prévoit la mise en œuvre des normes STIR/SHAKEN pour les appels vocaux sur protocole Internet. Voir : <https://crtc.gc.ca/fra/archive/2018/2018-484.htm>; <https://crtc.gc.ca/fra/archive/2021/2021-123.htm>

³⁹ Pour s'en convaincre, il suffit de jeter un œil sur la liste détaillée de fraudes recourant au téléphone ou au télécopieur établie par le Centre antifraude du Canada : <https://antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-fra.htm>

⁴⁰ Par exemple, l'Australie a adopté des lignes directrices pour les entreprises de télécommunications en matière de communications frauduleuses (*Scam Call Guidance*) qui prévoient une série de mesures pour mieux reconnaître, surveiller et bloquer les appels et les SMS frauduleux destinés aux consommateurs et qui favorisent le partage d'informations entre les acteurs. Voir : COMMUNICATIONS ALLIANCE LTD., *C661:2022 REDUCING SCAM CALLS and SCAM SMSs*, juillet 2022.

⁴¹ Nous n'ignorons point que le ministère propose aussi « de permettre aux titulaires de comptes de bloquer ou de désactiver des comptes ou certaines fonctionnalités d'un compte si elles soupçonnent que leur compte a été compromis. » Toutefois, il nous apparaît que ces éléments sont déjà couverts par les articles récemment ajoutés à la *Loi sur les banques* par la *Loi portant exécution de certaines dispositions du budget déposé au Parlement le 4 novembre 2025*.

potentiellement frauduleuse ou reçoivent un signalement à cet effet, les banques doivent avoir clairement l'obligation d'intervenir et de suspendre l'activité en cours, puis de faire enquête. Sans une telle obligation proactive, nous estimons que le résultat de l'ensemble de la Stratégie pourrait être largement compromis pour les consommateurs, sur qui reposerait alors un fardeau inégal de protection.

- La perturbation implique aussi **une intervention appropriée par le personnel de l'institution financière pour désamorcer les situations où la victime est sous l'emprise d'un criminel qui use de piratage psychologique**. Pour ce faire, le personnel de la banque devrait être formé non seulement pour reconnaître les indices de fraude, mais aussi pour s'adresser adéquatement au consommateur visé par la fraude afin de l'informer de la situation. Par exemple, nous avons vu des cas où des victimes se sont présentées en succursale pour effectuer des retraits considérables d'argent comptant, sans que le personnel n'intervienne de manière adéquate pour questionner davantage le consommateur ou suspendre la transaction.

Par ailleurs, nous doutons que de telles obligations de perturbation pourraient « déraisonnablement » priver les consommateurs de l'utilisation de leurs services (questions 31 et 33). Dans plusieurs cas de fraude qui nous ont été rapportés, il aurait suffi à la banque de bloquer la transaction manifestement suspecte, puis d'intervenir auprès du consommateur pour l'informer adéquatement, sans que cela ne lui cause un quelconque préjudice. De plus, nous attirons l'attention du ministère sur les initiatives développées par des banques au Royaume-Uni pour intervenir auprès de victimes avec lesquelles il est plus complexe de désamorcer la situation, telles que des victimes de fraudes amoureuses, qui ont mis sur pied des équipes d'intervention spécialisées (*Break the Spell teams*)⁴².

2.2.4. Réponse (questions 36 à 45)

Nous accueillons favorablement la proposition du ministère d'offrir un recours en indemnisation pour les consommateurs en cas de non-conformité par une organisation. Tel que mentionné précédemment (section 2.1.1), nous estimons que les mesures proposées dans la Stratégie doivent comporter des obligations

⁴² Anna Tims, 'He spent thousands': how a bank team tries to rescue scam victims, The Guardian, 1er février 2025, <https://www.theguardian.com/money/2025/feb/01/bank-team-scam-victims-fraud>

contraignantes pour les organisations concernées, assorties de sanctions pénales et civiles en cas de manquement. Cette approche s'arrime d'ailleurs à celle développée en Australie, où le cadre antifraude permet les recours civils du consommateur en cas de manquement⁴³.

Nous sommes également favorables à ce que les consommateurs aient accès à des processus clairs de règlement des différends via un point d'entrée unique, dans la mesure où ce processus leur permettrait aisément d'être indemnisés par un seul acteur, même dans les cas où la responsabilité pourrait être partagée parmi plusieurs d'entre eux. En outre, nous estimons que les organismes chargés du traitement des plaintes externes devraient avoir le pouvoir d'émettre des décisions contraignantes envers les entreprises afin d'éviter aux consommateurs d'avoir à se tourner vers les tribunaux.

Cela dit, Option consommateurs propose de bonifier significativement les obligations qui sont mentionnées au chapitre de la « réponse » :

- Les organisations devraient non seulement avoir l'obligation de disposer de canaux simples pour signaler les fraudes et porter plainte, mais également **l'obligation de répondre aux signalements reçus**. Une telle obligation serait particulièrement pertinente à l'égard des plateformes numériques, où les plaintes et les signalements peuvent souvent rester lettre morte. Selon une enquête de *Reuters*, 96 % des signalements de contenus frauduleux transmis par les utilisateurs de Facebook auraient ainsi été ignorés⁴⁴. Cela est d'autant plus préoccupant que, selon le Baromètre de confiance d'Option consommateurs et du Consortium de recherche empirique en droit interdisciplinaire numérique et financier (CREDI-NF), 24 % de Canadiens disent avoir déjà signalé une publicité frauduleuse sur les médias sociaux⁴⁵.
- Comme en Europe, le cadre pourrait également **prévoir la mise en place de « signaleurs de confiance » sur les plateformes**, qui seraient en mesure de

⁴³ Nous notons aussi que le cadre australien prévoit que la préférence doit être accordée à la compensation de la victime plutôt qu'à l'imposition d'une amende lorsque le contrevenant n'a pas de fonds suffisants. Voir : *Competition and Consumer Act 2010* (Australie), art. 58FD.

⁴⁴ Jeff HORWITZ, *Meta is earning a fortune on a deluge of fraudulent ads, documents*, Reuters, 6 novembre 2025, <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06>

⁴⁵ OPTION CONSOMMATEURS et CONSORTIUM DE RECHERCHE EMPIRIQUE EN DROIT INTERDISCIPLINAIRE NUMÉRIQUE ET FINANCIER, *Baromètre de confiance*, Étude réalisée auprès de la population canadienne par Léger, 2026 [à paraître].

notifier de manière prioritaire les entreprises du contenu illégal sur les plateformes en ligne⁴⁶.

- De même, nous proposons de prévoir des mesures pour **élargir les capacités des organisations de récupérer des fonds ou des comptes piratés après une fraude**. Par exemple, nous avons reçu plusieurs témoignages de victimes qui rapportent avoir contacté très rapidement leur banque après avoir été victimes de transferts frauduleux; or, malgré la célérité de leur signalement, ces consommateurs se sont vu répondre qu'il était impossible de retourner les fonds transférés. D'autres consommateurs nous ont rapporté être incapables de récupérer leurs comptes de médias sociaux qui ont été usurpés, malgré toutes leurs tentatives auprès de la plateforme.
- Considérant les impacts désastreux qu'ont les fraudes sur la santé mentale des victimes, **une Stratégie nationale antifraude ne peut être complète sans aborder la question du soutien psychologique aux victimes**. Nous estimons que les entreprises des secteurs visés devraient s'assurer que leurs équipes sont formées pour accompagner adéquatement les victimes, et les diriger vers les ressources appropriées.

2.3. Autres aspects (questions 46 à 50)

Bien que la sensibilisation des Canadiens sera manifestement insuffisante à elle seule pour endiguer la vague de fraude qui frappe le pays, Option consommateurs est évidemment favorable au déploiement de stratégies visant à mieux informer les consommateurs des risques d'arnaques. Pour atteindre cet objectif, nous estimons que les milieux communautaires devraient être mis à partie en s'assurant de soutenir les organismes de la société civile faisant de l'éducation financière et de la prévention sur les fraudes.

En outre, nous proposons deux mesures pour s'assurer d'une meilleure coordination des organisations en matière de fraude :

- Premièrement, nous proposons de nommer un ministre responsable de la fraude, comme cela a été fait au Royaume-Uni. Une telle nomination

⁴⁶ Règlement sur les services numériques, art. 22.

permettrait notamment à un élu responsable de chapeauter l'ensemble des organisations luttant contre la fraude.

- Deuxièmement, le gouvernement devrait profiter de l'expertise acquise par le Centre antifraude du Canada depuis plusieurs années, en envisageant de fusionner cet organisme avec la nouvelle agence nationale.

Sommaire des principales recommandations

- **Établir un régime de responsabilité des banques exigeant qu'elles remboursent leurs clients victimes de fraude, à moins qu'ils aient commis une négligence grave dans le cadre de la fraude.**
- **Établir un régime de responsabilité des entreprises de télécommunications et des plateformes numériques qui manquent à détecter et à bloquer les contenus frauduleux prévoyant :**
 - **l'obligation de rembourser les victimes des arnaques qui ont trouvé leur point d'entrée via leurs services;**
 - **un recours récursoire pour les institutions financières qui ont indemnisé un client victime de fraude.**
- **S'assurer que le cadre antifraude multisectoriel soit contraignant pour tous les secteurs visés et qu'il rehausse le seuil des obligations déjà existantes pour les organisations.**
- **Développer un cadre permettant aux organisations d'échanger rapidement de l'information précise pour bloquer immédiatement l'action des fraudeurs, dans le respect des droits des consommateurs.**
- **Rendre publiques des données statistiques sur la fraude dans chaque institution financière.**
- **Mieux prévenir les fraudes en exigeant des organisations visées par le cadre qu'elles :**
 - **informent clairement leurs clients lorsqu'elles font l'objet d'une hausse de cas de fraude d'un type spécifique;**
 - **adaptent leurs méthodes pour mettre en garde les consommateurs ou pour les authentifier aux besoins de chaque type de clientèle;**
 - **mettent en œuvre des méthodes d'authentification à deux facteurs pour l'ensemble des opérations pouvant comporter des risques pour les consommateurs.**

- **Rehausser significativement les obligations de détection des fraudes envisagées dans la consultation sur le cadre antifraude multisectoriel.**
- **Élargir les obligations de perturbation applicables aux banques, afin de prévoir notamment :**
 - **l'obligation expresse de bloquer les transactions suspectées d'être frauduleuses;**
 - **l'obligation d'intervenir de manière appropriée pour désamorcer les situations où la victime est sous l'emprise d'un criminel qui use de piratage psychologique.**
- **Bonifier les obligations en matière de réponse à la fraude :**
 - **instaurer une obligation de répondre aux signalements reçus;**
 - **prévoir la mise en place de « signaleurs de confiance » sur les plateformes numériques ;**
 - **élargir les capacités des organisations de récupérer des fonds ou des comptes piratés après une fraude;**
 - **créer une obligation d'accompagner adéquatement les victimes.**
- **Nommer un ministre fédéral responsable de la fraude, comme cela a été fait au Royaume-Uni.**