Rapport de recherche

Les aînés et la fraude au Canada

OPTION consommateurs

Ce projet a été financé par la Fondation Mirella et Lino Saputo ; les opinions exprimées ici sont celles de l'auteur et ne reflètent pas nécessairement celles de la Fondation Mirella et Lino Saputo.

Rédigé par Luis Pineda

Option consommateurs
507, Place d'Armes, bureau 1101
Montréal (Québec)
H2Y 2W8
Téléphone : 514 598-7288 | 1 888-412-1313
Télécopieur : 514 598-8511

Courriel : info@option-consommateurs.org
Site Internet : www.option-consommateurs.org

À propos d'Option consommateurs
Option consommateurs est une association à but non lucratif qui a pour mission d'aider les consommateurs et de défendre leurs droits.
Option consommateurs informe les consommateurs qui ont une mésentente avec un commerçant, les reçoit en consultation budgétaire et donne des séances d'information sur le budget, l'endettement, le droit de la consommation et la protection de la vie privée. Chaque année, nous réalisons des recherches sur des enjeux de consommation d'importance. Nous intervenons également auprès des décideurs et des médias pour dénoncer des situations inacceptables.
Pour faire changer les choses, les actions d'Option consommateurs sont multiples : recherches, actions collectives et pressions auprès des instances gouvernementales et des entreprises. Vous pouvez nous aider à en faire plus en soutenant Option consommateurs. Pour plus d'information : www.option-consommateurs.org.

Table des matières

Remerciements

L'auteur tient à remercier les employés, stagiaires et bénévoles qui œuvrent chez Option consommateurs et qui, de près ou de loin, ont collaboré à cette recherche. Il tient particulièrement à remercier Alexandre Plourde et Sara Eve Levac pour leurs commentaires, Catherine Bélanger-Khoury pour le partage de ses analyses, ainsi qu'Alison Ostheimer et Ma'ila Charland, étudiantes en droit à l'Université de Montréal, pour leur aide et leur soutien pendant la recherche.

Résumé

La fraude atteint des sommets au Canada. En 2024, le Centre antifraude du Canada (CAFC) a reçu 108 878 signalements de fraude, représentant plus de 638 millions de dollars en pertes. Selon cet organisme, ces chiffres ne représenteraient que 5 à 10 % des cas de fraude se produisant au Canada.

Bien qu'une part considérable des signalements provienne de personnes âgées, le phénomène liant fraude et vieillissement demeure peu exploré. Son étude soulève en effet de nombreux défis, notamment le flou conceptuel entourant la notion d'aîné, la disparité des catégorisations des différents types de fraude, ainsi que le caractère essentiellement exploratoire et descriptif de la littérature existante.

Pourtant, les conséquences de la fraude peuvent être catastrophiques pour les victimes, en particulier pour les personnes les plus vulnérables. Ses effets dépassent les seules pertes financières : elle affecte aussi la santé physique et mentale des victimes ainsi que celle de leurs proches. La fraude est ainsi un enjeu majeur de sécurité économique et de santé publique.

À l'exception d'une loi au Québec qui n'est pas encore en vigueur, actuellement le Canada ne dispose d'aucune législation protégeant l'ensemble des victimes de fraude. Selon la loi, seules les transactions dites « non autorisées » sur la carte de crédit font, dans certains cas, l'objet d'une obligation légale de remboursement par les institutions financières. Pour les autres situations, les victimes se retrouvent dépourvues de protection, et ce, même si elles ont été la cible d'une supercherie sophistiquée. Cette situation crée un sentiment d'injustice chez les victimes, qui s'interrogent sur le caractère arbitraire des lois encadrant le remboursement, en distinguant entre celles qui méritent d'être remboursées et celles qui ne le méritent pas.

Option consommateurs recommande que le Canada et le Québec se dotent d'un encadrement robuste pour prévenir la fraude et protéger les victimes. À l'instar de l'Australie, le Canada devrait responsabiliser l'ensemble des acteurs dans les principaux secteurs où les fraudeurs opèrent — comme les services financiers, les télécommunications et les plateformes numériques — et les inciter ainsi à adopter des mesures de protection plus efficaces. Comme l'Union européenne, le Canada pourrait s'attaquer aux contenus frauduleux diffusés sur les plateformes en ligne, en tenant les géants du web responsables de la prévention et de l'atténuation des risques liés au monde numérique. De plus, à l'instar du Royaume-Uni, le Canada gagnerait à exiger des institutions financières qu'elles remboursent les victimes de tout type de fraude, contribuant ainsi à pallier ses conséquences. Le Canada pourrait également envisager de mettre en place des mesures spéciales de protection pour les personnes les plus vulnérables, comme les aînés, qui ne devraient pas pouvoir se voir refuser un remboursement, quelles que soient les circonstances.

Introduction

La fraude est un crime de portée transnationale ayant de lourdes conséquences sur la santé publique et la sécurité nationale[1]. Ses effets dépassent les seules pertes financières : elle touche aussi la santé physique et mentale des victimes ainsi que celle de leurs proches[2]. De plus, la fraude nuit à la confiance envers le système financier canadien, dans un contexte d'incertitude économique croissante[3].

En 2024, le Centre antifraude du Canada (CAFC) a reçu 108 878 signalements de fraude, représentant plus de 638 millions de dollars en pertes[4]. Un nombre important de ces signalements provient de personnes âgées, qui pourraient être davantage ciblées par les fraudeurs en raison de leur vulnérabilité[5]. Cette situation pourrait avoir des conséquences à long terme, notamment à cause du vieillissement de la population canadienne[6].

Les associations de consommateurs dénoncent depuis longtemps le manque de protection des victimes de fraude, tout spécialement des personnes les plus vulnérables, ainsi que les obstacles qu'elles rencontrent lorsqu'elles essaient de se faire rembourser auprès des banques[7].

Cette recherche a voulu se pencher sur le phénomène de la fraude ciblant les aînés, afin de mieux le comprendre et de formuler des recommandations visant à protéger les victimes.

Pour ce faire, nous avons tenté de répondre aux questions suivantes à partir d'une revue de la littérature scientifique, ainsi que de l'analyse des législations les plus importantes au Canada, en Australie, au Royaume-Uni et dans l'Union européenne.

---

[1] Interpol, *Interpol Global Financial Fraud Assessment*, 2024, 10.
[2] David Burnes et al., "Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis," *American Journal of Public Health* 107, no. 8 (août 2017): 13, https://doi.org/10.2105/AJPH.2017.303821.
[3] Paiements Canada, *Cadre des politiques du nouveau système de paiement en temps réel du Canada : Document de consultation sur le système de paiement en temps réel*, 2025, 30, https://www.paiements.ca/sites/default/files/PaymentsCanada_Real-TimeRail_ConsultationDocument_Fr.pdf.
[4] Centre antifraude du Canada (CAFC), « Trousse d'outils 2025, Montre-moi la fraude », 2025, 9.
[5] Madeleine Pilote-Côté, "Fraude : les jeunes doivent protéger leurs proches," *Le Journal de Montréal*, 14 avril 2025, https://www.journaldemontreal.com/2025/04/14/fraude-les-jeunes-doivent-proteger-leurs-proches.
[6] Statistics Canada, Government of Canada, "The Older People Are All Right," 23 septembre 2024, https://www.statcan.gc.ca/o1/en/plus/7059-older-people-are-all-right.
[7] Zone Politique – ICI.Radio-Canada.ca, "PDL 72 : pas assez de mordant contre la fraude bancaire, selon Option consommateurs," *Radio-Canada*, 2 octobre 2024, https://ici.radio-canada.ca/nouvelle/2108980/projet-loi-72-fraude-option-consommateurs.

Questions de recherche

- Quel est l'état des connaissances sur le phénomène de la fraude ciblant les aînés ?
- Quelles sont les fraudes les plus courantes à l'encontre des aînés ?
- Quel est le niveau de responsabilité des institutions financières face à la fraude ? Quels types de fraudes sont susceptibles d'être remboursés ?
- Quelles sont les juridictions les plus protectrices en matière de prévention et de remboursement en cas de fraude ?
- Quelles sont les meilleures recommandations pour protéger les aînés victimes de fraude au Canada ?

1. Les défis d'étudier la fraude ciblant les aînés

Les études cherchant à comprendre le phénomène de la fraude ciblant les aînés se heurtent à des obstacles majeurs et étroitement liés : un manque de clarté conceptuelle quant à la notion d'aîné, une disparité dans la caractérisation des différents types de fraude, ainsi que le caractère exploratoire et descriptif de la littérature sur le sujet.

Les débats visant à définir à partir de quel moment une personne devient une aînée ont cours depuis longtemps et n'ont pas abouti à des solutions définitives[8]. Cette même difficulté est encore présente aujourd'hui dans les études portant sur la fraude ciblant les aînés. Chaque auteur propose une définition différente de ce qu'est un aîné : une personne âgée de 50 ans et

[8] Simone de Beauvoir, *La vieillesse* (Paris: Gallimard, 1970), 8–9, https://shs.cairn.info/la-vieillesse--9782070444151?tab=sommaire.

plus[9], quelqu'un de 55 ans et plus[10], des personnes de 60 ans et plus[11], ou toute personne de 65 ans et plus[12]. Entre la limite inférieure et la limite supérieure d'âge dans ces différentes définitions — 50 et 65 ans — il existe un écart considérable de 15 ans.

Quant à la fraude, la plupart des définitions s'inspirent de celle du *Code criminel* du Canada, qui la décrit comme tout acte commis par « quiconque [qui] par supercherie, mensonge ou autre moyen dolosif […] frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur[13] ». Autrement dit, il s'agit de tout acte qui, par la tromperie, cherche à obtenir un bien, généralement de nature monétaire[14]. Il convient de souligner que, dans le langage courant, la notion de fraude ne se limite pas à un acte criminel et qu'elle est souvent utilisée pour désigner des comportements malveillants ou des actes pouvant porter préjudice à une personne sans nécessairement relever de la définition légale du crime[15].

Si la définition de la fraude est généralement large dans la littérature, les adjectifs qui l'accompagnent ainsi que les différentes typologies rendent le phénomène d'autant plus flou et polysémique. Ainsi, la littérature peut parfois

---

[9] Rusli Abdullah, Muhammad Amirrul Alhafiz Bin Mohd Zukry, et Nur Aqmal Bin, « Strategies for Protecting Senior Citizens Against Online Banking Fraud and Scams: A Systematic Literature Review », ResearchGate, 22 octobre 2024, 5547, https://www.researchgate.net/publication/382868338_STRATEGIES_FOR_PROTECTING_SENIOR_CITIZENS_AGAINST_ONLINE_BANKING_FRAUD_AND_SCAMS_A_SYSTEMATIC_LITERATURE_REVIEW ; Cassandra Cross, « 'But I've Never Sent Them Any Personal Details Apart from My Driver's Licence Number …': Exploring Seniors' Attitudes towards Identity Crime », *Security Journal* 30, no. 1 (janvier 2017): 78, https://doi.org/10.1057/sj.2015.23 ; Cassandra Cross, « "They're very lonely": Understanding the fraud victimisation of seniors », *International Journal for Crime, Justice and Social Democracy* 5, no. 4 (2016): 62.

[10] Donald Rebovich et Leslie Corbo, « The distillation of national crime data into a plan for elderly fraud prevention: A quantitative and qualitative analysis of US Postal Inspection Service cases of fraud against the elderly », dans *The New Technology of Financial Crime*, (Routledge, 2022), 126–49, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003258100-7/distillation-national-crime-data-plan-elderly-fraud-prevention-quantitative-qualitative-analysis-postal-inspection-service-cases-fraud-elderly-donald-rebovich-leslie-corbo.

[11] Niroop Sugunaraj, Akshay Ram Ramchandra, et Prakash Ranganathan, « Cyber fraud economics, scam types, and potential measures to protect US seniors: A short review », dans *2022 IEEE International Conference on Electro Information Technology (eIT)* (IEEE, 2022), 623, https://ieeexplore.ieee.org/abstract/document/9813960/?casa_token=66mHLYr6ZfYAAAAA:fDbHixfMRo2_bJ8hxiJy3-QsZ2OnzTPVk_45GvcC7z-KPJDQMcs_RPAtipueDkOtsMWy7aXv6tQ ; FBI, *Elder Fraud Report*, 2023, https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf.

[12] Steven Kemp et Nieves Erades Pérez, « Consumer fraud against older adults in digital society: Examining victimization and its impact », *International Journal of Environmental Research and Public Health* 20, no. 7 (2023): 1 ; Carole A. Cohen, « Consumer Fraud and the Elderly: A Review of Canadian Challenges and Initiatives », *Journal of Gerontological Social Work* 46, nos. 3-4 (18 juillet 2006): 137–44, https://doi.org/10.1300/J083v46n03_08.

[13] Code criminel, LRC 1985, c C-46, art. 380(1).

[14] Cassandra Cross, « "They're very lonely" », 61.

[15] Laura Huey et Lorna Ferguson, « What do we know about senior citizens as cybervictims? A rapid evidence synthesis », *CrimRxiv*, 2022, 22, https://assets.pubpub.org/i1rp6ysl/e6b80803-869b-4d90-ad26-30615a7c4abc.pdf.

parler de « fraude financière[16] », de « fraude bancaire en ligne[17] », de « cyberfraude[18] » ou encore de « fraude à la consommation[19] » pour désigner, plus ou moins, un même phénomène.

Le développement d'une typologie de la fraude se heurte également à plusieurs obstacles. Premièrement, un même type de fraude peut être nommé différemment selon les organisations concernées. Par exemple, le Service de Police de la Ville de Montréal (SPVM) utilise la notion de « fraude du faux représentant[20] » pour désigner un fraudeur qui se fait passer pour un employé de banque. Toutefois, cette catégorie n'existe pas au sein du Centre antifraude du Canada, qui pourrait classer ce type de fraude dans d'autres catégories, comme la « fraude de service » ou la fraude de « l'enquêteur bancaire[21] ». Deuxièmement, les fraudeurs combinent souvent plusieurs types de fraude ou emploient des méthodes hybrides. C'est le cas des fraudes amoureuses, qui peuvent inclure une demande d'investissement (« fraude à l'investissement »), souvent réalisée par l'achat de cryptomonnaies (« fraude liée aux cryptomonnaies[22] »). Enfin, les fraudes évoluent à une vitesse fulgurante, ce qui rend difficile l'élaboration d'une typologie conceptuellement utile[23].

Concernant les aînés spécifiquement, la littérature distingue généralement l'exploitation ou l'abus financier de la fraude[24]. L'abus et l'exploitation financière sont commis par un proche, un soignant ou une autre personne de confiance.

---

[16] David Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », e13–21.
[17] Rusli Abdullah, Muhammad Amirrul Alhafiz Bin Mohd Zukry, et Nur Aqmal Bin, « Strategies for Protecting Senior Citizens Against Online Banking Fraud and Scams », 5547.
[18] Niroop Sugunaraj, Akshay Ram Ramchandra, et Prakash Ranganathan, « Cyber fraud economics, scam types, and potential measures to protect US seniors: A short review ».
[19] Steven Kemp et Nieves Erades Pérez, « Consumer fraud against older adults in digital society: Examining victimization and its impact » ; Carole A. Cohen, « Consumer Fraud and the Elderly », 137–44.
[20] Service de police de la Ville de Montréal (SPVM), « Fraude des faux représentants – Service de police de la Ville de Montréal (SPVM) », consulté le 30 avril 2025, https://spvm.qc.ca/fr/Fiches/Details/Fraude-des-faux-representants.
[21] Gendarmerie royale du Canada, Centre antifraude du Canada (CAFC), « Service », 31 janvier 2020, https://antifraudcentre-centreantifraude.ca/scams-fraudes/service-fra.htm#a4 ; Gendarmerie royale du Canada, Centre antifraude du Canada (CAFC), « Enquêteur bancaire », 31 janvier 2020, https://antifraudcentre-centreantifraude.ca/scams-fraudes/b-investigator-enqueteur-fra.htm.
[22] Interpol, « Interpol Global Financial Fraud Assessment », 2024, 5, 13.
[23] Comme nous le verrons plus loin, la distinction juridique entre fraude « non autorisée » et « autorisée » s'avère plus utile pour cerner le problème et envisager un remboursement des victimes. Cela dit, les différentes typologies peuvent être importantes pour informer et alerter le public face à la fraude.
[24] Niroop Sugunaraj, Akshay Ram Ramchandra, et Prakash Ranganathan, « Cyber fraud economics, scam types, and potential measures to protect US seniors: A short review », 623 ; Katalin Parti, « "Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization », 2022, 20, https://vtechworks.lib.vt.edu/items/fa169b03-376e-4884-aa43-37fb317acae2 ; David Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 14.

En revanche, les fraudes et escroqueries financières ciblant les aînés sont généralement commises par des inconnus.

Enfin, probablement en raison du flou conceptuel, un défi majeur pour la compréhension du phénomène réside dans l'état actuel des études sur le sujet. Les recherches sur la fraude ciblant les aînés sont plutôt exploratoires, descriptives et manquent de diversité ainsi que de bases solides permettant de proposer des politiques publiques concrètes pour prévenir ou faire face à la fraude[25].

Par exemple, les connaissances sur l'ampleur du phénomène et sur ses effets réels sur les aînés restent limitées[26]. Des lacunes persistent quant aux variables cognitives, psychologiques, contextuelles, et structurelles qui pourraient rendre les aînés particulièrement vulnérables à la fraude[27]. La plupart des solutions proposées se résument à des stratégies individuelles de prévention[28]. De plus, la sous-représentation des signalements de fraude et le manque de données complètement fiables limitent l'ensemble des connaissances sur la fraude ciblant les aînés (section 2)[29].

2. Ce que disent les statistiques

La fraude est un problème grandissant au Canada et constitue le type de cybercrime le plus répandu au pays, selon le Programme de déclaration uniforme de la criminalité du Centre canadien de la statistique juridique et de la sécurité des collectivités (CCSJSC)[30].

Il convient d'abord de signaler que toutes les statistiques souffrent d'un problème de sous-représentation, en raison de la tendance des victimes à ne

---

[25] Laura Huey et Lorna Ferguson, « What do we know about senior citizens as cybervictims? », 2–11.
[26] Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 21.
[27] W. Carter, *Digital Deception and the Aging Mind: A Psychological Analysis of Online Fraud Targeting Older Adults* (2025), 2, 3, 5, https://www.preprints.org/frontend/manuscript/96080fe65a8ac7e413506c1a92646468/download_pub.
[28] Huey et Ferguson, « What do we know about senior citizens as cybervictims? », 17-18.
[29] Maya Dubord, *Mesurer la cybercriminalité : Canada, Australie, Royaume-Uni*, *Vol. 5, no 3*, Chaire de recherche en prévention de la cybercriminalité, https://www.prevention-cybercrime.ca/_files/ugd/9d4ef1_544470dbb0294c3e96ff2a27d44ef0a8.pdf ; Carter, *Digital Deception and the Aging Mind*, 3.
[30] Statistique Canada, « Cybercrimes déclarés par la police, nombre d'affaires et taux pour 100 000 habitants, Canada, provinces, territoires, régions métropolitaines de recensement et Police militaire des Forces canadiennes », 25 juillet 2024, https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=3510000201; Statistique Canada, « Cybercrimes déclarés par la police, selon l'infraction reliée à la cybercriminalité, Canada (certains services de police) », 25 juillet 2024, https://www150.statcan.gc.ca/t1/tbl1/fr/cv!recreate-nonTraduit.action?pid=3510000101.

pas déclarer la fraude[31]. En effet, selon certaines estimations, moins du tiers des cas de fraude sont signalés aux autorités[32], et des sondages réalisés au Canada indiquent que ce taux pourrait être aussi bas que 11 %[33]. Pour le Centre antifraude du Canada, ces chiffres ne représenteraient que 5 à 10 % des cas de fraude au pays[34].

Selon certains auteurs, la sous-représentation pourrait être plus importante encore chez les aînés[35]. Par exemple, les personnes âgées pourraient ne pas signaler la fraude dont elles sont victimes et la cacher à leurs proches par peur d'être blâmées, d'être perçues comme ayant perdu des capacités cognitives ou d'être remises en question quant à leur capacité à maintenir leur indépendance financière. En effet, comme nous le verrons plus loin (section 3), la fraude s'accompagne généralement de sentiments de honte, de peur et de déni[36].

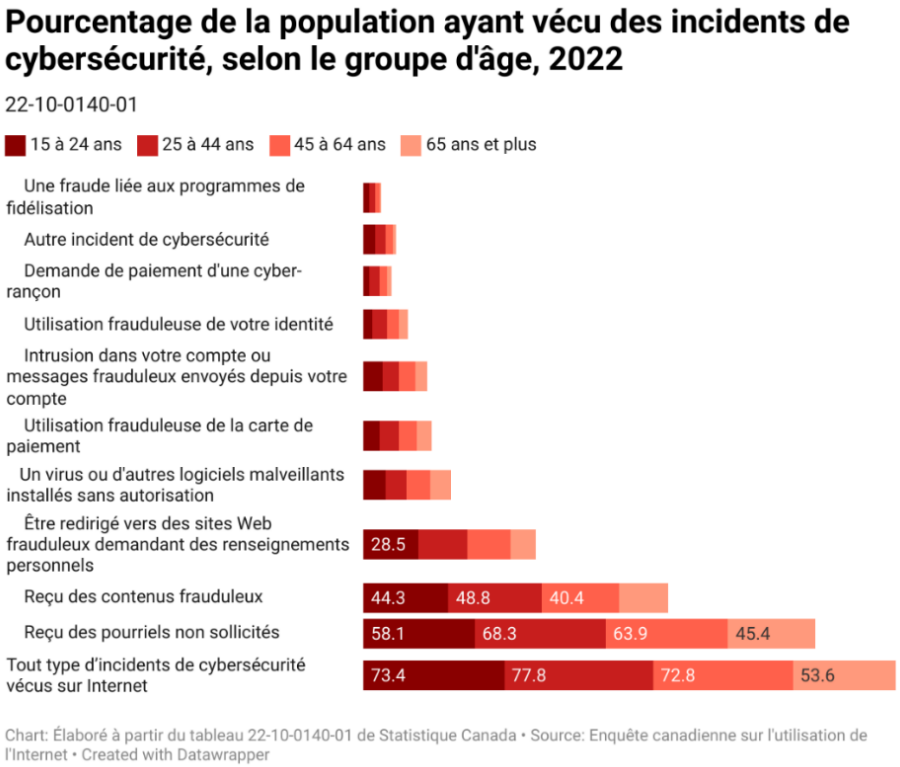
Cela dit, les données disponibles permettent de faire un constat général : il n'existe pas de profil type de personne plus encline qu'une autre à subir ce type de crime. Quelles que soient les caractéristiques démographiques, toutes les personnes sont susceptibles d'être victimes de fraude[37]. Les méthodes employées par les fraudeurs sont si sophistiquées que, contrairement à ce qu'on pourrait penser, les individus jeunes ou hautement scolarisés courent autant de risques d'en être victimes que les autres[38].

En ce qui concerne les aînés, la fraude pourrait être le type de crime le plus fréquemment subi par les personnes âgées, comparativement à d'autres formes de criminalité[39].

---

[31] Katalin Parti, « "Elder Scam" Risk Profiles », 23; David Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 19.
[32] Cassandra Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », *The Journal of Adult Protection* 23, no. 2 (31 décembre 2020): 99, https://doi.org/10.1108/JAP-08-2020-0035.
[33] Statistics Canada Government of Canada, « How Much Is Fraud Affecting Canadians and Canadian Businesses? », 13 mars 2025, https://www.statcan.gc.ca/o1/en/plus/7905-how-much-fraud-affecting-canadians-and-canadian-businesses.
[34] Centre antifraude du Canada, *Rapport annuel 2022*, page 4, https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-fra.pdf.
[35] Parti, « "Elder Scam" Risk Profiles », 23 ; Jan Bailey et al., « Older adults and "scams": Evidence from the mass observation archive », *The Journal of Adult Protection* 23, nº 1 (2021): 60, 62, 65 ; Carter, *Digital Deception and the Aging Mind*, 3.
[36] Carter, *Digital Deception and the Aging Mind*, 3.
[37] Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », 99.
[38] Tristan Péloquin, « Fraudes par cartes bancaires: "Tout avait l'air vrai" », *La Presse*, 21 octobre 2024, section Justice et faits divers, https://www.lapresse.ca/actualites/justice-et-faits-divers/2024-10-21/fraudes-par-cartes-bancaires/tout-avait-l-air-vrai.php.
[39] Annie Lecompte, « The Scale of Fraud against Seniors Is Huge, and Still Growing — Here's Why », *The Conversation*, 28 octobre 2024, http://theconversation.com/the-scale-of-fraud-against-seniors-is-huge-and-still-growing-heres-why-240595; Cassandra Cross, « "They're very lonely" », 61 ; Thomas Gabor et John Kiedrowski, *Crime and Abuse Against Seniors: A Review of the Research Literature With*

L'*Enquête canadienne sur l'utilisation de l'Internet* de Statistique Canada, menée en 2022, concluait que, pour tous les types d'incidents de cybersécurité, plus de la moitié (53,6 %) des personnes de 65 ans et plus avaient été touchées[40].

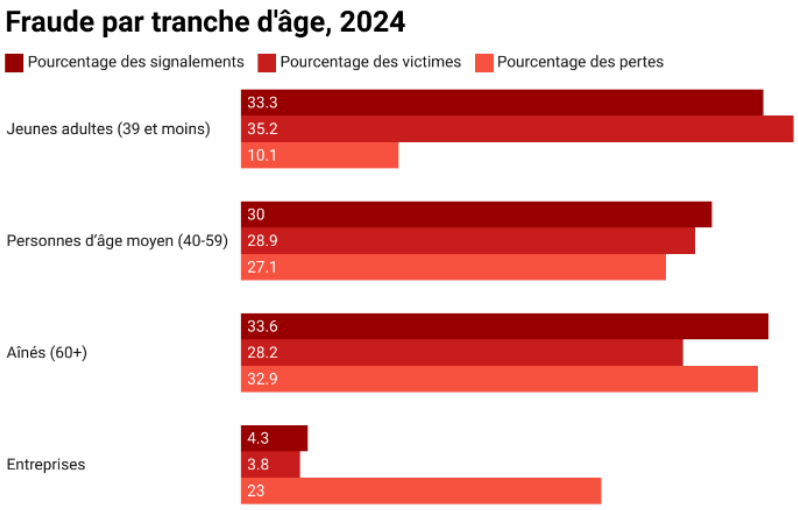


Quant aux données du Centre antifraude du Canada pour 2024, les personnes de 60 ans et plus représentent presque le tiers des victimes ; elles effectuent davantage de signalements et subissent des pertes financières plus importantes[41].

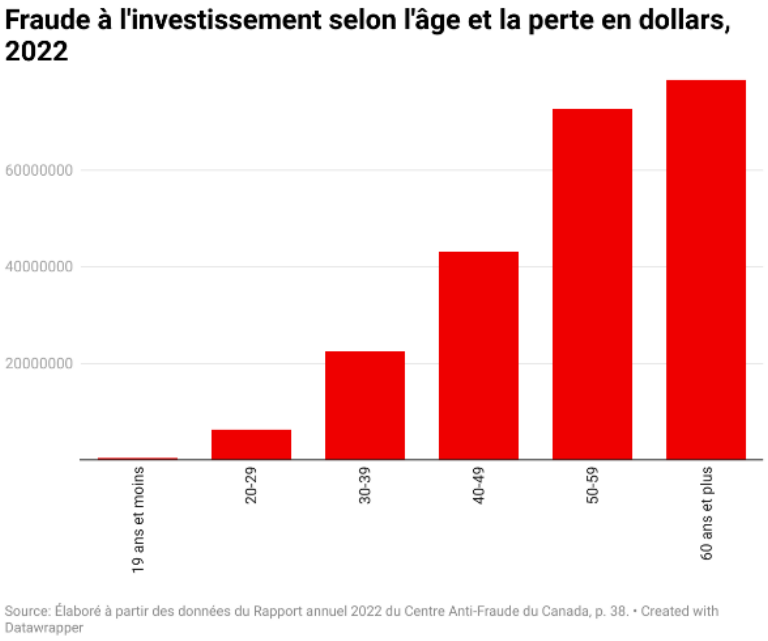
Special Reference to the Canadian Situation (2021), section 4.1 « Prevalence and Incidence of Criminal Victimization and Abuse Against Seniors », ministère de la Justice du Canada, consulté le 17 juin 2025, https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/crim/p41.html#tb1.

[40] Statistique Canada, « Incidents liés à la sécurité et à la vie privée survenus sur Internet, selon le groupe d'âge », 20 juillet 2023, https://www150.statcan.gc.ca/t1/tbl1/fr/cv.action?pid=2210014001.

[41] Centre antifraude du Canada (CAFC), « Trousse d'outils 2025 », 9.



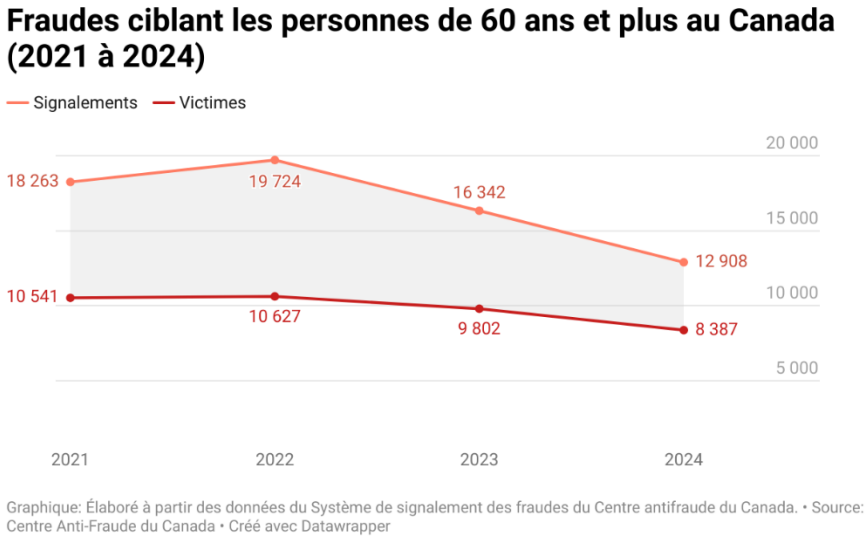
En effet, à partir des données de 2022, le rapport annuel du Centre antifraude du Canada montrait que les aînés perdaient davantage d'argent en raison de la fraude la plus coûteuse pour les consommateurs : la fraude à l'investissement[42].



Bien que les données du Centre antifraude du Canada concernant les personnes de 60 ans et plus permettent de constater qu'une baisse des

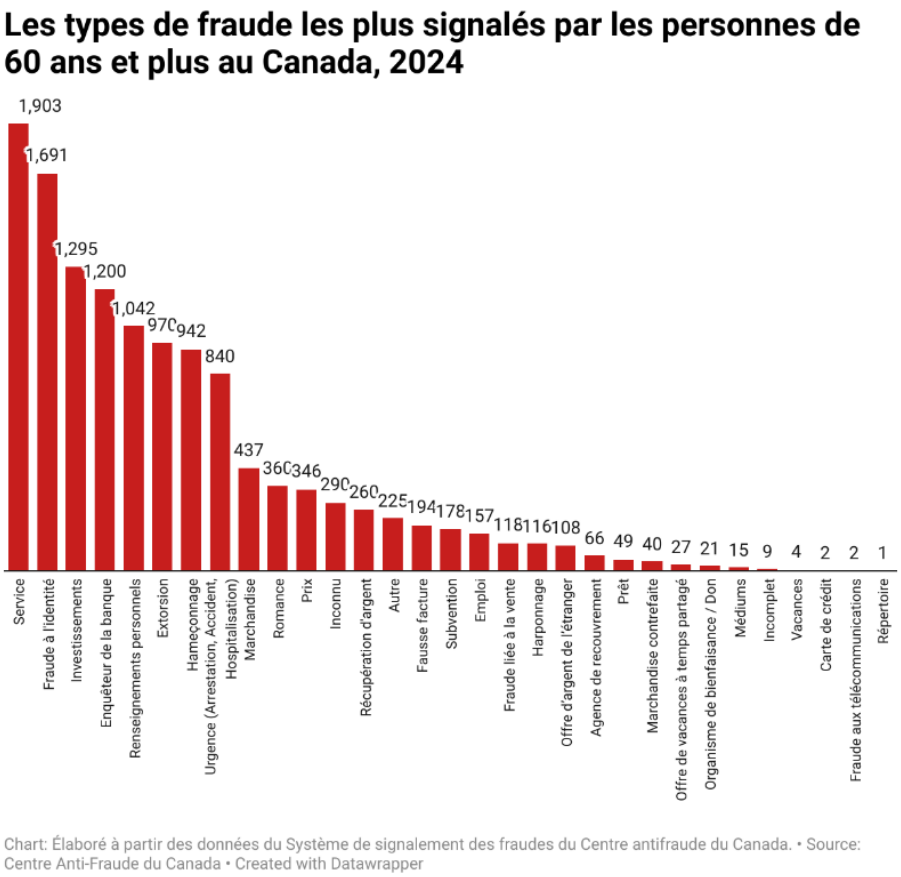
[42] Centre antifraude du Canada (CAFC), *Rapport annuel 2022*, 38.

signalements de fraudes visant cette tranche de la population est observée depuis 2022[43], la fraude demeure un problème récurrent pour les aînés[44].



Parmi les fraudes les plus signalées par les aînés figurent les fraudes de service (assurance, services financiers, assistance technique, télécommunications), les fraudes à l'identité (utilisation de renseignements personnels volés) et les fraudes d'investissement (sollicitations fausses ou trompeuses concernant des opportunités de placement offrant souvent un rendement supérieur à la normale)[45].

[43] Gouvernement du Canada, « Canadian Anti-Fraud Centre Fraud Data », Open Government Portal, 2024, https://open.canada.ca/data/en/dataset/6a09c998-cddb-4a22-beff-4dca67ab892f.
[44] David Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 13 ; Annie Lecompte, « The Scale of Fraud against Seniors Is Huge, and Still Growing — Here's Why », *The Conversation*, 28 octobre 2024, http://theconversation.com/the-scale-of-fraud-against-seniors-is-huge-and-still-growing-heres-why-240595 ; Cross, « "They're very lonely" », 61 ; Gabor et Kiedrowski, *Crime and Abuse Against Seniors*, section 4.1.
[45] Centre antifraude du Canada, « Scams by A-Z Index », 1 février 2023, https://antifraudcentre-centreantifraude.ca/scams-fraudes/azindex-eng.htm.



Enfin, les études internationales font, pour la plupart, le même constat : les personnes âgées sont souvent victimes de fraude, ce qui peut représenter un fardeau financier difficile à gérer pour elles et leurs proches[46].

3. Les causes et les conséquences de la fraude ciblant les aînés

Plusieurs hypothèses ont été proposées pour expliquer les raisons derrière la vulnérabilité des aînés à la fraude[47] :

---

[46] Steven Kemp et Nieves Erades Pérez, « Consumer fraud against older adults in digital society: Examining victimization and its impact », 1, 14-15; Parti, « "Elder Scam" Risk Profiles », 20; Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », 101; Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 14; Cross, « "They're very lonely" », 61-64.

[47] Financial Conduct Authority, *Finalised Guidance FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers*, February 2021, 15, https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf ; Huey et Ferguson, « What do we know about senior citizens as cybervictims? », 13-14; Sugunaraj, Ramchandra, et Ranganathan, « Cyber fraud economics, scam types, and potential measures to protect US seniors », 623; Rebovich et Corbo, « The distillation of national crime data into a plan for elderly

- Les aînés sont moins à l'aise avec la technologie ;
- Ils présentent un déclin cognitif et physique accru ;
- Ils sont souvent isolés ;
- Ils sont généralement polis et font confiance facilement ;
- Ils possèdent un capital important accumulé au fil des ans, notamment des fonds de retraite ;
- La retraite représente un bouleversement majeur dans leur vie, en termes de vulnérabilité financière et de perte du réseau professionnel ;
- Certains ont déjà été victimes de fraude, ce qui augmente les risques d'en être à nouveau victimes ;
- Certains ont tendance à prendre des risques ;
- Certains ont une confiance excessive en leurs connaissances financières.

Bien qu'il y ait encore des lacunes dans les recherches permettant de justifier le rapport de causalité entre chacun de ces facteurs et la fraude[48], ces hypothèses ne doivent pas être interprétées de manière isolée, mais plutôt comme faisant partie d'un phénomène multidimensionnel[49]. En effet, la vulnérabilité des aînés à la fraude serait influencée à la fois par des aspects cognitifs, psychologiques, contextuels et structurels.

Ainsi, au déclin cognitif (oublis, inattention, ralentissement, manque de pensée critique) s'ajoutent l'excès de confiance, la solitude, le deuil, le désir de contact social et le manque de littératie numérique. De plus, les aînés seraient particulièrement ciblés, étant perçus comme ayant des actifs et un patrimoine important accumulé au fil des ans. En l'absence de proches ayant la capacité de les avertir des risques, de lois protégeant les consommateurs contre la fraude ou de campagnes de sensibilisation sur ses dangers, tous ces facteurs convergeraient pour faciliter la fraude envers les aînés[50].

---

fraud prevention », 408, 416; Parti, « "Elder Scam" Risk Profiles », 22-23; Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 14; Cohen, « Consumer Fraud and the Elderly », 139.

[48] Kemp et Erades Pérez, « Consumer fraud against older adults in digital society », 14-15 ; Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », 101, 102, 104 ; Parti, « "Elder Scam" Risk Profiles », 28.

[49] Carter, *Digital Deception and the Aging Mind*, 1. L'Ombudsman des services bancaires et d'investissement (OSBI) du Canada déclarait que « Consumers are vulnerable or at higher risk of fraud, for example where: the consumer has no technology presence – i.e. no online banking profile, no computer, no email or other enabling technology ; the consumer is a senior ; the account is being controlled through a power of attorney ; the consumer is a previous fraud victim". Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 11 September 2024, 7, https://www.obsi.ca/media/dqdfevc2/obsi-response-to-finance-canada-consultation-on-strengthening-financial-sector-september-2024_en.pdf.

[50] Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », 102 ; Carter, *Digital Deception and the Aging Mind*, 1-6 ; Parti, « "Elder Scam" Risk Profiles », 23.

Quoi qu'il en soit, qu'il s'agisse de personnes aînées ou appartenant à d'autres tranches d'âge, une chose est certaine : les fraudeurs utilisent des méthodes hautement sophistiquées d'ingénierie sociale ou de piratage psychologique pour piéger leur cible[51]. Aussi connues sous le nom d'attaques de piratage humain, ces méthodes reposent sur des stratégies de manipulation et des « techniques psychologiques visant à susciter des réactions émotives et à exercer suffisamment de pression pour qu'une personne exécute une tâche », telle que fournir des informations personnelles ou envoyer de l'argent[52]. Ces techniques exploitent la peur, la confiance, le sentiment d'urgence ainsi que les aspirations légitimes à une vie exempte de soucis financiers.

En ce qui concerne les conséquences de la fraude, ses effets dépassent la simple perte monétaire et touchent à la fois l'individu et la société.

D'abord, les conséquences financières peuvent être catastrophiques pour la stabilité budgétaire des aînés et de leurs familles, telles que la perte de fonds de retraite, du patrimoine accumulé au fil des ans ou des épargnes mises de côté en cas d'urgence[53].

La fraude peut également entraîner de graves conséquences psychologiques et physiques[54]. Les victimes de fraude déclarent souvent ressentir de la colère, du stress, du regret, de la trahison, de la gêne, de la tristesse, de l'impuissance et de la honte[55]. Ces sentiments peuvent être amplifiés par le blâme et la culpabilisation dont elles font souvent l'objet (voir section 5)[56]. Qui plus est, parmi les effets observés figurent la dépression, les troubles anxieux, l'augmentation des douleurs ressenties, ainsi qu'un taux accru d'hospitalisation et une mortalité prématurée[57].

Ces conséquences peuvent être davantage pénibles pour les personnes aînées, notamment en ce qui concerne les effets physiques et

---

[51] Romance Fraud: The Linguistic Crime Scene with Dr Elisabeth Carter, 2025, https://www.youtube.com/watch?v=gbsP1_RplCk; Sugunaraj, Ramchandra, et Ranganathan, « Cyber fraud economics, scam types, and potential measures to protect US seniors », 624; FBI, « Elder Fraud Report », 18-19; Interpol, « Interpol Global Financial Fraud Assessment », 13; Rebovich et Corbo, « The distillation of national crime data into a plan for elderly fraud prevention », 413.

[52] Centre canadien pour la cybersécurité. *Piratage psychologique*. Octobre 2023, https://www.cyber.gc.ca/fr/orientation/piratage-psychologique-itsap00166#defn-piratage-psychologique.

[53] Huey et Ferguson, « What do we know about senior citizens as cybervictims? », 55; Jan Bailey et al., « Older adults and "scams" », 60, 62.

[54] Huey et Ferguson, « What do we know about senior citizens as cybervictims? », 15 ; Financial Conduct Authority, *Finalised Guidance FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers*, 13.

[55] Bailey et al., « Older adults and "scams" », 60, 62.

[56] Catherine Carpentier-Desjardins, « Le blâme et la responsabilisation des victimes de fraude » (Chaire de recherche en prévention de la cybercriminalité, 2025), https://www.prevention-cybercrime.ca/_files/ugd/9d4ef1_622ec9f1b17042c1a3dce5d6d5259587.pdf.

[57] Burnes et al., « Prevalence of Financial Fraud and Scams Among Older Adults in the United States », 13, 20.

psychologiques[58]. En plus d'avoir de la difficulté à se remettre de la perte financière, elles pourraient être perçues comme ayant des capacités cognitives diminuées et être privées de leur autonomie, ce qui entraînerait des conséquences telles que la perte de l'estime de soi[59].

Ensuite, il existe des effets sociétaux. La fraude mine les économies nationales et mondiales, affaiblit la confiance des consommateurs envers les industries utilisées par les fraudeurs[60], et remet en question l'intégrité des marchés financiers, des compagnies de télécommunications et des plateformes en ligne[61].

4. Blâmer la victime : la loi et les personnes fraudées au Canada

Après qu'une arnaque survient, l'auteur de la fraude est généralement difficile à retracer et l'argent détourné, quant à lui, s'évapore rapidement – d'autant plus qu'il s'agit d'un crime dont une forte proportion peut être transnationale[62]. Au niveau juridique, la question qui se pose alors est de déterminer qui doit assumer les pertes encourues en raison de la fraude. Est-ce le consommateur, l'institution financière ou, encore, une tierce partie, comme les entreprises de télécommunications ou les plateformes numériques ?

Comme nous le verrons, les victimes de fraude ne sont pas toutes égales devant la loi et, dans bien des cas, ce sont elles qui doivent assumer la perte. En raison d'une législation fragmentée qui ne s'attaque pas directement au problème, plusieurs victimes se retrouvent dépourvues de protection face au fléau de la fraude.

En effet, la protection dont bénéficie une personne victime de fraude varie selon que les transferts sont considérés comme « autorisés » ou « non autorisés », et selon le mode de paiement utilisé, qu'il s'agisse d'une carte de

---

[58] Kemp et Erades Pérez, « Consumer fraud against older adults in digital society », 7, 10-11 ; Bailey et al., « Older adults and "scams" », 60, 62.
[59] Bailey et al., « Older adults and "scams" », 60, 62.
[60] Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 10.
[61] Interpol, « Interpol Global Financial Fraud Assessment », 5. Rappelons que les principales infrastructures utilisées par les fraudeurs pour atteindre les consommateurs et leur soutirer de l'argent sont : les institutions financières comme les banques ; les compagnies de télécommunications, par la voie des appels ou des messages texte ; et les plateformes en ligne, comme les réseaux sociaux, à travers des publicités trompeuses. Australian Government, The Treasury, *Scams Prevention Framework: Protecting Australians from Scams*, janvier 2025, https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf.
[62] Interpol, « Interpol Global Financial Fraud Assessment », 2024, 10.

crédit ou d'un autre type de paiement[63]. Le cadre législatif couvre seulement les transactions « non autorisées » sur les cartes de crédit, tandis que ces mêmes transactions sur les cartes de débit sont couvertes uniquement par un code d'application volontaire[64].

Concernant spécifiquement les personnes âgées, le seul instrument de protection identifié se limite à un *Code de conduite pour la prestation de services bancaires aux aînés* — un code volontaire adopté par des institutions financières — lequel énonce des principes très généraux visant à les protéger en cas de fraude : « Les banques s'efforceront d'atténuer les préjudices financiers potentiels pour les aînés… Lorsque les banques prennent connaissance de la possibilité qu'un aîné ait subi un préjudice financier en raison d'exploitation financière, de fraude ou d'escroquerie, elles s'efforceront d'atténuer les risques de préjudice financier, tout en respectant la vie privée du client, sa sécurité et son autonomie »[65].

4.1. La transaction « non autorisée »

En règle générale, dans le cas où le consommateur n'a aucunement « autorisé » une transaction frauduleuse, c'est l'institution financière qui doit en assumer les pertes.

Une transaction « non autorisée » se produit lorsque le malfaiteur accède au compte de sa victime pour y effectuer des transactions à son insu, sans que la victime n'ait fait une quelconque action pour effectuer ces paiements[66]. C'est le cas, par exemple, d'un consommateur qui, en vérifiant un jour son compte, découvre des transferts dont il ne connaît ni la raison ni le destinataire, ou constate que sa carte a été volée[67].

Plusieurs juridictions canadiennes ont adopté des lois qui offrent expressément une protection à l'égard des transactions non autorisées sur la carte de crédit. Au Québec, la *Loi sur la protection du consommateur* prévoit ainsi que « la responsabilité du consommateur dont la carte [de crédit] a été utilisée sans son autorisation est limitée à la somme de 50 $ », sauf si l'institution financière « établit que le consommateur a commis une faute

---

[63] Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 3.
[64] Ibid., 10.
[65] Association des banquiers canadiens, « Code de conduite pour la prestation de services bancaires aux aînés », 2019, 4.
[66] Carpentier-Desjardins, « Le blâme et la responsabilisation des victimes de fraude ».
[67] Financial Consumer Agency of Canada, « Resolving an Unauthorized Transaction », *Education and Awareness*, 24 janvier 2018, https://www.canada.ca/en/financial-consumer-agency/services/resolving-unauthorized-transaction.html.

lourde[68] dans la protection de son numéro d'identification personnel »[69]. Des dispositions similaires se trouvent dans les lois sur la protection du consommateur de l'Alberta, de la Colombie-Britannique, du Manitoba, de l'Ontario et de Terre-Neuve-et-Labrador[70]. Au niveau fédéral, la *Loi sur les banques* énonce aussi une protection similaire, sauf si le consommateur a fait preuve de négligence grave ou, au Québec, a commis une faute lourde[71]. Cette même loi précise que l'utilisation d'identifiants personnels, par exemple un mot de passe ou un NIP, dans le cadre de l'utilisation non autorisée de la carte de crédit « ne constitue pas en soi une négligence grave »[72].

En résumé, à l'heure actuelle, seules les transactions « non autorisées » sur la carte de crédit font l'objet d'une protection et d'un remboursement prévus par la loi. Pour les autres modes de paiement, tels que la carte de débit ou les virements en ligne, aucune disposition de la loi n'offre expressément une protection aux consommateurs contre les transactions non autorisées. Au niveau fédéral, des codes volontaires et des principes adoptés par les institutions financières offrent toutefois certaines protections :

- Le *Code de pratique canadien des services de cartes de débit* stipule la même protection en cas d'opération non autorisée sur la carte de débit, et étend même le caractère non autorisé à certains cas où une personne a été victime de supercherie. Par exemple, l'Annexe A de ce code précise que « le titulaire d'une carte n'est pas considéré comme ayant divulgué "volontairement" le NIP, si le NIP a été obtenu par contrainte, supercherie, force ou intimidation[73] ».
- Les *Principes régissant la protection des consommateurs dans le commerce électronique : le cadre canadien* précisent que « les consommateurs ne devraient pas être tenus responsables des sommes qui leur sont facturées pour des "transactions non autorisées". Les

[68] Rappelons que le *Code civil du Québec* précise que « la faute lourde est celle qui dénote une insouciance, une imprudence ou une négligence grossières ». *Code civil du Québec*, art. 1474.
[69] *Loi sur la protection du consommateur*, RLRQ c P-40.1, art. 123 et 123.1.
[70] *Consumer Protection Act*, RSA 2000, c C-26.3, art. 88(1), 89, en ligne : CanLII https://canlii.ca/t/56fwd (consulté le 14 mai 2025) ; *Business Practices and Consumer Protection Act*, SBC 2004, c 2, art. 98–99, en ligne : CanLII https://canlii.ca/t/56gwl (consulté le 14 mai 2025) ; *Consumer Protection Act*, CCSM c C200, art. 35.2, 35.8, en ligne : CanLII https://canlii.ca/t/55gf2 (consulté le 14 mai 2025) ; *Consumer Protection Act*, 2023, SO 2023, c 23, Sch 1, art. 29, en ligne : CanLII https://canlii.ca/t/56564 (consulté le 14 mai 2025) ; *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1, art. 73–74, en ligne : https://assembly.nl.ca/legislation/sr/statutes/c31-1.htm (consulté le 14 mai 2025).
[71] *Loi sur les banques*, LC 1991, c 46, art. 627.33. « Est de 50 $ la somme maximale pour laquelle l'emprunteur peut être tenu responsable advenant l'utilisation non autorisée de la carte de crédit qui lui a été émise au Canada… ».
[72] Ibid.
[73] *Code de pratique canadien des services de cartes de débit*, article 10, clause 5; ANNEXE A, Guide d'interprétation de la section 5, clause (5).

commerçants devraient rembourser rapidement aux consommateurs les montants versés lors de transactions non autorisées[74] ».

Cependant, il s'agit là de codes volontaires, appliqués seulement par les entités signataires, et les décisions des tribunaux québécois en matière de fraude ont fait peu de références à ces instruments.

En l'absence de lois attribuant la responsabilité à la banque, ce sont les règles générales de la responsabilité civile qui permettront de déterminer qui doit supporter la perte résultante de la transaction non autorisée. Il s'agira donc, au cas par cas, d'analyser les circonstances de la fraude et de déterminer si la faute peut être attribuée au consommateur. Bien que la protection pour les transactions non autorisées sur la carte de débit soit moins claire et laisse place à plus d'interprétation, les victimes pourront généralement se faire rembourser si cette analyse ne révèle pas de manquements à leurs obligations de sécurité.

Dans cette analyse, on tiendra particulièrement compte des clauses du contrat entre le consommateur et son institution financière[75]. Souvent, ce contrat exige du consommateur non seulement d'informer l'institution financière de la fraude dans les plus brefs délais, mais aussi de respecter une multitude d'obligations liées à la protection de son NIP, qu'il ne doit pas divulguer sous aucun prétexte. Ce contrat peut aussi imposer des obligations en matière de sécurité informatique, comme l'utilisation de logiciels antivirus, de pare-feu et de logiciels anti-espions[76]. Cela dit, le contenu du contrat bancaire pourrait être contesté en certaines circonstances. Par exemple, le contrat bancaire ne pourrait pas contenir une clause imputant toute la responsabilité au consommateur en l'absence de faute de sa part, parce qu'une telle clause serait abusive, considérant qu'il s'agit d'un contrat d'adhésion que le consommateur ne peut pas librement renégocier[77].

Finalement, soulignons que la protection légale contre l'utilisation non autorisée pourrait cesser d'être cantonnée uniquement à la carte de crédit

---

[74] Groupe de travail sur la consommation et le commerce électronique, « Principes régissant la protection des consommateurs dans le commerce électronique : le cadre canadien », 1999, p. 9. Par ailleurs, la définition de « transaction non autorisée » présente une certaine ambiguïté, laissant penser que toute opération résultant d'une fraude serait « non autorisée » : « une transaction non autorisée par le consommateur résultant d'un vol, d'une fraude ou d'une erreur du commerçant » (p. 11).
[75] Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 3 ; Option consommateurs, *Commentaires présentés à la Commission des institutions, Projet de loi n˚ 72 – Loi protégeant les consommateurs contre les pratiques commerciales abusives et offrant une meilleure transparence en matière de prix et de crédit*, 2 octobre 2024, 4 https://s3.ca-central-1.amazonaws.com/option-consommateurs-assets/production/Revendications/option-consommateurs-pl72-memoire.pdf
[76] Option consommateurs, 4. Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 11.
[77] *Code civil du Québec*, art. 1437.

prochainement au Québec. En novembre 2024, le Québec a sanctionné un projet de loi modifiant la *Loi sur la protection du consommateur* pour étendre la protection légale en cas de transfert « non autorisé » à d'autres modes de paiement que la seule carte de crédit[78]. Ainsi, sauf en cas de faute lourde, la responsabilité du consommateur se limiterait à 50 $: « Le commerçant auprès duquel le consommateur détient un compte de dépôt à vue doit lui rembourser, dans le délai prévu par règlement, toute somme débitée de ce compte sans son autorisation ou celle d'une personne autorisée à y effectuer des opérations (…) Avant qu'il n'ait été avisé par le consommateur… de la fraude… le commerçant n'est tenu de rembourser l'ensemble des sommes ainsi débitées qu'en ce qu'il excède 50 $ »[79]. Cependant, cette modification n'a pas encore de date d'entrée en vigueur.

4.2. La transaction « autorisée »

En règle générale, lorsque le consommateur a lui-même « autorisé » le transfert frauduleux, c'est à lui d'assumer les pertes, en l'absence de lois encadrant ce type de fraude.

Une transaction « autorisée » survient lorsque les fraudeurs manipulent les victimes pour qu'elles effectuent des paiements vers des comptes qu'ils contrôlent, en utilisant des techniques de tromperie sophistiquées[80]. Bien évidemment, cette autorisation ne repose pas sur un consentement éclairé[81], car les victimes sont induites en erreur et amenées à croire que la transaction est légitime, souvent par le biais de techniques d'ingénierie sociale ou de manipulation psychologique comme l'usurpation d'identité, la création d'un sentiment d'urgence ou l'invocation d'une fausse autorité[82].

De cette manière, soit la victime envoie l'argent à un destinataire différent de celui qu'elle pensait, soit l'objet de la transaction n'est pas légitime,

---

[78] *Loi protégeant les consommateurs contre les pratiques commerciales abusives et offrant une meilleure transparence en matière de prix et de crédit*, PL 72 (2024, c 32), art. 12. Le nouvel article 65.1. de la *Loi sur la protection du consommateur* stipule : « Aux fins de la présente sous-section, "instrument de paiement" comprend une carte de débit ainsi que tout instrument de paiement électronique permettant au consommateur d'accéder à son compte de dépôt à vue, y compris par un appareil électronique, notamment un téléphone cellulaire, une tablette électronique ou un ordinateur, dans le but d'initier un ordre de paiement ».

[79] *Loi sur la protection du consommateur*, art. 65.1, telle que modifiée par le projet de loi 72, 2024.

[80] Australian Government The Treasury, « Scams Prevention Framework Summary of Reforms », septembre 2024, 6, https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf.

[81] Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 12-13.

[82] Chen Yang, « Protecting Financial Consumers from Authorized Push Payment Fraud: Is Reimbursement an Optimal Solution? », *Journal of Financial Regulation and Compliance*, ahead-of-print, no ahead-of-print: 2, consulté le 15 mai 2025, https://www.emerald.com/insight/content/doi/10.1108/jfrc-11-2024-0225/full/html.

contrairement à ce qu'elle croyait (un retour financier, l'amour de sa vie, ou des biens et services)[83]. C'est le cas, par exemple, de la fraude à l'investissement, où un consommateur autorise un paiement en croyant faire affaire avec une entreprise légale ou de la fraude amoureuse, où la victime envoie « volontairement » de l'argent à une personne qu'elle considère comme son amoureuse.

Aucune loi au Canada ne protège les victimes de fraude ayant « autorisé » une transaction. Encore ici, la donne pourrait changer prochainement au Québec en raison de l'adoption récente d'un projet de loi modifiant la *Loi sur la protection du consommateur*, qui offre certaines protections en cas de transfert « autorisé »[84] :

> « Le commerçant auprès duquel le consommateur détient un compte de dépôt à vue doit lui rembourser, dans le délai prévu par règlement, toute somme débitée avec son autorisation, ou avec celle d'une personne autorisée à y effectuer des opérations, dans le cas où il est victime d'une fraude.
>
> Le consommateur est tenu des pertes subies par le commerçant lorsque ce dernier établit qu'il a débité cette somme, soit en l'absence d'indices probants permettant de soupçonner la fraude, soit, en présence de tels indices, après avoir pris les précautions nécessaires pour tenter de la prévenir »[85].

Cette modification n'a pas encore de date d'entrée en vigueur. Bien qu'il s'agisse d'une avancée positive, en ce qu'elle reconnaît le besoin de protection des victimes ayant « autorisé » la transaction frauduleuse et fait porter le fardeau de la preuve sur l'institution financière, quelques doutes planent quant à son interprétation et à sa portée.

En effet, l'exclusion de protection « en l'absence d'indices probants permettant de soupçonner la fraude » pourrait laisser plusieurs consommateurs sans remboursement. La littérature souligne que l'ingénierie sociale inclut des méthodes permettant de contourner les contrôles antifraude, où les criminels indiquent aux victimes exactement quoi répondre aux questions de la banque afin de réduire les soupçons et d'outrepasser les mesures de sécurité[86]. De plus, la loi ne tient pas compte des personnes qui, en raison de leur

---

[83] Ibid., 2.
[84] *Loi protégeant les consommateurs contre les pratiques commerciales abusives et offrant une meilleure transparence en matière de prix et de crédit*, PL 72 (2024, c 32), art. 12.
[85] Ibid., art. 65.1.
[86] Jo Braithwaite, « 'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like? », *Journal of Financial Regulation* 10, no 2 (16 septembre 2024) : 185, https://doi.org/10.1093/jfr/fjae006 ; Romance Fraud: The Linguistic Crime Scene with Dr Elisabeth Carter, 2025, https://www.youtube.com/watch?v=gbsP1_RplCk.

vulnérabilité (voir section 5.2) et de la complexité de la fraude dont elles sont victimes, pourraient insister pour faire la transaction et ne pas faire attention aux précautions prises par la banque pour tenter de la prévenir[87].

Le degré de protection des consommateurs en vertu des nouvelles dispositions québécoises dépendra donc de la manière dont la fraude est classifiée, selon qu'elle résulte d'une transaction « autorisée » ou « non autorisée ». Deux exemples permettent d'illustrer le problème. Dans le premier, un consommateur reçoit un appel d'un faux représentant de sa banque, qui parvient à lui soutirer des renseignements permettant de déclencher un transfert d'argent. Le consommateur n'a ni demandé ni accepté de réaliser la transaction, mais, sans le savoir, il a partagé des informations permettant au fraudeur de l'effectuer. Dans un autre cas, le consommateur, sous l'effet d'une manipulation, accepte de transférer des fonds de sa marge de crédit vers son compte de débit personnel, mais le fraudeur redirige ensuite l'argent vers un compte différent. Dans ces situations, s'agit-il de transactions « non autorisées » ou « autorisées » ? La réponse à cette question déterminera dans quelle mesure la loi protège la victime de fraude. Si la transaction est considérée comme « non autorisée », elle pourra généralement se faire rembourser (voir section 4.1.). Mais si elle est considérée comme « autorisée », sa protection sera tributaire de l'existence d'indices probants permettant de soupçonner la fraude, lesquels auraient permis à l'institution financière d'agir.

Quoi qu'il en soit, à l'heure actuelle, il n'existe pas d'encadrement spécifique pour ce type de fraude résultant d'une transaction « autorisée » au Canada. Encore une fois, en l'absence de lois attribuant la responsabilité à la banque, ce sont les règles générales de la responsabilité civile, et particulièrement les clauses du contrat, qui permettront de définir le partage des responsabilités en cas de fraude, ce que les juges analysent au cas par cas. Or, contrairement aux cas de transactions non autorisées, les institutions financières vont généralement considérer le consommateur responsable de ces types de fraude et refuser de l'indemniser. Il est typique, par exemple, que la banque refuse d'indemniser le consommateur en invoquant les clauses contractuelles lui interdisant de divulguer un code de sécurité reçu par texto.

Ceci dit, les banques doivent faire preuve d'un certain degré de diligence, même à l'égard des transactions dites « autorisées ». Par exemple, quelques décisions ont été rendues concernant la responsabilité des banques en cas de fraude. Dans une affaire concernant un transfert frauduleux « autorisé », la

---

[87] Payment Systems Regulator, *Guidance: Authorised Push Payment Fraud Reimbursement – The Consumer Standard of Caution Exception Guidance*, décembre 2023, https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf.

Cour supérieure du Québec a conclu que : « *The banking contract implies a duty to act with reasonable prudence and diligence… Despite the principle of non-interference, banks are required to exercise a certain degree of care to protect their clients from fraud, especially in the face of suspicious activity* »[88]. Qui plus est, le même texte cite une autre décision de la Cour d'appel du Québec : « *When one of its customers undertakes transactions that the reasonable banker in the circumstances would consider to be suspicious, the bank must take appropriate measures.* (…) *Failure to take such measures, such as suspending a transaction while its correctness is verified, may result in liability to those who suffer a loss as a result* »[89]. En somme, les banques doivent trouver un équilibre entre le principe de non-ingérence, non-immixtion ou neutralité à l'égard du compte du client, et le principe de non-indifférence ainsi que la diligence raisonnable à l'égard d'opérations suspectes et irrégulières dans un compte bancaire, notamment en contexte de fraude.

En conséquence, comme on le constate, au niveau législatif, un grand pourcentage de fraudes, notamment les plus onéreuses, telles que la fraude à l'investissement ou la fraude amoureuse, échappent à toute protection légale lorsqu'il s'agit d'opérations « autorisées » par la victime.

4.3. Les intermédiaires en ligne

La responsabilité des entreprises de télécommunication et des plateformes en ligne en cas de fraude est un débat ouvert[90]. Bien que plusieurs personnes soient victimes de fraude à la suite d'un appel, d'un message texte ou après avoir cliqué sur une publicité trompeuse affichée sur les réseaux sociaux, le degré de responsabilité des entreprises offrant ces services est difficile à déterminer, celles-ci étant considérées par la loi comme de simples intermédiaires.

En principe, en vertu de la *Loi concernant le cadre juridique des technologies de l'information*, des intermédiaires tels que des plateformes en ligne ou des

[88] *Alfagomma Inc. c. HSBC Bank Canada*, 2022 QCCS 3655, 84–85.
[89] *Alfagomma Inc. c. HSBC Bank Canada*, 2022 QCCS 3655, 86. D'autres décisions rendues dans d'autres provinces canadiennes vont dans le même sens quant à la responsabilité des banques en cas de fraude. En Colombie-Britannique, une décision a conclu : « *A bank owes a duty of care to its customers, including a duty to inquire in the face of the bank's knowledge of a potential fraud* ». *Zheng v. Bank of China (Canada) Vancouver Richmond Branch*, 2023 BCCA 43, 39.
[90] Pour une compréhension détaillée des complexités liées à l'encadrement des technologies de l'information, voir Vincent Gautrais, Pierre Trudel et Nicolas Vermeys, *LCCJTI+ : perspectives de mise à jour de la Loi concernant le cadre juridique des technologies de l'information (RLRQ c C-1.1), 2001–2023, Rapport final – 28 novembre 2023* (Montréal : Centre de recherche en droit public, 2023), 2, 10–12, https://www.crdp.umontreal.ca/files/sites/101/2024/02/Rapport-final.pdf.

services de télécommunications ne sont pas responsables des activités illicites qui se déroulent par l'entremise de leurs services :

> « Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci. (…) De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services »[91].

De plus, un tel intermédiaire « n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite »[92]. Il n'a donc pas d'obligation de faire une surveillance des activités qui se déroulent par son entremise.

Cela dit, le fournisseur de ces services pourrait devenir imputable s'il a connaissance d'activités illicites effectuées par ses utilisateurs et qu'il ne fait rien pour les empêcher :

> « il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité »[93].

Dans ce sens, deux actions collectives ont été initiées en 2023 et 2024 au Québec visant la plateforme Facebook, sur la base que celle-ci diffuse des publicités trompeuses liées à des investissements frauduleux[94] et que des images manipulées de célébrités sont utilisées pour les promouvoir[95]. Ces affaires cherchent à établir la responsabilité de Facebook dans de nombreux cas de fraude et, le cas échéant, à obtenir un dédommagement du géant du web[96].

---

[91] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, art. 22.
[92] Ibid., art. 27.
[93] Ibid., art. 22.
[94] *Johanne Gauthier et Fernand Larouche c. Facebook Canada Ltd et Meta Platforms – Facebook inc.*, Cour supérieure du Québec, district de Montréal, no 500-06-001236-237.
[95] *Marie-Claude Barrette et John Viens v. Facebook Canada Ltd. et Meta Platforms, Inc.*, Cour supérieure du Québec, district de Montréal, no 500-06-001299-243.
[96] L'action collective de 2023 a passé le stade de l'autorisation en 2025. Voir : *Gauthier* c. *Facebook Canada Ltd.*, 2025 QCCS 1794 (CanLII).

Ces actions collectives soutiennent que Facebook agit en tant que « publicitaire » au sens de la *Loi sur la protection du consommateur*. En diffusant des publicités trompeuses, cette plateforme numérique contreviendrait aux articles 215 et suivants de cette loi, dont l'article 219 : « Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur »[97]. L'action collective de 2023 invoque également la *Loi sur la concurrence*, notamment l'interdiction des indications fausses ou trompeuses[98].

Quoi qu'il en soit, Facebook invoquait l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI) pour se présenter comme un simple intermédiaire en ligne et s'exonérer de toute responsabilité à l'égard des fraudes commises sur sa plateforme[99]. Le grand défi pour les demandeurs dans ces actions collectives sera d'écarter l'application de la LCCJTI, ou de démontrer que Facebook avait connaissance des contenus illicites diffusés sur sa plateforme.

Le constat général est que les consommateurs restent, une fois de plus, dépourvus de protection en cas de fraude à l'égard des compagnies de télécommunication et des plateformes en ligne, perçues par la loi comme de simples intermédiaires. Aucune loi n'impose de devoirs spécifiques à ces plateformes, par exemple pour exiger qu'elles vérifient les publicités qu'elles diffusent.

4.4. Le parcours du combattant

En vertu de la *Loi sur les banques*, les institutions financières doivent se doter d'une procédure interne d'examen des plaintes[100]. Ainsi, un consommateur victime de fraude qui se voit refuser le remboursement doit pouvoir porter officiellement plainte à la banque. De même, la banque doit communiquer à ses clients et au public « le nom de l'organisme externe de traitement des plaintes et la manière dont on peut communiquer avec celui-ci »[101].

Lorsque la victime n'a pas réussi à régler l'affaire par les canaux offerts par l'institution financière, elle peut donc envisager de contacter cet organisme externe, l'Ombudsman des services bancaires et d'investissement (OSBI). Cet

---

[97] *Loi sur la protection du consommateur*, art. 219.
[98] *Johanne Gauthier et Fernand Larouche c. Facebook Canada Ltd et Meta Platforms – Facebook inc.*, Cour supérieure du Québec, district de Montréal, no 500-06-001236-237.
[99] Zone Société – ICI.Radio-Canada.ca, « Fraude à la crypto : une action collective contre Facebook autorisée », *Radio-Canada*, 3 juin 2025.
[100] *Loi sur les banques*, LC 1991, c 46, art. 627.45.
[101] Ibid.

organisme ne peut formuler que des recommandations[102] pour régler des différends jusqu'à un montant de 350 000 $[103]. Ses décisions ne sont donc pas exécutoires et la banque peut refuser de les appliquer. De plus, selon un reportage de 2024, « en matière de fraude bancaire, les décisions de l'OSBI sont souvent défavorables au client. En 2023 seulement 17 % des gens qui ont porté plainte ont obtenu un remboursement ou un règlement »[104].

Reconnaissant ses limitations et le manque d'encadrement particulièrement des transferts autorisés en contexte de fraude, l'OSBI déclarait :

> « In 2023 approximately one in five fraud cases resulted in a settlement or recommendation for compensation to the consumer. In most cases we are not able to recommend compensation because we have no legal or regulatory basis to do so. Sharing confidential banking information, intentionally or unintentionally, is a breach of the agreement that consumers make when opening a bank account, leaving them liable for their losses in most fraud cases. Banks have limited obligations to protect their customers from these crimes »[105].

Au Québec, les victimes peuvent également se tourner vers l'Autorité des marchés financiers (AMF), l'organisme responsable de l'encadrement du secteur financier de la province, à l'exception des banques. Dans certaines circonstances — notamment si la fraude a été commise par une entreprise détenant ou ayant détenu un droit d'exercice délivré par l'AMF —, « un consommateur peut être indemnisé pour un montant maximal de 200 000 $ par réclamation » par l'intermédiaire du Fonds d'indemnisation des services financiers[106]. Bien évidemment, comme la plupart des fraudes sont commises par des personnes ou entreprises ne détenant pas un droit d'exercice auprès de l'AMF, ces cas ne sont pas couverts par le fonds d'indemnisation.

Comme on a pu le constater, il n'existe pas au Canada de lois obligeant les banques à assumer la responsabilité en cas de fraude où le consommateur a « autorisé » le transfert d'argent. Autrement dit, dans la plupart de ces cas, c'est le consommateur qui devra subir les pertes liées à la fraude ou engager

---

[102] Ibid., art. 627.49.
[103] OSBI, « Ce que nous faisons », *Ombudsman des services bancaires et d'investissement*, consulté le 9 mai 2025, https://www.obsi.ca/fr/a-propos-de-nous/ce-que-nous-faisons/.
[104] Radio-Canada, « Fraudés et laissés pour compte par leurs banques », *La facture*, 29 octobre 2024, https://ici.radio-canada.ca/tele/la-facture/site/segments/reportage/1892186/fraude-banque-virement-responsabilite-protection-ombudsman.
[105] Ombudsman for Banking Services and Investments, *Response to Request for Comments on Proposals to Strengthen Canada's Financial Sector*, 2.
[106] L'Autorité des marchés financiers, « Fonds d'indemnisation des services financiers », consulté le 12 mai 2025, https://lautorite.qc.ca/grand-public/indemnisation-et-protection-des-depots/reclamer-au-fonds-dindemnisation-des-services-financiers.

une procédure judiciaire pour tenter de récupérer son argent[107]. Ces démarches peuvent être longues et d'autant plus pénibles pour les personnes vulnérables, comme les aînés présentant des signes de déclin cognitif et physique.

Enfin, bien que limitées, les victimes disposent également d'autres ressources vers lesquelles se tourner en cas de fraude.

Les services de police et le Centre antifraude du Canada offrent la possibilité de signaler un cas de fraude et de bénéficier d'un accompagnement. Le Service de police de la Ville de Montréal propose aussi un service de soutien aux victimes par le biais de rencontres de groupe[108]. Pour sa part, le Centre antifraude du Canada dispose d'une « Senior Support Unit » où les personnes aînées victimes de fraude peuvent communiquer avec des bénévoles[109]. Finalement, au Québec, les victimes de fraude peuvent être accompagnées, soutenues ou référées à d'autres ressources grâce à deux organismes mis à leur disposition : le Centre d'aide aux victimes d'actes criminels et la ligne Aide Maltraitance Adultes Aînés[110].

Quoi qu'il en soit, un problème majeur demeure : seules les victimes considérées comme n'ayant pas « autorisé » la transaction ont droit à un remboursement. Cela laisse planer un sentiment d'injustice et soulève une question légitime : pourquoi certaines victimes mériteraient-elles d'être remboursées, tandis que d'autres ne le mériteraient pas ? Enfin, cette politique inéquitable de remboursement donne l'impression que les victimes sont systématiquement blâmées : en plus d'avoir été fraudées, les banques leur annoncent qu'elles ne seront pas remboursées, car leur victimisation serait de leur faute[111].

---

[107] Radio-Canada, « Fraudés et laissés pour compte par leurs banques », *La facture*, 29 octobre 2024, https://ici.radio-canada.ca/tele/la-facture/site/segments/reportage/1892186/fraude-banque-virement-responsabilite-protection-ombudsman ; Isabelle Richer, « 220 clients de la Banque Royale victimes de fraude : l'institution refuse de les rembourser », *Ici Radio-Canada Info*, vidéo, 2 juin 2025, https://ici.radio-canada.ca/info/videos/1-10395057/220-clients-banque-royale-victimes-fraude-institution-refuse-rembourser.

[108] Ariane Krol, « Dossier: Des fraudes amoureuses qui tournent à la tragédie », *La Presse*, 11 avril 2025, sect. Justice et faits divers, https://www.lapresse.ca/actualites/justice-et-faits-divers/des-fraudes-amoureuses-qui-tournent-a-la-tragedie/2025-04-11/programme-d-aide-du-spvm/apres-l-enfer-de-la-relation.php.

[109] *Aging Vibrantly*, « Putting a Stop to Frauds and Scams Targeting Seniors », 62, consulté le 9 mai 2025, https://open.spotify.com/episode/1OjKQfsNj2TRJcsfWpFbKu; Cross, « "They're very lonely" ».

[110] Centres d'aide aux victimes d'actes criminels (CAVAC), « Qui sommes-nous? », consulté le 12 mai 2025, https://cavac.qc.ca/a-propos-du-cavac/qui-sommes-nous/; « Ligne Aide Maltraitance Adultes Aînés », consulté le 12 mai 2025, https://lignemaltraitance.ca/fr.

[111] Radio-Canada, « Fraudés et laissés pour compte par leurs banques », *La facture*, 29 octobre 2024, https://ici.radio-canada.ca/tele/la-facture/site/segments/reportage/1892186/fraude-banque-virement-responsabilite-protection-ombudsman.

5. La protection des victimes à l'étranger

Le Canada n'est pas le seul pays à subir une vague grandissante de fraude[112]. Certains pays ont récemment adopté des lois visant soit à prévenir la fraude, soit à protéger les personnes qui en ont été victimes. Parmi les juridictions qui ont attiré notre attention en raison de la robustesse de leur législation, de leur poids économique et de leur similitude avec le Canada figurent l'Australie, le Royaume-Uni et l'Union européenne.

Un trait commun aux législations de l'Australie et du Royaume-Uni est qu'elles cherchent à s'attaquer explicitement à la fraude « autorisée », et non uniquement aux fraudes « non autorisées ». Cela est tout à fait logique, car, comme au Canada, les transferts non autorisés faisaient déjà l'objet d'une protection et permettaient le remboursement du consommateur[113]. En Australie, la fraude autorisée est désignée par le terme « scam »[114], et au Royaume-Uni, par l'expression « Authorized Push Payment (APP) »[115].

Également, les deux pays ont mis en place, ou sont en train de mettre en place, des mesures techniques de lutte contre la fraude, comme le protocole « Confirmation of Payee » (CoP). Ce protocole permet d'identifier le nom associé à un compte à l'aide des données bancaires, de sorte que le nom fourni par le payeur et celui du bénéficiaire doivent correspondre. Il s'agit d'une méthode efficace pour détecter les escroqueries par redirection (les fraudeurs incitent la personne à envoyer de l'argent, à son insu, sur un compte bancaire différent de celui qui lui avait été annoncé[116]), mais elle n'est pas utile dans les cas où un fraudeur a fourni un nom de compte et des coordonnées bancaires correspondantes[117]. Au Canada, Paiements Canada, l'organisme de règlement des paiements, envisage d'adopter un tel protocole dans le cadre du nouveau système de paiement en temps réel[118].

---

[112] Interpol, « Interpol Global Financial Fraud Assessment », 2024.
[113] Jo Braithwaite, « 'Authorized Push Payment' Bank Fraud », 179 ; ARAG Law, « Your Right to a Refund for an Unauthorised Payment », consulté le 6 juin 2025, https://www.araglaw.co.uk/blog/your-right-to-a-refund-for-an-unauthorised-payment/ ; Financial Rights Legal Centre, « Reversing Bank Transactions », 1 novembre 2022, https://financialrights.org.au/factsheet/reversing-bank-transactions/.
[114] Australian Government, The Treasury, *Scams Prevention Framework: Protecting Australians from Scams*.
[115] Payment Systems Regulator, *Consolidated Policy Statement: APP Scams Reimbursement Requirement*, mai 2025, https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf.
[116] Nedbank Private Wealth, « What Is a Payment Redirection Scam? », consulté le 23 juin 2025, https://nedbankprivatewealth.com/what-is-a-payment-redirection-scam/.
[117] Braithwaite, « 'Authorized Push Payment' Bank Fraud », 181; Brendan Alder, « New Confirmation of Payee Service Hits Important Milestone », *Australian Banking Association* (blog), 8 août 2024, https://www.ausbanking.org.au/new-confirmation-of-payee-service-hits-important-milestone/.
[118] Paiements Canada, *Cadre des politiques du nouveau système de paiement en temps réel du Canada : Document de consultation sur le système de paiement en temps réel*, 2025, https://www.paiements.ca/sites/default/files/PaymentsCanada_Real-

Ce qui différencie les deux pays, c'est que l'Australie privilégie une approche préventive de responsabilisation des différents acteurs dont l'infrastructure est utilisée par les fraudeurs (institutions financières, entreprises de télécommunications, plateformes numériques) (section 5.1), tandis que le Royaume-Uni met l'accent sur le remboursement des victimes, en particulier des personnes les plus vulnérables (section 5.2)[119].

Enfin, l'Union européenne a légiféré pour encadrer les services numériques comme les plateformes en ligne (section 5.3). Entre autres, son objectif était de lutter « contre la diffusion de contenus illicites en ligne et contre les risques pour la société que la diffusion d'informations trompeuses ou d'autres contenus peuvent produire »[120]. Cela inclut, bien évidemment, le contenu frauduleux. Bien qu'en principe cette législation ne diffère guère de la *Loi concernant le cadre juridique des technologies de l'information* du Québec en ce qui touche la non-responsabilité des intermédiaires en ligne (section 4.3), quelques stipulations vont plus loin pour prévenir l'affichage de tout contenu illicite sur ces plateformes.

5.1. L'Australie

L'approche de l'Australie consiste à formuler une vision d'ensemble de l'écosystème de la fraude, avec des obligations robustes en matière d'application de la loi, assorties de sanctions en cas de non-respect[121]. En effet, les entreprises de secteurs comme les banques, les télécommunications et les plateformes numériques qui ne respectent pas leurs obligations s'exposent à des amendes pouvant atteindre 50 millions de dollars[122].

Parmi les mesures adoptées figure la création du National Anti-Scam Centre, en juillet 2023, dont l'objectif est de centraliser les données sur la fraude et de faciliter le partage d'informations entre les régulateurs, les forces de l'ordre et

---

TimeRail_ConsultationDocument_Fr.pdf; Payments Canada, « Overseeing a World-Class Payment System », consulté le 10 juin 2025, https://www.payments.ca/overseeing-world-class-payment-system ; Vivek Mehta, « Canada Must Combat Payments Fraud through a Confirmation of Payee (CoP) Solution », *Vm's Notepad* (blog), 15 avril 2024, https://medium.com/vms-notepad/canada-must-combat-payments-fraud-through-a-confirmation-of-payee-cop-solution-0c381ecb16c3.

[119] Catherine Carpentier-Desjardins, « Responsabilités en matière de fraude bancaire. Étude de cas du Royaume-Uni et de l'Australie » (Chaire de recherche en prévention de la cybercriminalité, 2024), https://www.prevention-cybercrime.ca/_files/ugd/9d4ef1_cdf8c649d93f4b50b6989b2a7241d7a5.pdf.

[120] Union européenne, *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 (règlement sur les services numériques)*, considérant 9.

[121] The Treasury, « Scams Prevention Framework Protecting Australians from scams », 8.

[122] Ibid., 4.

l'industrie[123]. Un an après sa création, les pertes liées aux escroqueries signalées avaient chuté de 41 %[124].

Depuis 2023, l'Australie a conçu une stratégie connue sous le nom de *Scam Prevention Framework*, mise en place notamment par le biais d'amendements législatifs à la *Competition and Consumer Act 2010*[125].

L'une de ses dispositions phare est la création, par secteur, de codes spécifiques obligatoires. Bien qu'ils soient encore en cours d'élaboration, ces codes s'appliqueront initialement aux banques, aux entreprises de télécommunications et aux plateformes numériques, mais pourraient également inclure de nouveaux secteurs[126]. Par exemple, les banques seraient tenues d'avertir de manière proactive les clients des tendances récentes en matière d'escroquerie, de prendre des mesures additionnelles de protection pour les transferts à haut risque, et même de s'assurer que les avertissements soient compris par les clients issus de l'immigration dont l'anglais n'est pas la première langue[127].

Du côté des consommateurs, l'Australie a développé des mécanismes internes et externes de résolution des litiges pour les plaintes concernant les entités régulées par le *Scam Prevention Framework*[128]. Également, le gouvernement australien a prévu, à partir de 2025, de financer une campagne de sensibilisation auprès des consommateurs pour identifier et signaler les escroqueries[129].

Enfin, concernant le remboursement des victimes, le *Scam Prevention Framework* est censé garantir des compensations « where businesses have not met their obligations and a consumer has suffered a loss as a result »[130]. Cependant, les dispositions à ce sujet ne sont pas encore claires. Le cadre australien a été salué pour ses mesures préventives, mais critiqué pour son manque de mécanismes concrets de récupération des fonds perdus par les victimes de fraude[131].

---

[123] Ken Westbrook, « What the US Can Learn from Australia's Scam Crackdown », *GASA*, 23 avril 2025, https://www.gasa.org/post/what-the-us-can-learn-from-australia-s-scam-crackdown.
[124] The Treasury, « Scams Prevention Framework Protecting Australians from scams », 2.
[125] The Treasury, « Scams Prevention Framework Summary of reforms ».
[126] Ibid., 9.
[127] The Treasury, « Scams Prevention Framework Protecting Australians from scams », 3-4.
[128] The Treasury, « Scams Prevention Framework Summary of reforms », 7.
[129] The Treasury, « Scams Prevention Framework Protecting Australians from scams », 2.
[130] Ibid., 7.
[131] Carpentier-Desjardins, « Responsabilités en matière de fraude bancaire: étude de cas du Royaume-Uni et de l'Australie », 7.

5.2. Le Royaume-Uni

La sophistication des méthodes d'ingénierie sociale utilisées pour commettre des fraudes peut contourner même les meilleurs systèmes antifraude[132]. Pour cette raison, même le système de prévention le plus robuste ne tranche pas la question du remboursement des victimes lorsque la fraude n'a pas pu être évitée. Le Royaume-Uni s'est attaqué à ce problème par le biais du *Financial Services and Markets Act 2023*, qui confère au *Payment Systems Regulator* (PSR) le pouvoir de publier des exigences en matière de remboursement en cas de fraude[133].

Après la mise en place d'un code volontaire de remboursement des victimes de fraude en 2019, le *Contingent Reimbursement Model Code* (CRM), le *Payment Systems Regulator* (PSR) a mis en œuvre un régime obligatoire, en vigueur à partir du 7 octobre 2024. Ce régime présente les caractéristiques suivantes[134] :

- Il s'applique à tous les prestataires de services de paiement opérant sur le *Faster Payment System* (FPS), qui concentre 97 % des cas de fraude APP, ainsi qu'au système *CHAPS*[135], où se produisent 4 % de ces fraudes en valeur monétaire[136] ;
- Il concerne les consommateurs, les petites entreprises et les organismes de bienfaisance ;
- Il s'applique aux fraudes signalées dans un délai de 13 mois à partir de l'envoi du dernier paiement ;
- La victime doit être remboursée dans un délai de cinq jours, sauf si l'institution financière a besoin de plus de temps pour recueillir des informations supplémentaires ;
- L'institution émettrice et l'institution réceptrice doivent assumer chacune 50 % du remboursement ;
- Le plafond de remboursement est fixé à 85000 £ (environ 157000 $) ;
- Les institutions émettrices peuvent exiger une franchise pouvant aller jusqu'à 100 £ (environ 187 $), sauf s'il s'agit d'une personne vulnérable ;
- Les seules exceptions au remboursement concernent les cas où le consommateur a agi de manière frauduleuse ou a fait preuve d'une

[132] Braithwaite, « 'Authorized Push Payment' Bank Fraud », 176.
[133] Financial Services and Markets Act 2023 (R.-U.), art. 72.
[134] Payment Systems Regulator, « Consolidated policy statement APP scams reimbursement requirement », 8-9; Braithwaite, « 'Authorized Push Payment' Bank Fraud », 184.
[135] La réglementation du système CHAPS est un peu différente, puisqu'elle relève de la supervision de la Bank of England. Payment Systems Regulator, « Consolidated policy statement APP scams reimbursement requirement », 6-8.
[136] Braithwaite, « 'Authorized Push Payment' Bank Fraud », 183-84.

négligence grave. Toutefois, si la victime est une personne vulnérable, elle doit être remboursée, peu importe le degré de négligence.

Le seuil de la négligence grave est relativement élevé, ce qui permet à la majorité des victimes d'être remboursées[137]. En effet, la négligence grave correspond au non-respect de l'une des normes de diligence suivantes[138] :

- Premièrement, les consommateurs doivent tenir compte des interventions effectuées par l'institution financière ou par une autorité compétente.
- Deuxièmement, ils doivent signaler rapidement la fraude à l'institution financière.
- Troisièmement, ils doivent répondre à toute demande raisonnable d'information émanant de l'institution financière.
- Enfin, les consommateurs doivent consentir à ce que l'institution financière transmette un rapport à la police ou à une autorité compétente.

Par ailleurs, l'intégralité du fardeau de preuve pour démontrer la négligence grave du consommateur repose sur l'institution financière[139].

Quant à la vulnérabilité — qui garantit le remboursement en toutes circonstances —, sa définition est assez large : « A vulnerable [consumer] is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care »[140]. Il s'agit d'une définition intéressante, car elle est cohérente avec les recherches qui soutiennent que la vulnérabilité n'est pas une catégorie fixe, mais tributaire des circonstances individuelles[141]. De plus, cette notion large de la vulnérabilité peut inclure des personnes indépendamment de leur

---

[137] Chen Yang, « Protecting Financial Consumers from Authorized Push Payment Fraud », 6.
[138] Payment Systems Regulator, *Guidance: Authorised Push Payment Fraud Reimbursement – The Consumer Standard of Caution Exception Guidance*.
[139] Ibid., 3.
[140] Payment Systems Regulator, « Consolidated policy statement APP scams reimbursement requirement », 17. En fait, le Payment Systems Regulator renvoie le lecteur à un document de la Financial Conduct Authority qui doit guider le traitement des personnes vulnérables : "Firms should think about vulnerability as a spectrum of risk. All customers are at risk of becoming vulnerable and this risk is increased by characteristics of vulnerability related to 4 key drivers. • Health – health conditions or illnesses that affect ability to carry out day-to-day tasks. • Life events – life events such as bereavement, job loss or relationship breakdown. • Resilience – low ability to withstand financial or emotional shocks. • Capability – low knowledge of financial matters or low confidence in managing money (financial capability). Low capability in other relevant areas such as literacy, or digital skills". Cette même institution declare : "Firms should understand how vulnerability can be perpetuated or worsened by their own actions, or inaction". Financial Conduct Authority, *Finalised Guidance FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers*.
[141] Cassandra Cross, « Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons », 104.

tranche d'âge, bien que quelques caractéristiques données comme exemple touchent directement les aînés : « physical disability, retirement, severe or long-term illness, bereavement, hearing or visual impairment, mental health condition or disability, poor or non-existent digital skills, low mental capacity or cognitive disability »[142]. Des données de 2020 montraient qu'entre 46 % et 53 % des personnes adultes au Royaume-Uni présentaient des caractéristiques de vulnérabilité[143].

L'approche du Royaume-Uni présente de nombreux avantages. Citons, par exemple, la responsabilisation des institutions financières, y compris des institutions réceptrices où les fraudeurs détiennent des comptes[144]. Cette approche permet également de limiter les effets néfastes de la fraude sur les individus, tout en instaurant un sentiment de justice universelle, dans lequel toutes les victimes peuvent facilement être remboursées sans avoir à multiplier les démarches.

Pourtant, cette législation présente aussi certaines limites. Pensons, par exemple, au fait que l'entité régulatrice, le *Payment System Regulator* (PSR), ne dispose de pouvoirs réglementaires que sur les systèmes de paiement britanniques qui transigent en livre sterling ; ces pouvoirs ne s'étendent pas aux paiements transfrontaliers, ce qui réduit la portée de la lutte contre un crime transnational comme la fraude[145]. De plus, bien que la grande majorité des fraudes autorisées aient lieu sur des systèmes réglementés comme le *Faster Payment System* (FPS) ou *CHAPS*, une législation fragmentée par système de paiement pourrait entraîner une migration des fraudes vers d'autres systèmes[146].

5.3. L'Union européenne

Le *Règlement sur les services numériques* de 2022 propose un ensemble de mesures visant à combattre activement le contenu illégal sur les plateformes numériques, ce qui inclut le contenu trompeur et frauduleux.

En principe, à l'instar de la *Loi concernant le cadre juridique des technologies de l'information* du Québec, l'Union européenne propose « un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires »[147]. Ainsi, « le fournisseur de services n'est pas responsable

---

[142] Financial Conduct Authority, *Finalised Guidance FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers*, 10-11.
[143] Financial Conduct Authority, *Finalised Guidance FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers*, 10.
[144] Braithwaite, « 'Authorized Push Payment' Bank Fraud », 186.
[145] Payment Systems Regulator, « Consolidated policy statement APP scams reimbursement requirement », 9; Braithwaite, « 'Authorized Push Payment' Bank Fraud », 187.
[146] Braithwaite, « 'Authorized Push Payment' Bank Fraud », 188.
[147] *Règlement sur les services numériques*, art. 1.

des informations stockées à la demande d'un destinataire du service à condition que le fournisseur:

a) n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent; ou

b) dès le moment où il en prend connaissance ou conscience, agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible »[148].

Cela également « à condition que le fournisseur: a) ne soit pas à l'origine de la transmission; b) ne sélectionne pas le destinataire de la transmission; et c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission »[149]. Enfin, comme au Québec, « les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales »[150].

Cependant, cette exemption de responsabilité en cas de contenu illégal affiché sur les plateformes en ligne n'est que conditionnelle. En effet, le *Règlement sur les services numériques* prévoit des « règles relatives à des obligations de diligence spécifiques »[151] qui pourraient rendre responsables les fournisseurs de services intermédiaires en cas de fraude. Ainsi, les fournisseurs de services intermédiaires du monde numérique sont tenus 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 illicite[152].
- Des mécanismes internes de signalement du contenu illicite[153]. Ces mécanismes, facilement accessibles aux consommateurs, permettraient à l'entreprise de prendre connaissance du contenu illégal et pourraient la rendre responsable en cas de fraude.
- Des mesures organisationnelles pour que des « signaleurs de confiance », un rôle attribué par les États membres de l'Union

[148] Ibid., art. 6.
[149] Ibid., art. 4.
[150] Ibid., art. 8.
[151] Ibid., art. 1.
[152] Ibid., art. 15.
[153] Ibid., art. 16.

européenne, puissent notifier de manière prioritaire les entreprises du contenu illégal sur les plateformes en ligne[154].

- 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 présentée[155].
- Des mécanismes pour informer les consommateurs ayant acheté un produit ou un service illégal sur la nature de celui-ci et sur tout recours pertinent[156]. Cette mesure s'applique pour les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance.

Plus important encore, les « fournisseurs de très grandes plateformes en ligne » (ayant 45 millions ou plus d'utilisateurs moyens mensuels actifs)[157], comme Facebook, auraient des obligations supplémentaires de gestion des « risques systémiques » :

- Recenser, analyser et évaluer « tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux… et le droit fondamental à un niveau élevé de protection des consommateurs »[158].
- Prendre des mesures d'atténuation des risques. Cela inclut le marquage visible des « hypertrucages »[159], où des images manipulées ressemblent à des personnes réelles, comme des vedettes invitant à faire des investissements. Cette mesure permet de contrer une pratique très utilisée en contexte de fraude[160].
- Mettre à la disposition du public un registre afin de renforcer la transparence de la publicité en ligne, incluant qui paye pour la publicité et qui la reçoit[161].
- Partager des données avec les États membres de l'Union européenne et des chercheurs agréés, permettant de contrôler et d'évaluer le respect du règlement et la compréhension des risques systémiques[162].

---

[154] Ibid., art. 22.
[155] Ibid., art. 26.
[156] Ibid., art. 32.
[157] Ibid., art. 33.
[158] Ibid., art. 34.
[159] Ibid., art. 35.
[160] *Marie contre Goliath*. Réalisé par Christian Lalumière. Animé par Marie-Claude Barrette. Canada : Attraction Images Productions VIII inc., 2025. Diffusé le 31 mars 2025. Disponible sur ICI Tou.tv : https://ici.tou.tv/marie-contre-goliath.
[161] *Règlement sur les services numériques*, art. 39.
[162] Ibid., art. 40.

De plus, le *Règlement sur les services numériques* encourage l'élaboration de codes de conduite volontaires pour contribuer à son application et faire face aux contenus illicites et aux risques systémiques[163]. Bien que volontaires, « en cas de non-respect systématique des codes de conduite, (les entités en charge) peuvent inviter les signataires desdits codes à prendre les mesures qui s'imposent »[164].

Finalement, on trouve une mesure de responsabilisation importante qui pourrait être envisagée par les consommateurs victimes de fraude cherchant à obtenir un dédommagement : « Les destinataires du service ont le droit de demander réparation aux fournisseurs de services intermédiaires, conformément au droit de l'Union et au droit national, pour les dommages ou pertes subis en raison d'une violation par lesdits fournisseurs des obligations qui leur incombent au titre du présent règlement »[165].

En somme, le Canada gagnerait à s'inspirer de l'Australie, du Royaume-Uni et de l'Union européenne pour mieux protéger les victimes de fraude. D'une part, la prévention implique de responsabiliser les acteurs dont l'infrastructure est utilisée pour commettre la fraude, notamment les banques, les compagnies de télécommunication et les plateformes numériques[166]. D'autre part, le remboursement universel des victimes permet de réduire les effets de la fraude et d'éviter de faire porter le blâme aux personnes fraudées. De plus, l'accent mis sur les « personnes vulnérables » en tant que sujets de protection particulière permet d'inclure davantage de personnes que par la seule tranche d'âge, et constitue une approche cohérente avec le fait que la vulnérabilité est fluide.

Conclusion et recommandations

Bien qu'une part considérable des signalements de fraude provienne de personnes âgées, le phénomène liant fraude et vieillissement demeure peu exploré. Son étude soulève de nombreux défis, notamment le flou conceptuel entourant la notion d'aîné, la disparité des catégorisations des différents types de fraude, ainsi que le caractère essentiellement exploratoire et descriptif de la littérature existante.

Quoi qu'il en soit, les personnes victimes de fraude sont mal protégées au Canada. Malgré l'ampleur du problème, le pays ne dispose pas d'une stratégie nationale de lutte contre la fraude. Le cadre canadien en la matière est épars,

[163] Ibid., art. 45-46.
[164] Ibid., art. 45.
[165] Ibid., art. 54.
[166] Ombudsman for Banking Services and Investments, 11.

réparti entre différentes lois provinciales et fédérales, codes de conduite et décisions des tribunaux. Ce cadre manque de balises claires qui responsabilisent les principaux secteurs dont l'infrastructure est utilisée pour commettre des fraudes : les institutions financières, les compagnies de télécommunications et les plateformes en ligne.

De plus, seules certaines victimes de transactions « non autorisées » pourraient, dans certains cas, être remboursées par les banques. Cela pousse à croire que les institutions financières blâment systématiquement les victimes de fraude ayant « autorisé » la transaction, en laissant entendre que la responsabilité leur revient, bien qu'elles aient été la cible de stratégies d'escroquerie particulièrement raffinées.

Pourtant, les conséquences de la fraude peuvent être catastrophiques pour les victimes, en particulier pour les personnes les plus vulnérables. Ses effets dépassent largement les seules pertes financières : elle affecte aussi la santé physique et mentale des victimes, ainsi que celle de leurs proches. La fraude constitue ainsi un enjeu majeur de sécurité économique et de santé publique. En outre, elle nuit à la confiance envers le système financier canadien dans un contexte d'incertitude économique croissante.

Bien que davantage de recherches soient nécessaires pour mieux comprendre le phénomène de la fraude ciblant les aînés et proposer des politiques publiques fondées sur des bases solides, force est de constater le besoin urgent de développer des mesures préventives et de protection pour les victimes.

À l'instar de l'Australie, le Canada devrait responsabiliser l'ensemble des acteurs des principaux secteurs utilisés par les fraudeurs — comme les services financiers, les télécommunications et les plateformes numériques — et leur imposer l'adoption de mesures de protection plus efficaces. Cela inclut le développement de campagnes ciblées de sensibilisation et d'éducation.

À l'instar du Royaume-Uni, le Canada gagnerait à exiger des institutions financières le remboursent des victimes de tout type de fraude. Une telle mesure contribuerait à atténuer les conséquences catastrophiques de ce crime, à faire prévaloir une protection universelle à toutes les personnes, et à réduire les délais et les démarches auxquels les victimes sont confrontées.

Également à l'instar du Royaume-Uni, le Canada pourrait envisager de mettre en place des mesures spéciales de protection pour les personnes vulnérables, qui ne devraient pas pouvoir se voir refuser un remboursement, quelles que soient les circonstances. La notion de personne vulnérable, plutôt que celle d'aîné, permettrait d'inclure un plus grand nombre de personnes et

serait cohérente avec le constat selon lequel il n'existe pas de profil démographique plus enclin à être victime de fraude.

Finalement, comme au sein de l'Union européenne, le Canada pourrait s'attaquer aux contenus frauduleux affichés sur les plateformes en ligne en exigeant des géants du web des mesures fortes de prévention et d'atténuation des risques.

Pour protéger les aînés victimes de fraude, nous formulons les recommandations suivantes :

- **L'établissement d'un cadre légal de protection uniforme pour tous les types de fraude (transactions « non autorisées » et « autorisées ») et pour tous les modes de paiement, faisant reposer une responsabilité accrue sur les banques et exigeant le remboursement universel des victimes ;**
- **Des mesures spéciales de protection pour les personnes vulnérables, dont les aînés, qui devraient être remboursées en cas de fraude, quelles que soient les circonstances ;**
- **Des exigences robustes responsabilisant les institutions financières, les compagnies de télécommunications, les plateformes numériques et tout autre secteur dont l'infrastructure est utilisée pour commettre des fraudes ;**
- **Des exigences pour les institutions financières, les compagnies de télécommunications, et les plateformes numériques de partage de données concernant le nombre et le type de fraudes commises via leur infrastructure ainsi que les caractéristiques démographiques des victimes, dont l'âge.**
- **Le financement d'études à long terme visant à mieux comprendre le phénomène liant fraude et vieillissement, ainsi que ses impacts sur la population et l'économie ;**
- **Le soutien financier aux organismes d'accompagnement des victimes de fraude, dont les associations de consommateurs et d'aide aux aînés.**