RAPPORT ANNUEL 2022

Centre antifraude du Canada

Gendarmerie royale du Canada | Royal Canadian Mounted Police | Bureau de la concurrence Canada | Competition Bureau Canada | Police Provinciale de l'Ontario | Canada

ISSN : 2816-8348

PS61-46F-PDF

Communiquer avec nous à :

antifraudcentre-centreantifraude.ca

Centre antifraude du Canada | Facebook

Centre antifraude du Canada (@antifraudecan) | Twitter

Table des matières

Avant-propos

J'ai le plaisir de vous présenter le rapport annuel 2022 du CAFC (le Rapport). Il contient une analyse approfondie des tendances, des statistiques et des conseils fondés sur nos observations de la dernière année. Dans le cadre d'un nouveau partenariat du Centre antifraude du Canada (CAFC) avec l'Initiative pour un gouvernement ouvert du gouvernement du Canada, l'ensemble de données utilisé dans le présent rapport est également **publié en ligne à des fins de consultation, de recherche et d'examen transparents**. Cet ensemble de données constitue la première contribution de la GRC à l'Initiative pour un gouvernement ouvert.

On parle de fraude en cas de tromperie intentionnelle visant à voler de l'argent, des biens ou des renseignements. Si l'objectif de gains personnels ou financiers de la fraude est demeuré le même au fil des années, les fraudeurs changent souvent de tactiques, d'outils et de cibles pour améliorer leurs chances de réussite. Les progrès technologiques sont un catalyseur pour les avancées des techniques de fraude.

Les Canadiens continuent d'être victimes de cyberfraude. En 2022, le CAFC a reçu plus de 91 000 signalements pour un total d'environ 530 millions de dollars de pertes, soit les pertes liées à la fraude les plus élevées jamais enregistrées. Malheureusement, rien ne laisse présager que cette tendance va changer.

Dans le contexte des dernières années marquées par la montée des fraudes sur le thème de la COVID-19, de nouvelles tendances se dessinent. Par exemple, nous observons une augmentation des publicités frauduleuses dans les médias sociaux et sur les sites Web. Les publicités sur ces plateformes incitent les utilisateurs à cliquer sur un lien frauduleux ou à communiquer avec un fraudeur et se révèlent très efficaces pour nuire aux Canadiens. Nous prévoyons que cette tendance se poursuive.

Nous remarquons également que les technologies émergentes et le cyberenvironnement favorisent des formes d'escroquerie plus complexes que les utilisateurs ont de plus en plus de mal à détecter comme de la fraude. Dans le cyberenvironnement, les fraudeurs peuvent également dissimuler plus facilement leur identité, se faire passer pour des amis, des figures d'autorité ou d'autres personnalités, voire créer d'innombrables comptes gérés par des services ou des programmes automatisés (robots).

L'environnement de la fraude et de la cybercriminalité en constante évolution et l'augmentation des pertes montrent l'importance du CAFC en tant que service de police national. Le CAFC offre une assistance directe aux Canadiens et aux organisations canadiennes touchés par la fraude, harmonise et coordonne les efforts de lutte contre la fraude avec les services de police nationaux et internationaux et participe à des efforts complets d'éducation et de sensibilisation à la fraude partout au Canada.

Bien que le CAFC travaille sans relâche avec ses partenaires pour combattre la fraude, chaque citoyen canadien a un rôle à jouer. On continue d'estimer que seulement de 5 à 10 % des cas de fraude et de cybercriminalité sont signalés. Il est important que toute personne visée par une fraude soumette un signalement au CAFC. Les signalements occupent une place essentielle dans nos efforts de prévention, de sensibilisation et de perturbation.

Chris Lynam
Directeur général
Centre national de coordination contre la cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)
Gendarmerie royale du Canada

Résumé

Le rapport annuel 2022 du CAFC donne un aperçu des fraudes signalées au CAFC entre le 1er janvier et le 31 décembre 2022. Le rapport met en lumière les grandes tendances en matière de fraude et de cybercriminalité et présente une vue d'ensemble des efforts continus et des interventions du CAFC dans l'environnement de la fraude actuel.

Le CAFC reçoit des signalements des Canadiens, des entreprises et des organisations canadiennes ainsi que des signalements internationaux en lien avec le Canada. Ces signalements sont stockés dans la base de données du Système de signalement des fraudes (SSF) géré par le CAFC. Le CAFC analyse les signalements pour distinguer les tendances, recueillir des renseignements et éclairer les enquêtes policières.

L'année 2022 a été une année marquée par un nombre important de victimes et de pertes liées à la fraude au Canada. Le CAFC a observé quatre tendances constantes et généralisées au cours de cette période :

1. La fraude mène à des pertes plus importantes

Le CAFC a continué d'observer une hausse constante des pertes liées à la fraude en 2022. Le CAFC a reçu près de 91 000 signalements de fraude classique et de cyberfraude par l'entremise du centre d'appels et du système de signalement en ligne, qui représentent des pertes totalisant 530,4 millions de dollars. À titre de référence, en 2021, le CAFC avait observé des pertes totales d'environ 383 millions de dollars pour un nombre de signalements comparable à celui de 2022. Aux pertes liées à la fraude s'ajoute un nombre croissant de signalements de fraude à l'identité et de vol de renseignements personnels dont le coût ne peut pas être évalué avec exactitude[1]. Les fraudes liées aux cryptomonnaies et à l'investissement prennent également de plus en plus de place; environ 97 millions de dollars de pertes ont été déclarés pour la fraude à l'investissement dans les cryptomonnaies.

1 Veuillez consulter la section « **À propos des chiffres** » à la page 59 pour en savoir plus sur les raisons pour lesquelles le CAFC ne produit pas d'évaluations des pertes financières dues aux crimes liés à l'identité.

2. La fraude est de plus en plus personnelle

On admet communément que la majorité des fraudes constituent une forme de criminalité éloignée perpétrée par des opérations de fraude situées dans d'autres pays. La plupart des personnes pensent à tort que l'argent transite de la victime à l'opération de fraude de manière simple et directe.

Les opérations de fraude nationales et internationales recrutent de plus en plus de personnes au Canada pour les aider à commettre des fraudes. Des mules et des assistants à la fraude se rendent chez les victimes et communiquent directement avec les cibles potentielles. Cette tendance a pris rapidement de l'ampleur en 2022. Le CAFC s'est vu signaler de nombreux fraudeurs et cybercriminels menaçant ouvertement les victimes et utilisant du contenu explicite et des renseignements personnels et financiers pour escroquer les victimes et leurs familles. Les victimes ne sont pas seulement touchées par une perte d'argent ou un vol de renseignements, mais subissent également des préjudices psychologiques et émotionnels.

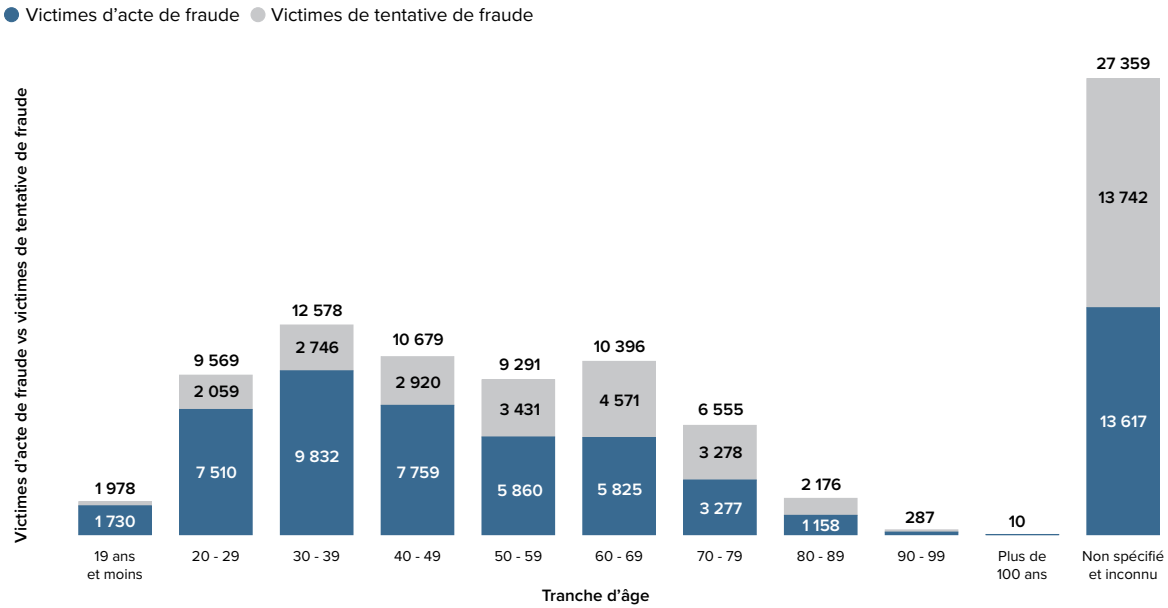
3. La fraude et la cybercriminalité ciblent tous les groupes d'âge

Autre hypothèse erronée : la fraude ne toucherait que les personnes âgées et les populations vulnérables. Bien que les signalements effectués par des personnes de 60 ans et plus aient dépassé tous les autres groupes d'âge en 2021, on observe un changement radical dans les signalements par tranche d'âge en 2022. Tous les groupes d'âge sont ciblés par la fraude en 2022. Les jeunes sont de plus en plus victimes de formes de fraude subtiles et adaptées à leur âge.

Les opérations de fraude utilisent les médias sociaux et d'autres applications pour cibler les jeunes. En 2022, le CAFC a reçu 7 510 signalements de personnes de 20 à 29 ans, 9 832 de personnes de 30 à 39 ans et 7 759 de personnes de 40 à 49 ans. Les signalements de personnes de 20 à 49 ans l'emportaient sur ceux des personnes de 50 à 89 ans, ce dernier groupe d'âge ayant présenté 16 120 signalements en 2022.

Les fraudeurs développent une capacité à cibler tous les utilisateurs d'Internet en faisant preuve de créativité. Les jeunes étant les plus susceptibles d'être approchés en ligne et ne comprenant pas nécessairement la menace que représente la fraude deviennent une cible privilégiée pour les opérations de fraude sur Internet.

Nombre de victimes de tentative de fraude vs nombre de victimes d'acte de fraude par tranche d'âge



Contrairement à 2021, en 2022, la majorité des signalements de fraude reçus provenaient de personnes âgées de 20 à 29 ans, de 30 à 39 ans et de 40 à 49 ans. Ces chiffres témoignent d'un changement vers de nouvelles techniques de fraude fructueuses utilisées sur les plateformes des médias sociaux et les applications en ligne qui ciblent les jeunes Canadiens.

4. Un accès plus facile aux renseignements personnels favorise la fraude

Comme les Canadiens publient des renseignements plus personnels ou précis sur des sites accessibles comme LinkedIn, Facebook, Instagram et Twitter, les opérations de fraude peuvent utiliser ces renseignements publics pour créer des scénarios de fraude ciblés et plus crédibles. Les fraudeurs sont en mesure, de cette manière, d'en savoir davantage sur les groupes d'amis, le travail, les aspirations professionnelles, les passe-temps et les centres d'intérêt d'une personne, ainsi que sur sa situation financière. Les fraudeurs peuvent également obtenir des renseignements volés par les cybercriminels. Cette tendance conduit à des tentatives de fraude précises, avancées et crédibles, qui augmentent le risque de victimisation.

De plus, les stratagèmes frauduleux envoyés par le biais de comptes volés ou piratés à des amis et à des abonnés en ligne de la personne se sont répandus en 2022. Cette tendance à l'échange de renseignements permet aux fraudeurs de mieux connaître la personne et de la cibler avec des formes de fraude plus subtiles. Dans ce contexte, la fraude à l'identité et le vol de renseignements personnels continuent d'être fortement représentés dans tous les groupes d'âge, comptant pour environ 27 600 signalements au CAFC en 2022.

À propos du CAFC

Situé à North Bay, en Ontario, et créé en 1993 sous le nom de PhoneBusters, le CAFC a été établi en réponse à la menace croissante des pratiques de télémarketing trompeuses. Aujourd'hui, le CAFC est le dépôt central de données et de renseignements sur la fraude au Canada exploité conjointement par la Gendarmerie royale du Canada (GRC), la Police provinciale de l'Ontario (PPO) et le Bureau de la concurrence du Canada.

Le CAFC s'engage à fournir en temps opportun des données et des renseignements exacts et utiles sur les fraudes pour sensibiliser et aider les citoyens, les entreprises, les forces de l'ordre et les institutions gouvernementales au Canada et ailleurs dans le monde.

En tant que service de police national administré par la GRC, le CAFC offre un soutien à tous les organismes d'application de la loi dans l'ensemble du Canada. Le Centre national de coordination contre la cybercriminalité (CNC3) de la GRC fait partie des organisations partenaires du CAFC relevant de la même sous-direction opérationnelle de la GRC.

Responsabilités essentielles du CAFC

PRÉVENTION

Le CAFC organise des campagnes de sensibilisation à la fraude, comme le Mois de la prévention de la fraude, et présente des exposés aux collectivités et aux organisations.

Le CAFC est la principale source nationale de documents et d'information sur la fraude et les crimes liés à l'identité. Des alertes, des conseils et des trousses de prévention en matière de fraude sont affichés sur le site Web du CAFC et distribués régulièrement aux partenaires.

PERTURBATION

Le CAFC collabore avec des partenaires, notamment des institutions financières, des sociétés émettrices de cartes de crédit, des fournisseurs de télécommunications et d'accès Internet, pour contrer la fraude.

Les activités de perturbation visent à démanteler les outils utilisés par les opérations de fraude et à prévenir la fraude avant qu'elle ne se produise.

Dans certains cas, le CAFC peut contribuer à intercepter les transferts d'argent frauduleux avant que la victime perde tout son argent.

RENSEIGNEMENT

Avec les signalements de fraude et de crimes liés à l'identité soumis par l'entremise du Système de signalement des fraudes, le CAFC peut effectuer des regroupements et fournir des données et des renseignements donnant matière à des poursuites. Ces travaux sont transmis aux services de police compétents afin d'enrichir les efforts d'enquête au Canada et à l'étranger.

Le CAFC regroupe également des statistiques et analyse les signalements pour informer les Canadiens et les partenaires sur les tendances en matière de fraude.

SOUTIEN

Le CAFC offre un soutien direct aux victimes de fraude. Par l'entremise du centre d'appels du CAFC, les analystes de la réception prodiguent des conseils aux victimes de fraude et aiguillent les personnes effectuant le signalement vers des services supplémentaires.

Le Groupe de soutien aux aînés du CAFC fournit du soutien et des conseils ciblés aux aînés et aux victimes vulnérables de fraude.

PARTENARIATS

La fraude exige une approche globale sociétale avec la participation de tous les groupes touchés, y compris les particuliers, les entreprises du secteur privé et les services de police, qui doivent collaborer pour prévenir la fraude.

Le CAFC entretient des partenariats solides avec des organisations comme les entreprises de messagerie, les sociétés de télécommunications, les institutions financières et la communauté policière en général afin de prévenir la fraude et de contribuer aux enquêtes.

Le CAFC gère le Groupe d'échange de renseignements sur la criminalité financière et coordonne les communications sur la fraude entre les services de police compétents.

Le CAFC s'est associé récemment au Centre national de coordination contre la cybercriminalité (CNC3) avec lequel il collabore pour créer un nouveau Système national de signalement des incidents de cybercriminalité et de fraude (SNSICF).

Rôle du CAFC pour faciliter les enquêtes et prévenir la fraude

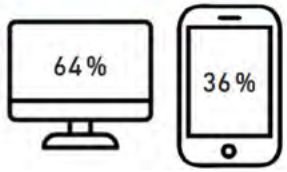
Rapport annuel 2022 du CAFC

MÉTHODE DE SOLLICITATION

Les cybercriminels adaptent les méthodes employées pour solliciter leurs victimes

En 2022, 62,4 % des personnes ayant signalé une escroquerie au CAFC ont également déclaré en avoir été des victimes. Les pertes financières moyennes des victimes ont augmenté de 34,6 % par rapport à 2021 et se sont élevées à 14 000 dollars par victime.

ENVIRON **TROIS SIGNALEMENTS SUR CINQ** AU CAFC ONT ÉTÉ RÉALISÉS PAR **L'ENTREMISE DU SYSTÈME DE SIGNALEMENT DES FRAUDES EN LIGNE DU CAFC.**



530M $
Pertes déclarées au CAFC en 2022

91 000
Signalements reçus en 2022 au centre d'appels et sur le site Web du CAFC

ÉVOLUTION DES CRYPTOMONNAIES

La fraude à l'investissement représente le principal type de fraude utilisant les cryptomonnaies comme mode de paiement, et enregistre des pertes totales de **96 M$** en 2022. Ce chiffre représente une augmentation de **62 %** par rapport à 2021 et de **458 %** par rapport à 2020.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Signalez une fraude
1-888-495-8501

Victimes et pertes financières

Dans le sillage de cette tendance à la hausse, des pertes dues à la fraude sans précédent ont continué d'être enregistrées en 2022. Le CAFC a reçu des signalements de pertes de plus de 530 millions de dollars, ce qui constitue un record historique dans les données du CAFC. À titre de comparaison, le CAFC s'est vu signaler des pertes de 380 millions de dollars en 2021 et de 165 millions de dollars en 2020.

Les 10 principales fraudes – Nombre de signalements de fraude

Type de fraude	Nbre de signalements	% de tous les signalements	Nbre de victimes	% de victimes
Fraude à l'identité	19 543	21,5 %	19 435	99,4 %
Hameçonnage	10 647	11,7 %	2 584	24,3 %
Extorsion	8 266	9,1 %	2 330	28,2 %
Renseignements personnels	8 086	8,9 %	6 155	76,1 %
Service	6 309	6,9 %	4 571	72,5 %
Investissement	4 671	5,1 %	4 283	91,7 %
Enquêteur bancaire	4 255	4,7 %	974	22,9 %
Marchandises	4 001	4,4 %	3 190	79,7 %
Marchandises contrefaites	3 993	4,4 %	3 943	98,7 %
Other	3 302	3,6 %	673	20,4 %
Autre	**73 073**	**80,4 %**	**48 138**	**65,9 %**

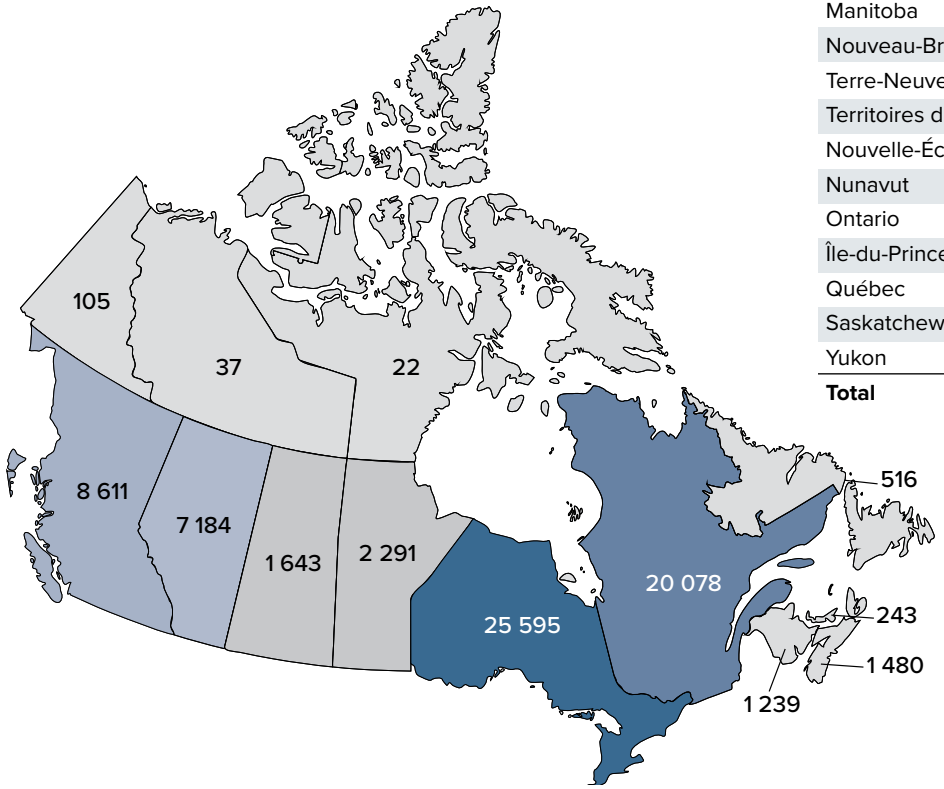
L'extorsion, le vol de renseignements personnels, l'hameçonnage et la fraude à l'identité ont continué de faire l'objet de nombreux signalements en 2022. La fraude liée aux marchandises a également été souvent signalée, principalement en lien avec la tendance des achats en ligne.

En 2022, le CAFC a reçu plus du double de signalements de fraude à l'investissement par rapport à l'année précédente, lesquels signalements ont également généré le plus de pertes jamais enregistrées. Les fraudes liées à un stratagème de rencontre et le harponnage ciblant les organisations ont également entraîné des pertes importantes par victime.

Les 10 principales fraudes – Pertes financières

Type de fraude	Perte financière	Perte moyenne en dollars par victime
Investissement	308 977 217 $	72 140 $
Stratagème de rencontre	59 017 857 $	55 835 $
Harponnage	58 090 488 $	77 765 $
Service	21 090 880 $	4 614 $
Extorsion	19 049 210 $	8 176 $
Urgence (prison, accident, hôpital, aide)	9 424 134 $	8 513 $
Marchandises	8 787 475 $	2 755 $
Autre	7 262 565 $	10 791 $
Emploi	7 115 019 $	4 253 $
Enquêteur bancaire	6 743 980 $	6 924 $
Total	**505 558 825 $**	**24 536 $**

Nombre de signalements par province ou territoire



Province ou territoire	Nbre de signale-ments	Nbre de signalements pour 100 000 habitants	% de victimes	Perte financière
Alberta	7 184	169	62,7 %	52 052 868 $
Colombie-Britannique	8 611	172	65,6 %	77 029 243 $
Manitoba	2 291	171	63,1 %	10 405 018 $
Nouveau-Brunswick	1 239	160	55,6 %	3 163 724 $
Terre-Neuve-et-Labrador	516	101	59,5 %	1 415 861 $
Territoires du Nord-Ouest	37	90	54,1 %	200 392 $
Nouvelle-Écosse	1 480	153	54,7 %	3 792 630 $
Nunavut	22	60	63,6 %	122 610 $
Ontario	25 595	180	63,9 %	213 501 876 $
Île-du-Prince-Édouard	243	157	60,9 %	1 020 967 $
Québec	20 078	236	71,7 %	42 962 079 $
Saskatchewan	1 643	145	66,1 %	9 330 966 $
Yukon	105	261	56,2 %	385 383 $
Total	**69 044**	**187**	**65,9 %**	**415 383 617 $**

L'Ontario et le Québec ont continué d'enregistrer le plus grand nombre de signalements au CAFC. Si la plupart des provinces et des territoires ont fait état d'un nombre de signalements stable en 2022, celui du Québec a presque doublé, passant de 10 479 en 2021 à plus de 20 000 en 2022. Le nombre de signalements de l'Ontario est passé de 19 084 en 2021 à 25 595 en 2022. Les résidents de l'Alberta et de la Colombie-Britannique ont également fait environ 2 000 signalements de plus en 2022 qu'en 2021. Le « % de victimes » indique le pourcentage total de signalements de fraude ayant fait une victime au CAFC par opposition aux signalements de tentative de fraude.

Réussites opérationnelles en 2022

Coordination des vérifications du bien-être avec les services de police locaux

Vivre une situation de fraude peut être un événement extrêmement traumatisant qui change une vie. Certaines personnes signalent une fraude au CAFC seulement après avoir perdu la totalité de leurs économies à l'insu de leur famille ou après avoir vendu ou hypothéqué leur maison ou encore après avoir emprunté de l'argent à des amis et à des membres de leur famille. Dans certaines situations, les personnes peuvent faire état d'idées suicidaires ou menacer de se faire du mal lorsqu'elles communiquent avec le CAFC. Dans d'autres types de fraudes, comme l'extorsion, les personnes qui signalent un événement de fraude peuvent craindre pour leur vie, le fraudeur ayant menacé de leur nuire ou de nuire à leur famille.

Dans ce cas, les analystes du CAFC ajoutent une mention aux dossiers concernés et communiquent immédiatement avec la police locale pour qu'elle entreprenne des vérifications du bien-être aux domiciles désignés. Le CAFC a sollicité la police locale pour procéder à 85 vérifications du bien-être en 2022.

Efforts de soutien opérationnel en 2022

Le CAFC offre du soutien opérationnel pour appuyer les efforts d'enquête en collaboration avec les services de police locaux au Canada et à l'étranger. En 2022, le CAFC a apporté du soutien opérationnel aux services de police et à d'autres partenaires dans 811 cas. Parmi de nombreux autres, les principaux partenaires externes en 2022 comprenaient la Police provinciale de l'Ontario, le Service de police de Winnipeg, Postes Canada, EUROPOL et la Sûreté du Québec.

Coordination et soutien à l'harmonisation

Les enquêtes sur la fraude s'étendent souvent sur plusieurs administrations et frontières, et les différentes opérations de fraude peuvent cibler les Canadiens dans chacune des provinces et chacun des territoires. Afin de mieux coordonner les enquêtes nationales sur les fraudes, le CAFC gère le Groupe d'échange de renseignements sur la criminalité financière (GERCF). Le GERCF soutient l'échange d'information entre les services de police et agit comme point de contact central pour coordonner les enquêtes policières. En 2022, le CAFC a transmis 370 dossiers de renseignement aux membres du GERCF.

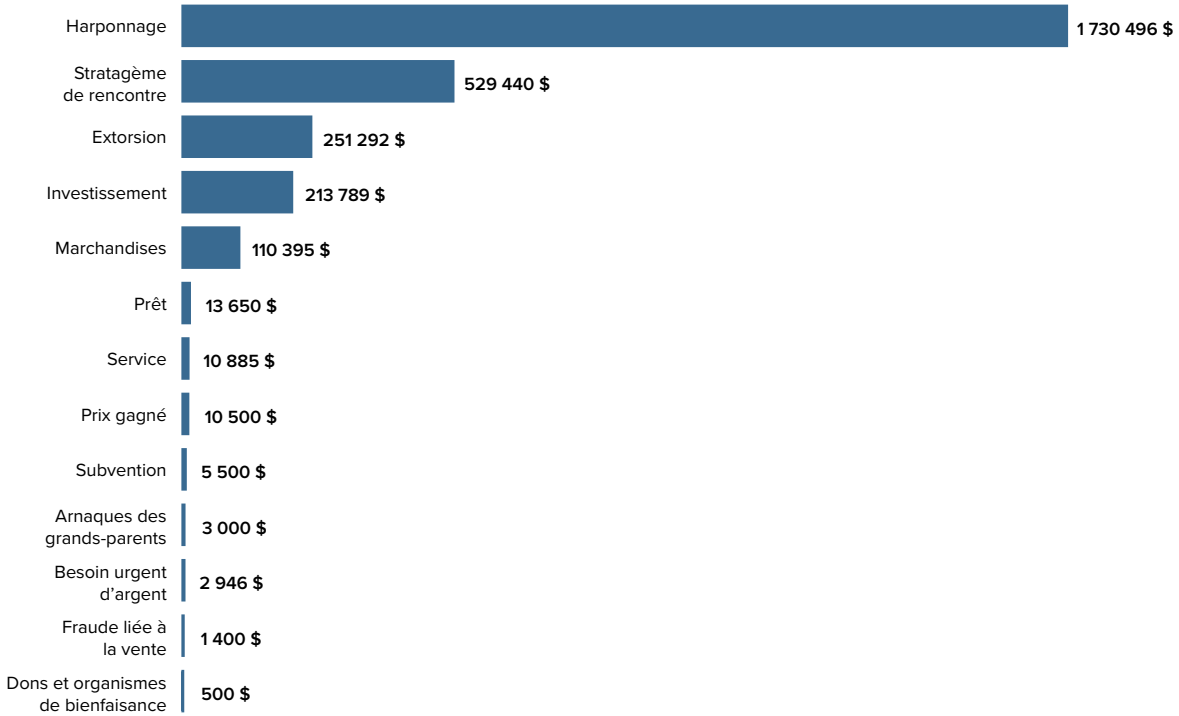
Récupération de l'argent des fraudes en 2022

Lorsqu'une personne ou une organisation signale un incident de fraude, le CAFC peut collaborer avec des partenaires financiers pour geler et récupérer l'argent obtenu frauduleusement. En 2022, le CAFC a contribué à 40 cas de gel et de récupération de fonds, ce qui a

mené à la récupération de 2,9 millions de dollars pour les victimes de fraude. Ces cas comprennent une somme de plus de 100 000 $ récupérée à 12 reprises et une somme de 776 000 $ récupérée en lien avec un événement de harponnage[2].

Le CAFC commence également à percevoir des résultats positifs grâce aux services de traçage des cryptomonnaies. En 2022, le CAFC a réussi à retracer le mouvement de cryptomonnaies obtenues frauduleusement vers une plateforme d'échange donnée et a contribué à la récupération d'environ 17 000 $ en bitcoins.

Sommes récupérées par type de fraude



* Les sommes sont converties en dollars canadiens

Les pertes dues au harponnage représentaient la majorité de l'argent recouvré en 2022. Les attaques d'harponnage continuent de générer des pertes importantes, les fraudeurs ciblant les entreprises et les organisations à l'aide de messages courriel subtils et de manœuvres d'usurpation d'identité.

2 Le CAFC fournit des renseignements donnant matière à des poursuites aux partenaires policiers et financiers, qui procèdent ensuite à la récupération des fonds volés dans la mesure du possible. Si ces statistiques sont utiles à des fins de référence, les récupérations auxquelles contribue le CAFC nécessitent que les partenaires rendent compte des résultats finaux des cas au CAFC. Il arrive que les partenaires ne présentent pas de rapport au CAFC; par conséquent ces statistiques pourraient être sous-évaluées.

Mules

Les opérations de fraude s'appuient sur des mules pour transférer les fonds volés. Les mules peuvent entraver les efforts de traçage de l'argent des institutions financières et des organismes d'application de la loi et permettre aux opérations de fraude de transférer l'argent vers d'autres administrations ou pays.

Les mules continuent de jouer un grand rôle dans la fraude. En 2022, le Groupe du soutien opérationnel du CAFC a ouvert 90 dossiers liés aux mules. Dans un grand nombre de ces dossiers, le personnel du CAFC a observé des liens et des transferts fréquents entre deux mules ou plus souvent situées au Canada.

Le récit suivant tiré d'un dossier du CAFC en 2022 illustre les particularités de l'activité des mules :

En avril 2022, une entreprise de messagerie nord-américaine a communiqué avec le CAFC pour signaler avoir intercepté un colis suspect contenant 4 500 $. Le colis avait été envoyé par une personne en Ontario à une adresse à Minneapolis au Minnesota. Une analyse plus poussée a révélé qu'un total de 50 000 $ avait été transféré du résident de l'Ontario à cette adresse du Minnesota par l'intermédiaire d'autres colis.

Le CAFC a communiqué avec le service de police local américain. La police locale s'est présentée à l'adresse concernée et a découvert que la résidente était victime d'une fraude liée à un stratagème de rencontre. La victime de Minneapolis a déclaré à la police qu'elle recevait des colis au nom de son partenaire amoureux, un investisseur travaillant en Russie. Son amoureux lui demandait de déposer et de transférer l'argent dans un guichet automatique de bitcoins. En réalité, la victime de Minneapolis jouait involontairement le rôle de mule pour le suspect, son amoureux.

Le CAFC a également communiqué avec le service de police local de la victime ontarienne. Après une enquête approfondie, la police locale a conclu que la victime ontarienne entretenait une relation intime en ligne avec le même suspect que la victime à Minneapolis.

Le fraudeur faisait croire à la victime ontarienne que la personne à Minneapolis était sa « nounou » et lui demandait d'envoyer l'argent à l'adresse de Minneapolis pour aider la nounou à payer ses factures médicales. La victime ontarienne avait envoyé treize colis distincts contenant de l'argent comptant à la victime située à Minneapolis. La victime de Minneapolis déposait ensuite l'argent reçu dans le portefeuille du suspect à un guichet automatique de bitcoins.

Une enquête approfondie a montré que la victime de Minneapolis avait accepté et déposé plus de 300 000 $ provenant de onze autres victimes sur deux ans.

Réalisant qu'elle participait activement à une opération de fraude, la victime de Minneapolis a déclaré au CAFC qu'elle cesserait toute communication avec le suspect et n'accepterait plus de colis. Peu après, le suspect a communiqué avec les deux victimes pour leur expliquer que le CAFC tentait de rompre leurs relations et que ces relations devaient se poursuivre.

Le suspect utilisait des noms différents avec les deux victimes et encourageait les victimes à communiquer régulièrement entre elles pour assurer le succès des transferts d'argent. Jusqu'à ce que le CAFC et la police locale prennent contact avec les victimes, les deux personnes n'avaient pas réalisé qu'elles étaient victimes de fraude sentimentale et ignoraient que leur expérience était rattachée au même fraudeur. Cet exemple montre que les victimes de fraude ont besoin d'information, de sensibilisation et de soutien continus; c'est ce qu'offre le CAFC en partenariat avec les services de police locaux.

Plan de prévention de la fraude

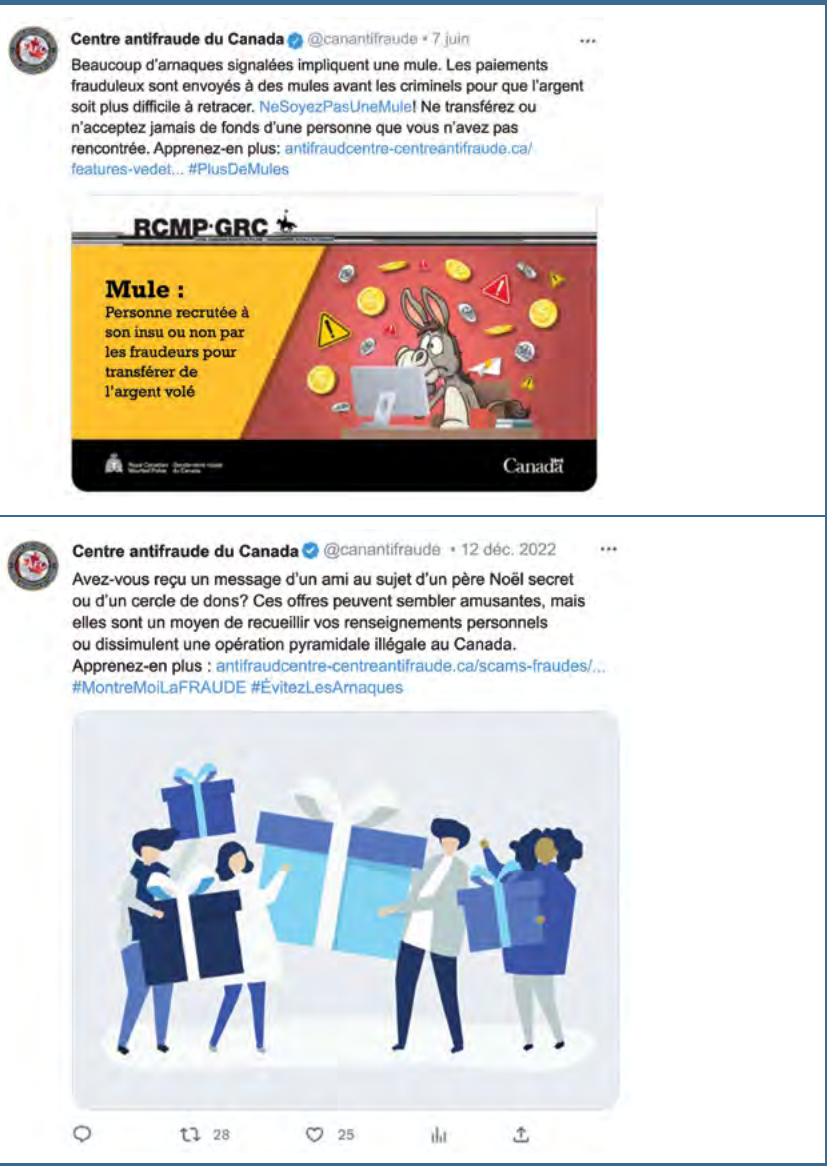
Le CAFC copréside le Mois de la prévention de la fraude (MPF) chaque année en mars, en collaboration avec des partenaires clés comme le Bureau de la concurrence du Canada et la Police provinciale de l'Ontario (PPO), pour sensibiliser les Canadiens à la fraude. Au cours du Mois de la prévention de la fraude de 2022, le CAFC a fourni les éléments suivants :

- 24 exposés à des groupes communautaires et à des partenaires, parmi lesquels plusieurs présentations aux réfugiés ukrainiens du Québec sur la prévention de la fraude
- Information par l'entremise de publications sur Facebook et Twitter
- Documents affichés sur le site Web du CAFC
- Bulletins et trousses d'outils distribués à plus de 700 partenaires
- 421 réponses aux demandes des médias

Démontrant la valeur de la campagne du MPF, les mots-clics officiels du CAFC #FPM2022 (en anglais) et #MPF2022 (en français) ont été utilisés sur environ 30 millions de comptes Twitter et 11,5 millions de comptes Facebook.

Bien que le Mois de la prévention de la fraude soit l'une des plus importantes campagnes de sensibilisation du CAFC, l'organisation a également dirigé une Campagne de sensibilisation aux mules avec la PPO et la GRC, participé au Mois de la sensibilisation à la cybersécurité et mené une campagne contre les escroqueries du temps des Fêtes, entre autres activités.

Sur ses comptes Facebook et Twitter et sur son site Web, le CAFC partage régulièrement de l'information sur la fraude avec des milliers d'abonnés.



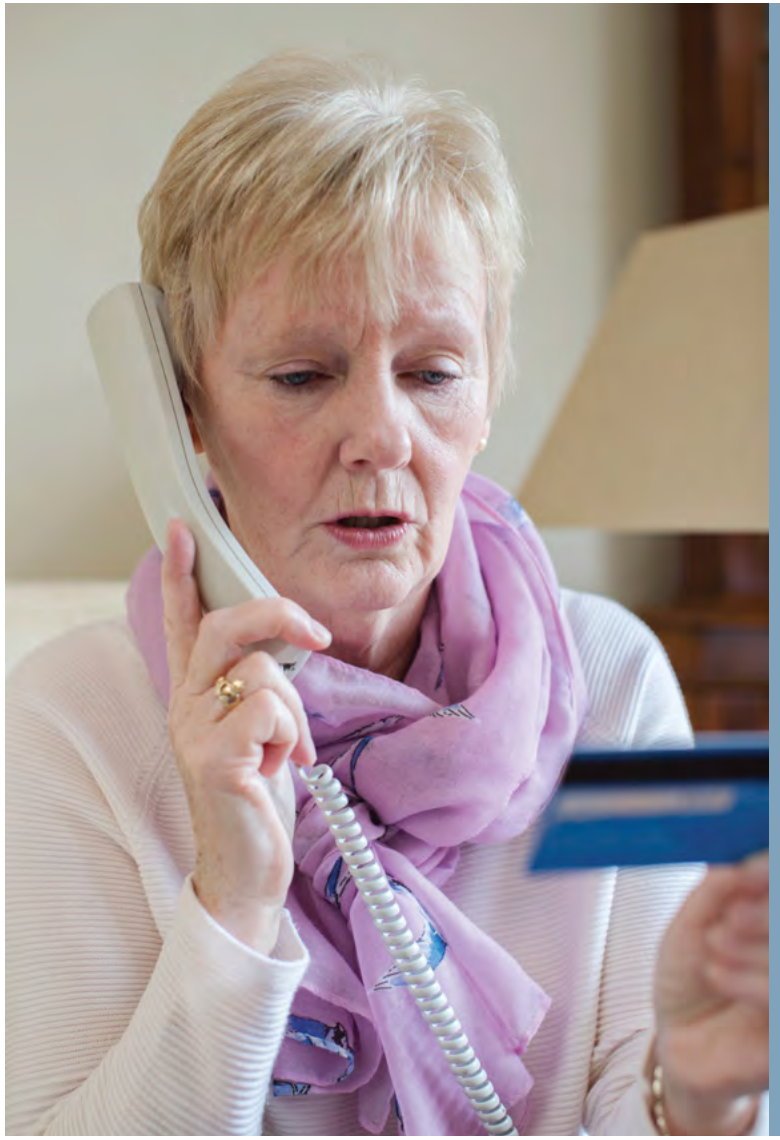
En lien avec les tendances en matière de fraude, le CAFC fournit des perspectives clés aux articles des médias afin de sensibiliser le public à la fraude. Voici quelques exemples de 2022 :

- **Grandparent scams are on the rise. Here's how you can protect yourself (CTV News) [Les arnaques des grands-parents en hausse : voici comment vous protéger]**
- **10 common crypto scams and how to avoid them (MoneySense) [10 fraudes fréquentes liées aux cryptomonnaies et comment les éviter]**
- **'Protect your wallet and your heart,' warns woman after finding Ontario beau's romance scam links (CBC News) [« Protégez votre portefeuille et votre cœur », recommande une femme après avoir découvert les liens de son amoureux avec un stratagème de rencontre]**

Groupe de soutien aux aînés

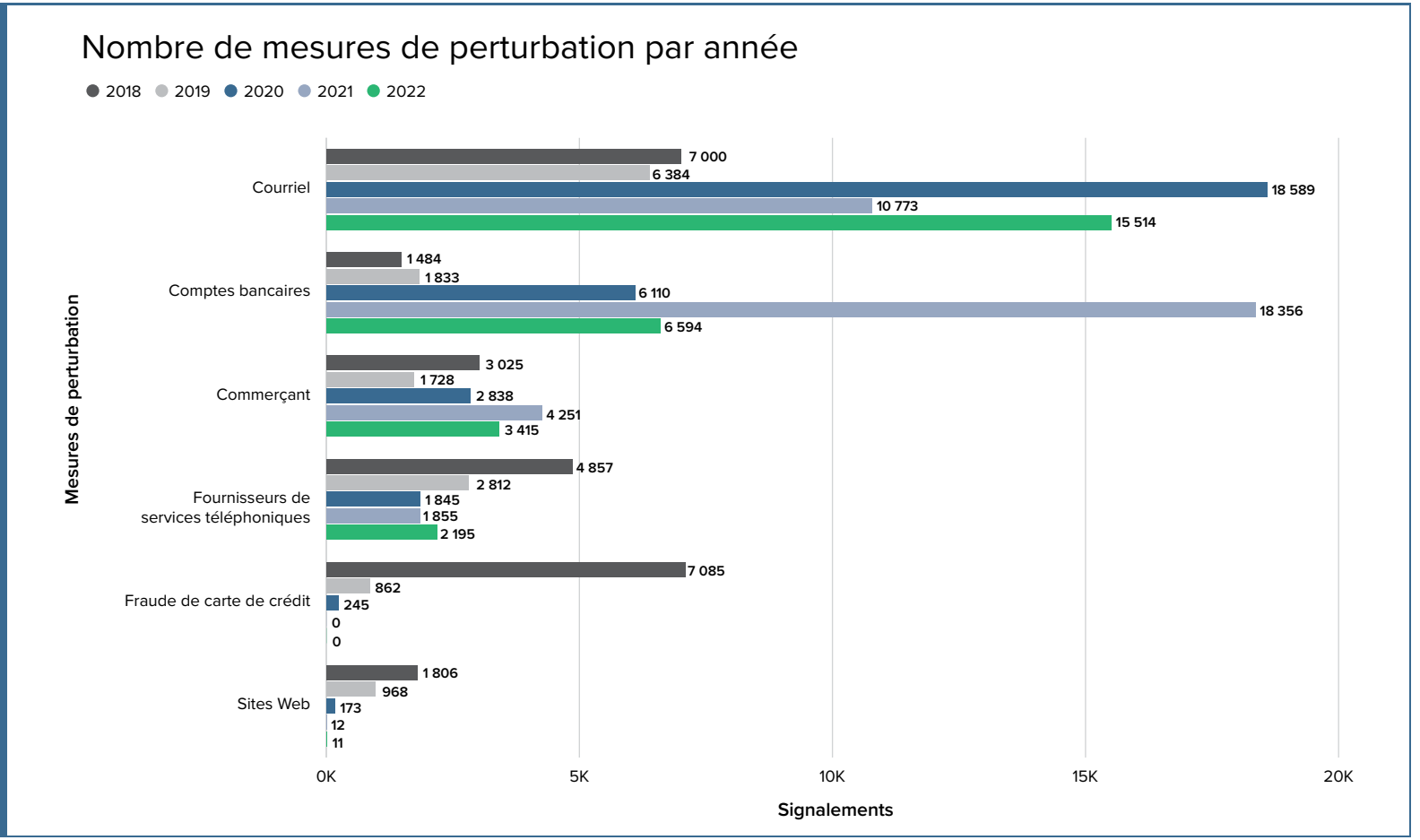
Le Groupe de soutien aux aînés (GSA) du CAFC est composé de bénévoles qui consacrent leurs efforts à réduire l'incidence de la fraude au Canada. Le GSA est une composante essentielle du CAFC, qui conseille, informe et rassure les Canadiens vulnérables ciblés par les fraudeurs. Le GSA reçoit les signalements renvoyés par l'Unité de réception quand celle-ci a déterminé que de l'aide supplémentaire était nécessaire pour une personne âgée ou une personne vulnérable.

En 2022, le GSA a pris en charge 698 signalements et fait 80 présentations, assurant ainsi une sensibilisation et un soutien directs dans l'ensemble du Canada.



Mesures de perturbation

Le CAFC collabore étroitement avec les forces de l'ordre, les partenaires fédéraux et l'industrie pour perturber les activités de fraude. Pour perturber la fraude, le CAFC reçoit et communique des renseignements essentiels tirés des signalements de fraude, collabore avec les partenaires pour retirer des adresses, des comptes bancaires et de crédit, des comptes d'entreprise et des numéros de téléphone frauduleux de leurs systèmes. En 2022, l'objectif opérationnel du CAFC a consisté à neutraliser les adresses courriel, les comptes bancaires, les comptes de commerçant et les numéros de téléphone frauduleux en collaboration avec les fournisseurs de services téléphoniques. Ces efforts jouent un rôle essentiel pour démanteler les infrastructures criminelles qui pourraient être réutilisées pour d'autres victimes. Cette activité crée des obstacles pour le fraudeur et freine les activités criminelles.



Exemples de réussites opérationnelles en collaboration avec les partenaires policiers

Opération Eagle Sweep

Les partenaires policiers nationaux et internationaux sollicitent le soutien du CAFC pour les enquêtes, sous la forme d'un échange d'information et de renseignements provenant de son dépôt de signalements. Les données du CAFC peuvent être intégrées dans des enquêtes plus vastes susceptibles de mener à l'arrestation des fraudeurs et à la cessation d'opérations de fraude.

Par exemple, le CAFC a assuré la coordination de l'opération Eagle Sweep, une enquête internationale sur une opération mondiale de fraude du président dirigée par le Federal Bureau of Investigation (FBI) des États-Unis. Dans ce rôle, le CAFC a coordonné les efforts d'aide des services de police canadiens et a transmis des renseignements sur les victimes canadiennes. L'enquête a abouti à l'arrestation de deux individus au Canada[3].

Arrestations pour fraude au soutien technique transnationale

Les Canadiens continuent d'être touchés par la fraude au soutien technique. Dans ce type d'arnaque, les fraudeurs prennent contact avec les victimes par téléphone, par l'intermédiaire de publicités en ligne ou par courriel, pour les avertir de problèmes avec leur ordinateur. Ces opérations de fraude coordonnées ciblent souvent les aînés ou les victimes vulnérables aux habiletés numériques limitées.

Comme l'observent les forces de l'ordre, les cas de fraude sont souvent reliés à des opérations de fraude internationales ciblant les Canadiens. Pour y remédier, les forces de l'ordre et les partenaires doivent coordonner les efforts, échanger de l'information et collaborer. En 2022 par exemple, le CAFC a participé à une enquête sur une fraude au soutien technique menée par la police régionale de Peel et des forces de l'ordre étatsuniennes et indiennes, qui a conduit à l'arrestation d'une personne au Canada, d'une personne aux États-Unis et de trois personnes en Inde[4].

3 Coordinated Global Operation Disrupted BEC Schemes — FBI [Une opération mondiale perturbe les tentatives de fraude du président]
4 Search Warrant Executed in International Fraud Investigation [Mandat de perquisition exécuté dans le cadre d'une enquête internationale sur la fraude]

Tendances en matière de fraude en 2022

L'environnement numérique continue de favoriser la fraude

Les Canadiens passent toujours plus de temps en ligne. En 2022, 54 % des Canadiens passaient plus de cinq heures par jour en ligne et 24 % entre trois et quatre heures par jour[5]. Plus que jamais, la vie canadienne est intrinsèquement liée au monde numérique.

Les Canadiens utilisent de plus en plus Internet pour faire des achats, comme le montrent les achats en ligne de biens et de services passés de 57,4 milliards de dollars en 2018 à 84,4 milliards de dollars en 2020[6].

Les Canadiens utilisent Internet pour communiquer et entrer en relation les uns avec les autres. Plus de 70 % des Canadiens utilisent les médias sociaux et 76 % communiquent au moyen d'applications de messagerie instantanée[7].

De plus, le télétravail devient rapidement une réalité permanente pour de nombreux travailleurs canadiens. Le tiers des entreprises canadiennes ont offert aux employés la possibilité de télétravailler pendant la pandémie de COVID-19 et cette possibilité pourrait être maintenue au-delà de la pandémie[8].

Le lien étroit continu des Canadiens avec le cyberenvironnement explique qu'un plus grand nombre de Canadiens sont – et continueront d'être – la cible de cybermenaces malveillantes, dont les fraudes et les crimes liés à l'identité.

L'hameçonnage et le harponnage, qui ciblent les adresses courriel professionnelles et organisationnelles et des particuliers, sont les principales méthodes utilisées par les cyberacteurs malveillants pour accéder aux systèmes des entreprises, voler des renseignements personnels et d'entreprise et commettre des fraudes. L'hameçonnage a été le type de fraude le plus souvent signalé au CAFC en 2022, avec plus de 10 600 signalements. Le harponnage est également fortement représenté en 2022, avec plus de 1 500 signalements totalisant des pertes de plus de 58 millions de dollars.

Les fraudeurs qui se livrent à la contrefaçon de marchandises et à la fraude liée aux marchandises utilisent les habitudes d'achat en ligne des Canadiens à leur avantage et adaptent leurs appâts aux nouvelles tendances. Les médias sociaux sont également fortement représentés à titre de plateforme dominante pour diffuser les scénarios de fraude à un vaste sous-ensemble de la population canadienne.

5 Canadian Internet Registration Authority (CIRA) (2022). ***Canada's Internet Factbook 2022*** / L'Autorité canadienne pour les enregistrements Internet (CIRA) (2022). ***Dossier documentaire 2022 sur Internet au Canada***.

6 Statistics Canada. (June 22, 2021) **Canadian Internet Use Survey, 2020**. *The Daily*/Statistique Canada. (22 juin 2021). **Enquête canadienne sur l'utilisation d'Internet, 2020**. *Le Quotidien.*

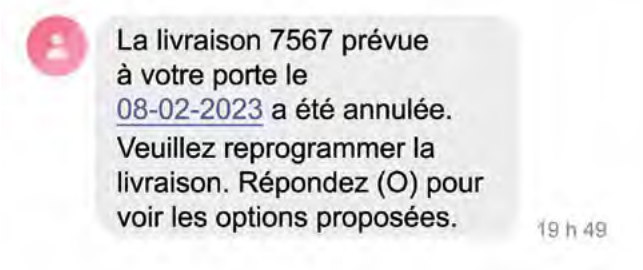
7 Ibid.

8 Statistics Canada. (September 13, 2022). **Digital Technology and Internet Use, 2021**. *The Daily*/Statistique Canada. (13 septembre 2022). **Technologie numérique et utilisation d'Internet, 2021**. *Le Quotidien.*

Méthodes de sollicitation

Le CAFC a constaté que le nombre de signalements par méthode de sollicitation (manière dont le fraudeur entre en contact une première fois avec les victimes) en 2021 est similaire en 2022. Le téléphone et les télécommunications sont demeurés, avec une faible marge, la forme de sollicitation initiale la plus courante, bien que les sollicitations sur Internet signalées aient donné lieu à un nombre plus élevé de victimes.

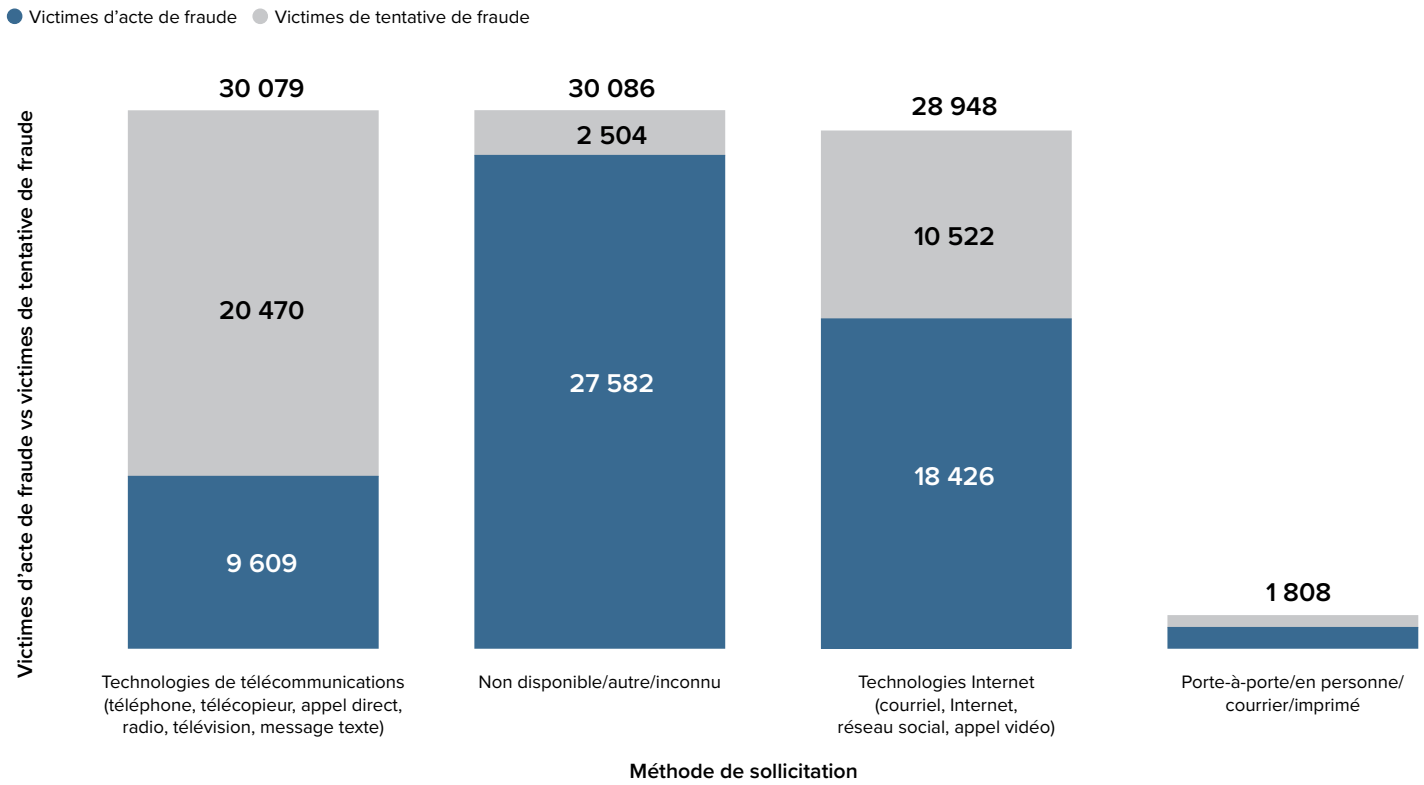
Pour ce qui est des technologies des télécommunications comme méthode de sollicitation, le CAFC continue de voir se répandre l'utilisation des textos par les fraudeurs pour communiquer avec les victimes potentielles.



Les opérations de fraude utilisent des services et des technologies de messagerie texte automatisée pour diffuser des messages frauduleux à un grand nombre de Canadiens à des coûts opérationnels extrêmement faibles.

Dans l'exemple ci-contre, si le destinataire répond au message (sous n'importe quelle forme), le texte est suivi d'un appel du fraudeur qui vise à poursuivre son offensive.

Victimes de tentative de fraude vs victimes d'acte de fraude par méthode de sollicitation



Les statistiques sur les méthodes de sollicitation de 2021 sont en grande partie similaires en 2022. Toutefois, les signalements faisant état de l'utilisation des technologies Internet comme moyen de sollicitation initial sont associés à un nombre beaucoup plus élevé de victimes. Les fraudes par téléphone sont souvent plus intrusives et dérangeantes que les escroqueries sur Internet, par conséquent les personnes sont plus enclines à signaler les tentatives de fraude par téléphone que celles sur Internet.

Fraude sur les médias sociaux

Les Canadiens passant beaucoup de temps sur des sites comme Facebook, Twitter, Instagram et TikTok, les fraudeurs et les cyberacteurs malveillants utilisent ces sites pour lancer de nombreuses formes de fraude. Compte tenu de la quantité massive d'information régulièrement affichée sur ces sites, les utilisateurs ont de plus en plus de mal à faire la distinction entre les comptes, les pages, les publicités et les conversations légitimes et frauduleux. Comme la plupart des plateformes de médias sociaux sont gratuites, elles offrent une méthode peu coûteuse pour les fraudeurs pour tromper les Canadiens.

Les Canadiens mettant de plus en plus de renseignements personnels en ligne et communiquant avec leurs groupes d'amis sur les sites de médias sociaux, les fraudeurs et les auteurs de menaces sont en mesure de trouver des renseignements détaillés pour personnaliser des tentatives de fraude à leur encontre.

Grâce aux mentions j'aime, aux abonnements, aux gazouillis partagés et aux commentaires qui sont publics, les fraudeurs peuvent acquérir une bonne connaissance des habitudes sociales des personnes. Ils sont en mesure de trouver l'ami proche d'un utilisateur et d'en apprendre davantage sur ses relations et ses centres d'intérêt. Parmi les renseignements figurent, entre autres, les emplois antérieurs, les écoles fréquentées, la ville d'origine et les lieux de résidence. Ces renseignements constituent un contexte parfait pour les fraudeurs pour lancer des formes de fraude complexes et sophistiquées.

Par exemple, les Canadiens utilisent des sites comme LinkedIn pour présenter leur cheminement professionnel et chercher un emploi. Les fraudeurs profitent du site pour créer de faux profils LinkedIn de gestionnaire recruteur ou d'employé au sein d'une entreprise pour pouvoir ensuite envoyer des messages directs spontanés et interagir avec les internautes. Le site ouvre la voie aux escroqueries liées à l'emploi, à d'autres formes de fraude et au recrutement de mules[9]. Autre exemple, les fraudeurs peuvent facilement se faire passer pour des amis, des collègues et des connaissances en ligne, surtout si des renseignements personnels sont accessibles. L'imposture peut créer une illusion de confiance et permettre d'exploiter le groupe d'amis élargi.

Les jeunes ont tendance à participer aux médias sociaux, beaucoup plus que tout autre groupe d'âge. En 2022, le CAFC a relevé une tendance alarmante à la fraude favorisée par ces plateformes, en particulier à l'encontre des personnes de moins de 30 ans. Le CAFC invite les Canadiens à s'informer sur les menaces potentielles en ligne et encourage les parents à en discuter avec leurs enfants.

9 Bond, Shannon. (27 mars 2022) **« That Smiling LinkedIn Profile Face Might be a Computer Generated Fake » [Ce visage souriant de profil LinkedIn pourrait être un faux généré par ordinateur]** NPR.

TÉMOIGNAGE D'UN SIGNALEMENT DE FRAUDE SUR LES MÉDIAS SOCIAUX

« Une amie sur Instagram m'a fait parvenir un message direct pour me demander si je souhaitais investir dans les bitcoins et m'expliquer qu'une de ses amies pouvait m'aider. J'ai créé un compte Shakepay pour pouvoir envoyer les fonds de mes comptes bancaires personnels à un site Web de négociation.

La personne m'a montré comment acheter des fractions de bitcoin et les soumettre à mon compte de titres, et j'ai transféré de l'argent de mon compte personnel sur Shakepay à une adresse de portefeuille de cryptomonnaies. La personne m'a dit que j'avais fait un profit, alors j'ai demandé à effectuer un retrait pour voir. La personne m'a alors expliqué que j'avais besoin d'un NIP qui nécessiterait des frais. En suivant le même processus, j'ai envoyé de l'argent pour obtenir le NIP.

Puis on m'a dit que pour retirer le montant souhaité, j'avais besoin de relever le niveau de mon compte de titres. J'ai donc utilisé le même processus à l'aide de Shakepay pour envoyer les fonds. J'ai envoyé de l'argent à partir de mes comptes chèques et d'une ligne de crédit.

Peu après, j'ai réalisé qu'il y avait quelque chose de louche lorsqu'on m'a dit qu'il n'était pas possible de me faire parvenir les fonds, car il y avait des frais de commission à payer.

Ce matin, j'ai encore reçu un message me disant qu'il existait un moyen d'obtenir mes fonds sans payer les frais de 4500 $. Un lien par texto m'a également été envoyé et j'ai vu tout de suite que les fraudeurs essayaient d'accéder à mon téléphone. Je n'ai pas répondu à la sollicitation et j'ai changé mon mot de passe. J'ai communiqué avec l'amie qui m'avait référé le gestionnaire de compte et elle a publié une story sur son Instagram expliquant qu'elle avait fait l'objet d'un piratage. »

Comment se protéger contre les fraudes sur les médias sociaux

- Examinez et mettez à jour fréquemment vos paramètres de confidentialité et de compte afin de limiter la quantité d'information accessible sur l'Internet ouvert.
- Ne répondez pas aux sollicitations d'une personne que vous ne connaissez pas et, dans la mesure du possible, assurez-vous d'être en mesure de vérifier l'identité de la personne à qui vous parlez.
- Ne communiquez jamais de renseignements personnels et n'envoyez jamais d'argent en ligne à une personne que vous ne connaissez pas et, dans la mesure du possible, vérifiez l'authenticité des produits ou des services pour lesquels vous versez de l'argent en ligne.
- Recherchez les comptes doubles pour vous assurer que votre compte n'est pas usurpé.
- Restez à l'affut des nouvelles fraudes sur les médias sociaux partagées sur le **site Web du CAFC.**

Comment les fraudeurs utilisent les médias sociaux

- Afficher des publicités frauduleuses, inciter les utilisateurs à communiquer avec eux ou à cliquer sur des liens vers des sites Web frauduleux.
- Exploiter de faux comptes ou des comptes robots, utiliser des processus automatisés pour communiquer avec les utilisateurs par le biais de messages directs.
- Gérer des groupes ou des pages Web frauduleux sur des plateformes de médias sociaux.
- Vendre des biens et des services contrefaits ou inexistants, faciliter la fraude liée aux marchandises.
- Établir un contact avec les utilisateurs à l'aide de scénarios et de thèmes de fraude précis (p. ex., fraude liée à un stratagème de rencontre sur des sites de rencontre).
- Utiliser les médias sociaux comme plateforme pour établir un premier contact avec les victimes potentielles.

Fraude liée aux cryptomonnaies et à l'investissement

Les cryptomonnaies offrent un moyen rapide, facile et efficace de transférer de l'argent dans le monde entier. Les marchés de cryptomonnaies canadiens et internationaux, ainsi que les guichets automatiques de cryptomonnaies, facilitent l'échange et le transfert de cryptomonnaies et d'espèces.

Si cela est avantageux pour les utilisateurs respectueux des lois, les cryptomonnaies sont demeurées un puissant catalyseur de la fraude en 2022. Les cryptomonnaies représentent le deuxième mode de paiement le plus utilisé pour la fraude en 2022 et ce mode de paiement continue de croître à un rythme très rapide par rapport aux autres modes de paiement. En 2022, le CAFC a reçu 5 281 signalements de fraude liée aux cryptomonnaies totalisant 125,9 millions de dollars de pertes, et les cryptomonnaies prédominent dans les cas de fraude impliquant des pertes élevées.

Les cryptomonnaies sont souvent utilisées de manière anonyme, et la probabilité de récupérer les cryptomonnaies perdues à la suite d'une fraude est nettement plus faible qu'avec les autres modes de paiement. De plus, les transactions en espèces ou les virements télégraphiques inhabituels sont plus susceptibles d'être signalés comme potentiellement frauduleux et d'être gelés que les échanges de grandes quantités de cryptomonnaies.

Les cryptomonnaies constituent de loin le mode de paiement le plus couramment utilisé dans la fraude à l'investissement.

Modes de paiement de la fraude à l'investissement

Type de fraude Modes de paiement	Investissement	
	N^{bre} du mode de paiement*	Perte en dollars
Cryptomonnaies	2851	$96,731,847
Non précisé et autre	1898	$115,620,554
Virement électronique	1430	$24,556,346
Virement télégraphique	579	$63,739,890
Carte de crédit	438	$571,200
Carte de débit	114	$107,497
Retrait bancaire automatique	88	$827,591
Service de paiement par Internet (p. ex. Paypal)	80	$257,819
Dépôt direct	71	$1,868,791
Chèque/mandat/traite bancaire	59	$4,029,386
Argent comptant	38	$576,972
Carte prépayée	17	$1,550
Western Union	11	$33,078
Ria financial	7	$36,680
MoneyGram	5	$17,950
Marchandises	2	$0
Transfast	2	$66
Transfert d'argent par Vigo	1	$0
Total	**7691**	**$308,977,217**

* Notez que chaque rapport reçu peut avoir plus d'un mode de paiement.

Le CAFC continue d'observer une tendance à la fraude à l'investissement en cryptomonnaies. En 2021, le CAFC a indiqué que la fraude à l'investissement en cryptomonnaies domine dans les signalements et entraîne des pertes et un nombre de victimes importants. En 2022, le CAFC a reçu 2 851 signalements de fraude à l'investissement en cryptomonnaies, soit de loin le type d'escroquerie liée aux investissements le plus répandu. La perte moyenne par victime de fraude à l'investissement est également plus élevée que pour la plupart des autres formes de fraude touchant des personnes, avec une perte moyenne déclarée de plus de 72 000 $.

Avec la croissance des finances décentralisées et des applications et plateformes d'investissement accessibles, les Canadiens sont de plus en plus enclins à investir en ligne. En outre, la promesse de rendements élevés et l'apparence de légitimité font que les Canadiens perdent plus d'argent que jamais dans la fraude à l'investissement. En 2022, le CAFC a reçu 4 671 signalements de fraude à l'investissement, qui ont entraîné des pertes totales d'environ 309 millions de dollars.

Les fraudes à l'investissement sont souvent lancées dans des publicités sur les médias sociaux, dans des vidéos ou par le biais de conversations sur les sites Web. De faux avis en ligne sont également utilisés pour donner une apparence de légitimité.

Bien que les escroqueries liées aux investissements en cryptomonnaies utilisent fréquemment des noms généraux comme « Bitcoin-Unlocked-Finance », les fraudeurs à l'investissement se font également passer pour des institutions financières et des entreprises canadiennes connues et réputées pour créer un sentiment de confiance. Il peut s'agir d'usurpation de sites Web et de coordonnées, ou de création de sites Web qui ressemblent à de vrais sites.

TÉMOIGNAGE D'UN SIGNALEMENT DE FRAUDE À L'INVESTISSEMENT

« J'ai entendu une publicité dans un balado que je reçois régulièrement par courriel. Une nouvelle forme d'opération de négociation avait été créée, et il était possible d'acheter dans les pays avec Internet haute vitesse et de vendre dans les pays avec Internet basse vitesse avant que les prix changent sur le graphique.

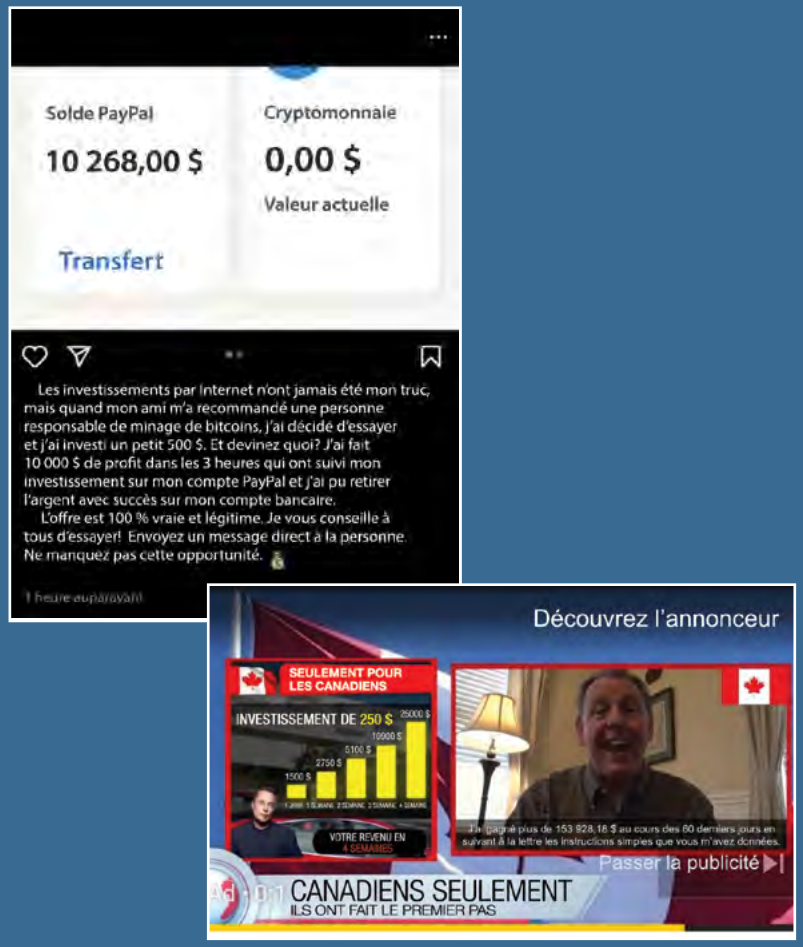
J'ai communiqué avec l'entreprise concernée le 22 août et je me suis inscrit moyennant un paiement de 250 $ par carte de crédit. Mon compte a commencé à afficher de bons pourcentages, alors j'ai investi davantage.

Le conseiller personnel me proposait quotidiennement d'investir plus d'argent pour effectuer des gains plus importants. J'avais fait de la spéculation sur séance pendant 22 mois par moi-même, et les transactions du conseiller me paraissaient légitimes. Je pouvais les suivre en regardant le graphique. J'ai fini par investir 8 500 $ en tout dans le compte.

Le conseiller s'est mis à m'appeler à répétition pour me pousser à emprunter de l'argent pour investir davantage. C'est à ce moment-là que j'ai réalisé que je pouvais être victime d'une escroquerie.

J'ai demandé à fermer mon compte et à récupérer mon argent. Personne ne répondait à mes appels ou à mes courriels. Quand j'ai appelé à partir d'un autre téléphone que le mien, une personne a pris l'appel puis a immédiatement raccroché. »

Les fraudeurs à l'investissement utilisent les publicités émises en continu et les médias sociaux pour diffuser les tentatives de fraude. Ce type de fraude comprend le piratage et l'usurpation de comptes d'utilisateurs réels pour faire parvenir des sollicitations aux amis et aux abonnés de ces utilisateurs.



Fraude à la récupération d'argent

Étroitement liée aux escroqueries à l'investissement et à la fraude liée aux cryptomonnaies, la fraude à la récupération d'argent a lieu après qu'une personne a déjà été escroquée. La victime est contactée par un fraudeur qui lui promet qu'elle récupérera l'argent perdu moyennant des frais. Dans certains cas, les fraudeurs déclarent avoir remarqué un « compte dormant inutilisé » et proposent leur aide pour restituer l'argent. Les victimes sont invitées à payer des frais avant de recevoir les services. En 2022, le CAFC a reçu 221 signalements de fraude à la récupération d'argent totalisant des pertes de 2,5 millions de dollars.

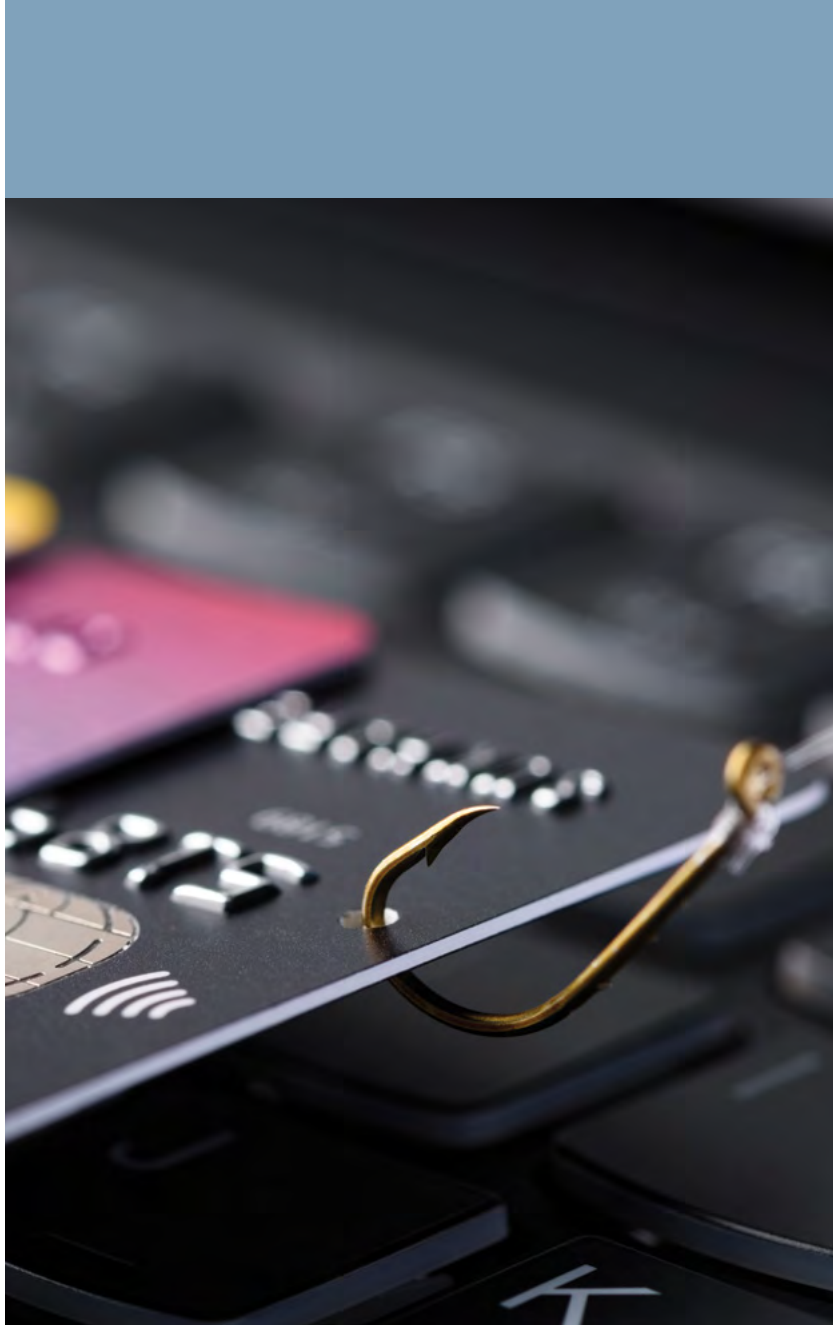
Dans de nombreux cas, la fraude à la récupération d'argent est reliée à la fraude initiale, et il s'agit pour les fraudeurs de poursuivre l'acte de fraude. Le fraudeur peut connaître le montant d'argent perdu et d'autres renseignements personnels. Les fraudeurs, souvent, proposent d'autres types de fraude et d'escroqueries à la récupération d'argent pour continuer de dépouiller la victime. Les fraudeurs utilisent également de nouvelles coordonnées pour dissimuler leur lien avec la fraude précédente.

Hameçonnage, fraude à l'identité et vol d'identité

L'hameçonnage est l'un des types de fraudes les plus souvent signalés. Sous la forme de messages textes ou de courriels demandant de répondre ou de cliquer sur un lien, ces tentatives servent à lancer d'autres formes de fraude, à voler des renseignements personnels ou à installer des logiciels malveillants et des virus. En 2022, le CAFC a reçu 10 647 signalements d'hameçonnage.

Les tentatives d'hameçonnage permettent au fraudeur d'obtenir des renseignements personnels comme des copies de permis de conduire, des cartes d'assurance maladie et des numéros d'assurance sociale (NAS), ainsi que des renseignements financiers comme les numéros de cartes de crédit et l'information sur les comptes bancaires. L'hameçonnage est donc étroitement lié au vol d'identité et à la fraude. Par ailleurs, l'hameçonnage entraînant l'installation de logiciels malveillants sur des appareils électroniques peut également conduire au vol de renseignements personnels à l'insu de la victime.

L'année 2022 a vu augmenter la diffusion à grande échelle de textos automatisés, les opérations de fraude attendant ensuite une réponse pour rappeler la victime. Le CAFC a observé une augmentation des signalements de vol d'identité et de fraude, avec 19 543 signalements en 2022. Les aînés et les populations vulnérables sont particulièrement vulnérables au vol d'identité et à la fraude. En 2022, le CAFC a reçu 2 510 signalements de victimes de plus de 60 ans.



TÉMOIGNAGE D'UN SIGNALEMENT D'HAMEÇONNAGE

« J'ai reçu un courriel d'hameçonnage soi-disant de ma compagnie émettrice de cartes de crédit. La bannière et l'aspect général du courriel paraissaient 100 % légitimes, y compris les logos et la police de caractères.

J'avais déjà reçu des courriels de leur part, mais je ne me souvenais de leur présentation. La compagnie expliquait qu'elle venait de mettre à jour nos cartes et l'image de marque, et j'ai donc pensé que le courriel faisait partie de ces changements. Le message était désigné comme étant urgent, alors j'ai cliqué sur le lien joint, qui m'a redirigé vers un lien Amazon. Je me suis demandé si c'était une erreur de ma part, alors j'ai cliqué de nouveau sur le lien, qui m'a de nouveau dirigé vers le même lien Amazon.

Le 2 décembre 2022, ma compagnie émettrice de cartes de crédit m'a appelé pour m'informer d'une utilisation de ma carte de crédit avec des montants inhabituels. Nous avons alors découvert que ma carte de crédit avait été utilisée, nous avons cherché la manière dont cela avait pu se produire et nous nous sommes rendu compte que la fraude avait été réalisée grâce au courriel que j'avais reçu. »

Harponnage

Le harponnage est la version ciblée de l'hameçonnage. Dans le cas du harponnage, les fraudeurs et les cybercriminels ciblent des victimes particulières au moyen de tentatives d'hameçonnage précises. Si l'hameçonnage consiste la plupart du temps à diffuser des appâts généraux à de nombreuses victimes potentielles, le harponnage vise à envoyer de l'information personnalisée à un public précis dans le but de faire des gains plus importants.

Ciblant les entreprises, les organisations gouvernementales et publiques et les particuliers, le harponnage est une forme de crime financier qui se répand et gagne en importance. En 2022, le CAFC a reçu 1 548 signalements de harponnage totalisant des pertes de 58,1 millions de dollars, comparativement à 1 852 signalements et à 54 millions de dollars de pertes en 2021.

Le harponnage est une menace susceptible de conduire à des pertes importantes pour les organisations et les particuliers. La plupart des entreprises, en particulier les petites et moyennes entreprises (PME), publient de l'information accessible sur leur mandat, leurs pratiques commerciales, les services offerts et les noms, titres, adresses courriel et responsabilités des membres de leur direction. Les opérations de fraude peuvent également extraire des renseignements sur certains employés sur leurs pages de média social ou leurs blogues. Toutes ces données clés peuvent être exploitées pour créer des tentatives de harponnage précises.

Bien que des renseignements subtils et détaillés puissent accroître les risques d'être victime de harponnage, les signalements tendent à montrer que les attaques de harponnage sont menées à l'aide de renseignements limités et d'information de base trouvée en ligne.

Les entreprises s'appuient sur d'autres entreprises pour soutenir leur organisation, qu'il s'agisse de la fourniture d'équipement et du soutien logistique ou de la mise en œuvre de logiciels et de matériel. Les entreprises s'échangent souvent des coordonnées, des renseignements financiers et d'autres informations précises avec différents fournisseurs et sociétés associés.

Une attaque de harponnage peut commencer par un cyberincident malveillant contre l'une de ces entreprises reliées, lequel entraîne le vol des renseignements des clients ou des partenaires. Une fois volés, les renseignements peuvent être utilisés pour créer une tentative de harponnage sophistiquée contre les entreprises associées, surtout si la société ne s'est pas aperçue que ses renseignements avaient été volés précédemment. Les tentatives de harponnage qui ciblent des organisations, en particulier lorsqu'elles sont en lien avec le fonctionnement de l'entreprise ou le paiement de factures, sont également appelées fraudes du président.

TÉMOIGNAGE D'UN SIGNALEMENT DE HARPONNAGE

« J'ai reçu un courriel de notre fournisseur avec une facture jointe auquel j'ai répondu par "merci". Il s'agit d'une situation normale et fréquente. Quelques jours plus tard, nous recevions une réponse à ce courriel de la part de la même personne nous demandant quand le paiement serait effectué. J'ai répondu que la facture serait payée la semaine suivante et que nous ferions également un suivi une fois celle-ci payée.

Une semaine plus tard, nous recevions un courriel de notre fournisseur nous indiquant qu'il avait récemment changé de coordonnées bancaires et qu'il fallait que tous les prochains paiements soient effectués sur le nouveau compte. Le courriel comportait la signature de la personne avec qui nous traitions habituellement et les mêmes renseignements qui accompagnaient la signature habituelle de cette personne.

Nous avons retourné un formulaire à la bonne adresse électronique, en exigeant la signature d'un représentant autorisé. Le formulaire a été rempli avec tous les détails et renvoyé avec la signature du représentant et un chèque annulé, ce qui est également requis. Nous avons mis à jour nos renseignements bancaires et payé la dernière facture à cette entreprise par dépôt direct.

J'ai reçu une autre facture par courriel sept jours plus tard provenant de la même adresse électronique et j'ai répondu par un autre "merci". Les deux factures étaient correctes et étaient envoyées par la bonne personne. Plus tard cette semaine-là, j'ai reçu une réponse au courriel avec la facture, en provenance de la même adresse électronique, me demandant quand le paiement de cette facture serait effectué. Le message contenait également la bonne adresse électronique, le bon numéro de facture et la signature accompagnée des renseignements de la personne avec qui nous avions l'habitude de travailler. J'ai répondu qu'un avis de paiement devrait leur parvenir, probablement le lendemain. Nous avons également payé cette facture.

Une semaine plus tard, nous avons reçu un courriel provenant de la même adresse électronique indiquant que l'entreprise venait de découvrir que ses comptes de courriel avaient été piratés et qu'elle n'avait jamais envoyé de courriel relatif à un changement de renseignements bancaires. »

Extorsion

L'extorsion consiste à obtenir de l'argent par le biais de menaces ou d'intimidation. L'extorsion continue d'être l'une des formes de fraude les plus souvent signalées au CAFC. En 2022, le CAFC a reçu 8 266 signalements d'extorsion, pour des pertes totales d'environ 19 millions de dollars. Bien que le nombre de signalements d'extorsion au CAFC ait diminué depuis 2018, les pertes financières et les pertes par victime ont augmenté de manière constante en 2022.

En 2022, le CAFC a observé une tendance à l'extorsion ciblant des groupes particuliers de Canadiens. Par exemple, les aînés sont ciblés par des menaces directes de leur nuire et de nuire aux membres de leur famille.

Dans d'autres cas, le fraudeur a recours à la menace si les personnes ne répondent pas à la tentative de fraude initiale. Des renseignements comme les adresses personnelles, les noms des membres de la famille ou d'autres renseignements personnels pouvant effrayer les victimes potentielles sont utilisés dans les extorsions.

Sextorsion

L'extorsion et la sextorsion en ligne ont continué d'avoir des répercussions en 2022. La sextorsion, ou l'exploitation sexuelle en ligne, consiste à tromper ou à pousser une victime à participer à des situations en ligne de nature sexuelle ou à les observer. Ces situations sont ensuite enregistrées ou filmées à l'insu de la victime. Le fraudeur menace d'envoyer le matériel enregistré à des amis, à des membres de la famille ou à des collègues de travail de la victime si celle-ci n'envoie pas de l'argent ou des images supplémentaires.

Les médias sociaux permettent aux fraudeurs de se familiariser avec les cercles sociaux d'une personne et de communiquer avec les victimes potentielles. Les plateformes de médias sociaux sont couramment utilisées dans la sextorsion.

En 2022, le CAFC a observé une augmentation des signalements de sextorsion ciblant les adolescents et les jeunes, notamment par l'intermédiaire des jeux vidéo en ligne, des groupes de clavardage et des médias sociaux. Les auteurs de menaces peuvent se faire passer pour des personnes plus jeunes afin de gagner lentement la confiance de la victime ou d'entamer une relation virtuelle.

Comme l'extorsion et d'autres formes de fraude, la sextorsion peut isoler et traumatiser la victime. Cette expérience pénible amène la victime à payer le fraudeur et à avoir peur de signaler le problème ou d'en parler à un parent ou à un tuteur. Malheureusement, payer n'est jamais une solution. Une fois que la personne a payé, elle fait l'objet de menaces continues.

Comme ce type de fraude vise les jeunes Canadiens et les adolescents, il est important que les parents et les enfants soient sensibilisés à cette menace en ligne. Pour obtenir de plus amples renseignements sur la sextorsion et pour signaler les cas d'enfants victimes sur Internet, veuillez consulter le Centre canadien de protection de l'enfance (CCPE).

TÉMOIGNAGE D'UN SIGNALEMENT DE SEXTORSION

« La communication a commencé sur Messenger après que j'ai reçu une demande d'ami Facebook. Nous avions tous les deux des amis en commun, alors j'ai accepté la demande.

La discussion est rapidement devenue explicite et a abouti à un appel vidéo au cours duquel la personne m'a filmé nu. Immédiatement elle m'a demandé 15 000 $, sinon elle détruirait ma vie. Elle m'a demandé d'envoyer un texto à un autre numéro de téléphone et a continué de me harceler et de me menacer.

J'ai envoyé 250 $ en espérant qu'on me laisse tranquille. Mais ça n'a pas marché, et la personne a commencé à me menacer de faire parvenir des images et des vidéos à ma famille et à mes amis si je n'envoyais pas plus d'argent. Le fraudeur a continué le lendemain et a envoyé des images sur Messenger à un grand nombre de mes contacts ainsi qu'à ma femme et à mon lieu de travail. Cet événement a généré de l'animosité entre ma femme et moi, et m'a mis dans l'embarras devant de nombreuses personnes qui me respectaient. »

Types de fraudes les plus courantes selon l'âge and les pertes monétaires

Tranche d'âge	Nbre de signalements	Nbre de victimes	% de victimes
19 ans et moins			
Extorsion	247	183	74,1 %
Fraude à l'identité	723	720	99,6 %
Renseignements personnels	290	281	96,9 %
20 - 29			
Extorsion	947	535	56,5 %
Fraude à l'identité	2 733	2 718	99,5 %
Renseignements personnels	1 074	952	88,6 %
30 - 39			
Fraude à l'identité	4 946	4 929	99,7 %
Renseignements personnels	1 572	1 410	89,7 %
Hameçonnage	1 074	390	36,3 %
40 – 49			
Fraude à l'identité	3 762	3 752	99,7 %
Renseignements personnels	1 251	1 060	84,7 %
Hameçonnage	996	328	32,9 %
50 – 59			
Fraude à l'identité	2 220	2 208	99,5 %
Renseignements personnels	1 026	789	76,9 %
Hameçonnage	1 120	308	27,5 %
60 ans et plus			
Extorsion	2 194	475	21,6 %
Fraude à l'identité	2 510	2 497	99,5 %
Hameçonnage	2 415	601	24,9 %

Tranche d'âge	Nbre de signalements	Perte en dollars	Perte moyenne en dollars par victime
19 ans et moins			
Extorsion	247	1 573 480 $	8 598 $
Investissement	43	346 463 $	9 624 $
Marchandises	112	114 775 $	1 148 $
20 - 29			
Extorsion	947	3 784 729 $	7 074 $
Investissement	411	6 324 110 $	16 730 $
Emploi	649	801 666 $	1 681 $
30 - 39			
Investissement	589	22 392 456 $	41 163 $
Marchandises	601	1 007 616 $	2 052 $
Stratagème de rencontre	133	3 274 550 $	34 110 $
40 – 49			
Investissement	630	43 238 558 $	74 293 $
Emploi	237	1 800 264 $	11 615 $
Stratagème de rencontre	168	10 836 571 $	84 004 $
50 – 59			
Investissement	582	72 710 657 $	133 170 $
Stratagème de rencontre	203	11 451 380 $	73 880 $
Service	648	1 441 000 $	2 888 $
60 ans et plus			
Investissement	858	78 760 257 $	95 583 $
Stratagème de rencontre	351	19 524 955 $	67 327 $
Service	2 130	8 566 972 $	5 148 $

L'extorsion et la sextorsion ciblant les personnes de moins de 30 ans sont une tendance continue, qui a donné lieu à un nombre accru de signalements et aux pertes les plus importantes pour ce groupe d'âge en 2022.

Extorsion ciblant des groupes ethniques particuliers

Le CAFC a observé des signalements ciblant des groupes ethniques précis au Canada. Cette forme d'extorsion étant souvent perpétrée dans la langue maternelle des victimes, les fraudes peuvent être réalisées dans la région d'origine de la personne ciblée. Par exemple, le CAFC a observé des actes d'extorsion visant des étudiants étrangers utilisant des menaces d'expulsion ou de refus de permis d'études ou de travail.

Comme dans les autres formes de fraude, les extorqueurs ciblent les victimes à l'aide de scénarios de fraude susceptibles de déclencher une réponse ou une réaction immédiate. La probabilité est grande que les nouveaux arrivants au Canada soient préoccupés par les questions de citoyenneté, d'immigration ou de permis et les fraudeurs exploitent cette préoccupation pour tenter de les escroquer.

Besoin urgent d'argent et arnaque des grands-parents

Une fraude du besoin urgent d'argent consiste pour le fraudeur à communiquer avec une victime potentielle, souvent par téléphone ou par ligne terrestre, et à lui faire croire qu'un membre de sa famille est arrêté, blessé, à l'hôpital ou en danger. Le fraudeur peut se faire passer pour un parent de la victime et jouer sur ses émotions pour la presser de payer des frais urgents afin d'éviter une poursuite, de participer à une défense ou de payer des factures médicales, entre autres scénarios. La personne au téléphone explique en général qu'une « consigne de silence » a été imposée et recommande de ne parler de la situation à personne dans le but d'isoler la victime et d'accroître les chances de réussite de la fraude.

Une variante de la fraude du besoin urgent d'argent, qui est devenue très fréquente en 2022, est « l'arnaque ou la fraude des grands-parents ». Il s'agit de fraudes du besoin urgent d'argent qui ciblent les personnes âgées. Les fraudeurs se font passer pour les petits-enfants ou une personne appelant les victimes au nom de leurs petits-enfants. Les personnes âgées, souvent réticentes à mettre fin à la conversation ou à raccrocher rapidement, donnent aux fraudeurs plus de temps pour exercer une pression et les convaincre.

Les aînés et les populations vulnérables sont particulièrement sensibles aux pressions ou menaces excessives déployées par les fraudeurs, lesquels peuvent harceler les personnes âgées d'appels en urgence à tout moment du jour et de la nuit avec des numéros de téléphone différents dans le but de les désorienter et de les effrayer encore plus. En 2022, le CAFC a reçu de nombreux signalements de victimes âgées qui ont d'abord ignoré ces formes d'escroquerie, avant de finir par payer à la suite des appels, des menaces et du harcèlement insistants des fraudeurs.

En 2022, le CAFC a reçu 2 494 signalements de fraude de besoin urgent d'argent qui représentent 9,4 millions de dollars de pertes. En comparaison, le CAFC avait reçu 1 106 signalements totalisant des pertes de 2,4 millions de dollars en 2021. Les personnes âgées sont fortement touchées par la fraude du besoin urgent d'argent, avec des pertes de 7,7 millions de dollars pour 1 672 signalements.

Dans les fraudes du besoin urgent d'argent et les fraudes des grands-parents, le CAFC observe une augmentation des contacts directs entre les associés à la fraude et les victimes. Les fraudeurs se présentent notamment chez les victimes pour récupérer l'argent et les aider à se rendre à la banque[10]. Les fraudeurs encouragent également les victimes à envoyer de l'argent comptant dans des colis par la poste.

Malgré les défis posés par ce type de fraude, les policiers parviennent à trouver et à arrêter les fraudeurs qui se trouvent au Canada. Par exemple :

- Le Service de police de la Ville de Montréal (SPVM) a procédé à l'arrestation de quatre individus responsables de plus de 100 signalements de fraude à l'encontre des aînés dans différents quartiers montréalais[11].
- La police régionale de York a arrêté deux personnes associées à quatre victimes de fraude des grands-parents dans la région[12]. Comme nous l'avons mentionné précédemment dans le présent rapport, les opérations de fraude massives ont de plus en plus souvent recours à des associés situés au Canada pour réaliser une partie de la fraude

Lorsque la fraude est signalée rapidement et qu'un modèle de fraude est établi, le CAFC et les partenaires policiers peuvent venir en aide aux victimes de la fraude.

10 For example : **« Grandparent scams: police officers have arrested two suspects targeting seniors »** / Par exemple : **« Fraude des grands-parents : les policiers arrêtent deux suspects ciblant des aînés »**

11 **"SPVM makes arrests in seniors fraud cases"**/**« Fraudes visant les aînés : le SPVM arrête quatre suspects »**

12 **« York Regional Police charge two people after woman loses $19K in grandparent scam » [La police régionale de York porte des accusations contre deux personnes après qu'une femme a perdu 19 000 $ dans une fraude des grands-parents]**

TÉMOIGNAGE D'UN SIGNALEMENT DE FRAUDE DE BESOIN URGENT D'ARGENT ET DES GRANDS-PARENTS

« Mon père a reçu un appel l'informant que mon fils avait eu un accident de voiture et qu'on avait trouvé de la drogue sur lui. Les fraudeurs ont ensuite passé à mon père un enfant au téléphone qui disait "Sors-moi d'ici, c'est horrible". Pour le sortir d'affaire, mon père devait verser 12 000 $. Un collecteur de fonds est venu chercher l'argent à son domicile.

Les mêmes fraudeurs ont de nouveau appelé, réclamant 12 000 $ de plus pour les procédures judiciaires et les frais d'avocat. Quelques jours plus tard, un autre messager est venu récupérer l'argent chez mon père.

Environ une semaine plus tard, ils ont demandé 5000 $ supplémentaires. Mon père a envoyé l'argent dans un colis par service de messagerie.

Une semaine après le contact précédent, les fraudeurs ont demandé 7000 $ de plus. Quand mon père a refusé, l'homme est devenu extrêmement violent et l'a menacé, lui et sa famille. Mon père avait très peur, alors il a de nouveau envoyé de l'argent par courrier à une autre adresse. Mon père nous voyait tous les jours mon fils et moi pendant la fraude, mais il ne nous a jamais rien dit par crainte des représailles. Les fraudeurs le menaçaient et il craignait pour sa vie et pour la nôtre.

Plus tard ce mois-là, mon frère a appelé mon père pour le mettre en garde contre les fraudes des grands-parents et mon père s'est alors confié à la famille.

Les harceleurs ont continué d'appeler mon père qui a refusé de leur obéir. Ils ont dit à mon père qu'il devait envoyer de l'argent rapidement, sinon on irait chercher mon fils à l'école et on l'arrêterait. Mon père a continué de s'opposer à leurs demandes et leur a dit que quelqu'un allait s'occuper de cette affaire pour lui. Les fraudeurs ont poursuivi leur harcèlement et leurs menaces; ils ont même appelé alors que nous nous trouvions au poste de police pour déposer un signalement. Mon père vit encore aujourd'hui dans la peur de ce que les fraudeurs pourraient faire. »

Stratagème de rencontre

Compte tenu de l'essor des sites Web et des applications de rencontre en ligne, les Canadiens sont susceptibles de nouer des relations amoureuses en ligne avec des personnes qu'ils n'ont jamais rencontrées directement ou qui ne se trouvent pas au Canada. En trouvant l'amour sur un site ou une application de rencontre, dans les médias sociaux ou par d'autres moyens, les Canadiens peuvent être victimes d'un stratagème de rencontre.

Offrir de la compagnie et de l'affection à des personnes à la recherche d'une relation est une méthode efficace pour tisser un lien avec des victimes potentielles. Une fois le lien créé, les fraudeurs peuvent tirer parti des sentiments éprouvés pour convaincre les victimes de leur envoyer de l'argent. La relation initiale peut évoluer vers des promesses de remboursement, des pressions ou de la culpabilisation, de la colère voire de l'extorsion ou des menaces.

Dans une variante du stratagème de rencontre qui contribue à des pertes substantielles, les fraudeurs peuvent commencer par un stratagème de rencontre qui devient ensuite une fraude à l'investissement. Dans ce type d'escroquerie désignée par le terme anglais **« pig butchering »** (la boucherie), la personne ciblée entre dans une relation virtuelle avec le fraudeur. Après un certain temps de relation, le fraudeur invite la victime à entreprendre une forme d'investissement. Les investissements les plus courants comprennent les cryptomonnaies, mais peuvent également inclure l'immobilier, l'or et d'autres modes d'investissement.

Une fois que le fraudeur a développé un lien avec une personne, il la convainc souvent de fournir des informations personnelles, des détails sur sa vie et son travail ou du matériel sexuel et explicite. Ces renseignements et ces documents peuvent être utilisés pour soutirer de l'argent à une victime ou la menacer si elle ne se répond pas aux demandes. À mesure que la fraude progresse, le fraudeur peut même demander à la victime de se rendre dans un autre pays, ce qui peut, dans des cas exceptionnels, constituer un danger pour la personne et mener à d'autres formes d'exploitation ou de victimisation.

Le stratagème de rencontre se déroule en général sur de longues périodes. Les membres de la famille attentifs peuvent être en mesure de remarquer des changements dans la personnalité ou les habitudes de la victime. Ces changements peuvent comprendre :

- **Utilisation d'Internet :** La victime peut passer beaucoup de temps en ligne ainsi que plus de temps dans des appels vidéo ou des conversations avec une personne en particulier (le fraudeur).
- **Réticence à parler d'une relation en ligne :** Malgré tout le temps passé à parler avec son amoureux ou amoureuse, la victime peut se montrer secrète ou évasive avec les membres de sa famille au sujet de la relation. Dans bien des cas, le fraudeur déconseille vivement à la victime de parler de la relation, par crainte que les membres de la famille découvrent la fraude et incitent la personne à mettre fin à la relation.
- **Difficultés financières :** Un stratagème de rencontre se déroulant souvent sur une longue période, la victime peut éprouver des difficultés financières chroniques, apparentes et peu ordinaires.
- **Changements de personnalité :** Le fraudeur peut pousser la victime à s'éloigner de ses amis et de sa famille pour renforcer le lien qui les unit et réduire les risques qu'un membre de la famille s'interpose.

En 2022, le CAFC a reçu 1 420 signalements totalisant 59 millions de dollars de pertes. Le stratagème de rencontre demeure l'une des formes de fraude les plus prolifiques observées par le CAFC. Le stratagème de rencontre peut être particulièrement traumatisante dans la mesure où la victime doit composer avec des pertes financières et émotionnelles au terme de la relation.

Les stratagèmes de rencontre ne commencent pas toujours sur les sites de rencontre ou les applications. Beaucoup sont lancées dans un message direct sur une application de messagerie ou sur les médias sociaux. Soyez prudent lorsque quelqu'un que vous ne connaissez pas communique avec vous et signalez tout profil douteux comme indésirable.

TÉMOIGNAGE D'UN SIGNALEMENT D'UN STRATAGÈME DE RENCONTRE

« Je suis récemment allée sur des sites de rencontre en ligne et j'ai rencontré un homme le 24 septembre 2022. Nous avons ressenti une connexion instantanée et j'étais avertie concernant les fraudes. Au fil de notre relation et parce que je me méfiais des arnaques, il m'a donné de nombreuses preuves de son identité. Il m'appelait deux ou trois fois par jour et finissait toujours par un appel le soir, où que je sois. Nos appels duraient parfois deux heures. Il me donnait beaucoup de détails, ses histoires étaient toujours pertinentes et l'information liée au passé cohérente.

Il m'a annoncé qu'il avait gagné un contrat pour lequel il devait se rendre en Turquie. Il m'a envoyé des documents sur son itinéraire, des vidéos faites sur place et d'autres éléments de détail.

À sa demande, je lui ai prêté de l'argent, car il me disait que son compte bancaire était bloqué. Il avait besoin de cet argent pour ouvrir un compte en Turquie afin d'effectuer un dépôt. J'ai transféré l'argent sur un compte particulier.

Deux semaines plus tard, il avait besoin d'argent supplémentaire, car la Turquie lui imposait un impôt sur ses revenus. Je lui ai transféré 10 000 $, puis j'ai acheté une traite bancaire pour 12 000 $ et l'ai déposée dans un autre compte. Aujourd'hui, il m'a demandé 30 000 $ de plus, et j'ai réalisé que j'étais victime d'une arnaque. »

Vous cherchez l'amour en ligne? Signes d'une relation pouvant être une fraude sentimentale :

- La personne dit qu'elle vit dans un autre pays ou ne veut jamais vous rencontrer en personne.
- La personne que vous rencontrez en ligne semble très pressée d'entamer une relation sérieuse.
- Après un certain temps, la personne commence à réclamer de l'argent pour faire face à des événements ou à des problèmes graves.
- La personne commence à manifester des comportements relationnels toxiques si vous ne lui envoyez pas l'argent (p. ex. se met en colère, se montre distante ou vous fait culpabiliser).
- La personne tente de vous convaincre d'investir de l'argent dans un projet ou des cryptomonnaies.

Usurpation d'identité d'organisations gouvernementales

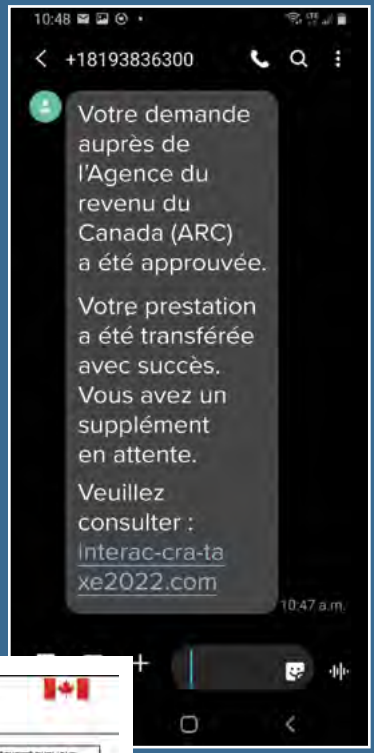
En 2022, le CAFC a observé des signalements de fraudeurs se faisant passer pour des institutions financières, l'Agence du revenu du Canada (ARC), l'Agence des services frontaliers du Canada (ASFC), des entreprises de messagerie et de livraison, la GRC, d'autres services de police nationaux et internationaux ainsi que d'autres organisations gouvernementales canadiennes[13]. Le CAFC a même reçu des signalements de fraudeurs se faisant passer pour le CAFC.

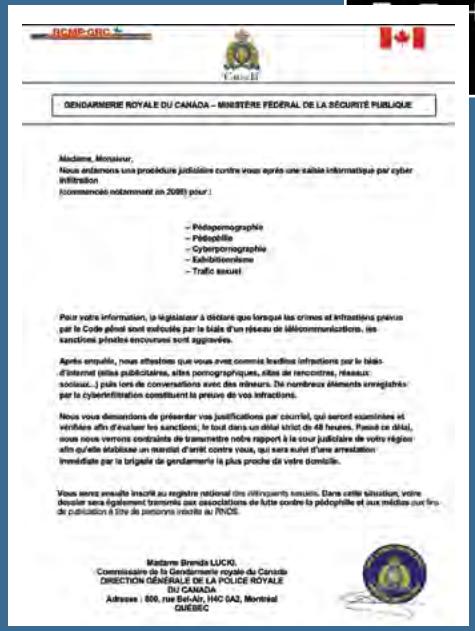
Selon les organisations dont l'identité a été usurpée, ces stratagèmes frauduleux sont reliés à plusieurs formes de fraude notables, dont les suivantes :

- Hameçonnage téléphonique et par message texte;
- Annulation de frais ou du paiement de marchandises (fraude liée aux marchandises);
- Tentatives d'extorsion et menaces d'arrestation, de punition, de préjudice ou d'amende;
- Vol de renseignements personnels, vol d'identité et fraude à l'identité par usurpation de l'identité d'institutions financières.

Plus précisément, le CAFC a observé un plus grand nombre de signalements de fraude à l'enquêteur bancaire. Cette fraude consiste pour un fraudeur à se faire passer pour un investisseur ou une autorité bancaire qui appelle au sujet de transactions suspectes. Le CAFC a reçu 4 255 signalements de fraude à l'enquêteur bancaire totalisant 6,7 millions de dollars de pertes en 2022.

Les fraudeurs se font passer pour différentes organisations canadiennes pour donner une apparence légitime à leurs messages. Les escroqueries par message texte et par courriel contenant des pièces jointes et des liens continuent d'être des techniques de tromperie populaires.




GENDARMERIE ROYALE DU CANADA – MINISTÈRE FÉDÉRAL DE LA SÉCURITÉ PUBLIQUE

13 « Mounties warning of scam using name of RCMP commissioner » [Les gendarmes mettent en garde contre une escroquerie utilisant le nom du commissaire de la GRC]

Fraude liée aux marchandises et aux marchandises contrefaites

Au lendemain de la pandémie de COVID-19, les Canadiens recommencent à se rendre en personne dans les magasins. Si le CAFC a encore reçu un nombre considérable de signalements de fraude liée aux marchandises et aux marchandises contrefaites en 2022, le nombre de signalements et les pertes monétaires ont diminué par rapport à 2021.

En 2022, le CAFC a relevé des pertes d'environ 8,8 millions de dollars et de 900 000 $ pour la fraude liée aux marchandises et la fraude liée aux marchandises contrefaites respectivement, pour un total de 7 994 signalements. Ces chiffres peuvent être comparés à 12,3 millions de dollars et 1 million de dollars respectivement en 2021, pour un total de 10 194 signalements.

TÉMOIGNAGE D'UN SIGNALEMENT DE FRAUDE LIÉE AUX MARCHANDISES

« Je cherchais un article sur Marketplace, et j'ai trouvé une annonce correspondant à cet article. J'ai pu obtenir l'adresse courriel du vendeur. Après acceptation de la vente, j'ai transféré de l'argent sur le compte du vendeur. Nous avons convenu d'un rendez-vous pour que je récupère l'article. Le jour venu, le vendeur a cessé de me répondre au téléphone et n'était pas présent à l'adresse indiquée.

J'ai communiqué avec ma banque qui m'a expliqué qu'une fois que l'argent était déposé, je ne pouvais pas annuler la transaction et je devais faire une déclaration à la police. »

Tendances en matière de fraude à l'identité, de vol d'identité et de vol de renseignements personnels

Le vol de renseignements personnels est étroitement associé à la plupart des formes de fraude. Si le fraudeur ne tente pas de voler de l'argent, il essaie de voler des renseignements personnels. Cela se traduit par d'autres formes de crime financier et de fraude.

Une fraude à l'identité découle d'un vol d'identité ou de renseignements personnels. Souvent, les victimes ne se rendent pas compte que leurs renseignements personnels ont été volés ou que leur identité peut être utilisée. Il existe d'innombrables façons de se faire voler des renseignements personnels ou son identité, notamment :

- En achetant quelque chose en ligne sur un site Web non sécurisé;
- En soumettant des renseignements personnels dans un questionnaire en ligne frauduleux;
- En omettant de déchiqueter des renseignements financiers ou personnels et en les déposant dans un bac de recyclage;
- En soumettant des renseignements de connexion à un site Web falsifié;
- En soumettant des renseignements personnels par téléphone à la demande d'un fraudeur se faisant passer pour un employé de banque ou un fonctionnaire.

Les scénarios de fraude peuvent être très simples ou très sophistiqués, et la perte de renseignements personnels peut être particulièrement préjudiciable pour la victime. Le vol d'identité et le vol de renseignements personnels peuvent entraîner des difficultés financières et personnelles durables, surtout si l'identité est utilisée pour commettre d'autres formes de fraude.

Après le vol, les fraudeurs peuvent se servir des identités usurpées pour cacher des activités criminelles, ouvrir des comptes bancaires frauduleux afin d'y déposer et d'y transférer les produits de la fraude, contracter des prêts et acheter des articles, voire accéder à d'autres comptes bancaires personnels pour voler de l'argent directement.

Le CAFC continue d'observer une augmentation des vols de renseignements personnels et des crimes liés à l'identité. En 2022, le CAFC a reçu 8 086 signalements de vol de renseignements personnels et 19 543 signalements de fraude à l'identité, contre 7 808 signalements de vol de renseignements personnels et 31 797 signalements de fraude à l'identité en 2021.

Remarque : La fraude à l'identité est utilisée pour obtenir des gains financiers. Toutefois, le CAFC n'est pas en mesure de déterminer avec exactitude les pertes financières dues aux crimes liés à l'identité, car les renseignements d'identification et les identités individuelles peuvent être utilisés de nombreuses manières illégales que ne connaît pas la victime au moment du signalement.

TÉMOIGNAGE D'UN SIGNALEMENT DE VOL D'IDENTITÉ OU DE FRAUDE À L'IDENTITÉ

« J'ai reçu un courriel d'Equifax m'avisant qu'un compte avait été ouvert à mon nom. Après vérification des informations sur Equifax, j'ai découvert une nouvelle carte de crédit suspecte dans une banque dont je n'ai jamais été client et la création d'une marge de crédit. J'ai également découvert qu'un nouveau numéro de téléphone était associé à mon compte Equifax légitime. J'ai appelé la banque pour signaler le problème, qui m'a conseillé de me rendre à la succursale. Là, j'ai réalisé que quelqu'un avait ouvert le compte de carte de crédit avec les renseignements volés. La banque a communiqué avec son unité responsable des fraudes et a pu fermer le compte.

J'ai par la suite fait une déclaration de fraude au service de police locale. Lorsque j'ai tenté de déposer une alerte de fraude à TransUnion, j'ai essayé de créer un compte. Je n'ai pas pu le faire, car un compte était déjà créé à mon nom. J'ai communiqué avec TransUnion par téléphone et nous avons compris qu'un compte avait été créé à l'aide d'une fausse adresse courriel et de l'adresse municipale correspondant à mon numéro d'assurance sociale. TransUnion a été en mesure de placer l'alerte de fraude et de supprimer le faux compte. »

Fraude et crime organisé

La fraude et le crime organisé international sont étroitement liés. Même si ce n'est pas nécessairement une nouvelle tendance, les entreprises criminelles sont de plus en plus souvent impliquées dans des opérations de fraude visant à extorquer ou à voler de l'argent aux Canadiens. La grande majorité des fraudes sont perpétrées par des groupes criminels organisés et internationaux qui ciblent un grand nombre de Canadiens. Par ailleurs, les fraudes coordonnées de type hameçonnage, qui ciblent des organisations du secteur privé, sont souvent perpétrées par des groupes similaires.

Comme les pertes dues à la fraude continuent d'augmenter en flèche et les pertes par victime de croître, les groupes de fraude organisée se montrent de plus en plus créatifs pour exécuter des transferts d'importantes sommes d'argent du Canada vers d'autres pays. Les mouvements d'argent inhabituels ou les transactions de grande ampleur sont souvent bloqués ou signalés par les institutions financières canadiennes. Face à cette diligence des institutions financières, les groupes de fraude utilisent des **mules** résidant au Canada pour faciliter le mouvement des fonds acquis frauduleusement.

Mules

On appelle **mule** toute personne qui, sciemment ou non, transfère ou transporte des fonds illicites pour le compte d'une organisation criminelle ou frauduleuse, dans le but de tromper les autorités pénales et réglementaires. Il existe deux sous-groupes de mules :

- Les mules qui participent **activement** à la fraude.
- Les mules qui participent **passivement** à la fraude.

Les mules qui participent **activement** à la fraude jouent volontairement le rôle d'intermédiaire pour les groupes de fraude. Les mules professionnelles peuvent récupérer des colis contenant de l'argent au domicile des victimes ou à un bureau de poste, ouvrir et exploiter des comptes bancaires en utilisant des identités volées ou simplement utiliser leurs propres identité et compte bancaire pour faire transiter de l'argent par leur compte en échange d'une partie des profits.

Une autre forme de participation active suit la fraude liée à l'emploi. Les victimes deviennent une mule active sans savoir qu'elles contribuent à une opération de fraude. Portant souvent le titre d'« agent financier » ou de « gestionnaire de portefeuille ou de compte client », ces personnes sont recrutées comme « préposé au traitement des paiements » pour l'opération de fraude. À cette fonction, la victime reçoit de l'argent dans son compte personnel ainsi que des instructions pour transférer l'argent dans des comptes inscrits détenus par les fraudeurs ou d'autres mules.

De plus, les victimes qui ont perdu des sommes considérables d'argent peuvent être contraintes à agir comme mule, avec la promesse qu'elles récupéreront une partie ou la totalité de leur argent si elles exécutent les tâches demandées.

Les victimes de fraude peuvent également être des mules **passives** dans les opérations de fraude. Les mules passives sont habituellement associées au vol d'identité et à la fraude à l'identité ainsi qu'au vol de renseignements personnels. L'opération de fraude utilise l'identité volée pour ouvrir de nouveaux comptes bancaires ou accéder à des comptes personnels à l'insu de la victime, puis fait transiter l'argent par le compte pour cacher le mouvement des fonds.

Les mules sont des acteurs clés des opérations de fraude au Canada. Le CAFC a observé le lien étroit entre les mules et la fraude du besoin urgent d'argent et des grands-parents, la fraude liée aux cryptomonnaies, la fraude à l'investissement et d'autres types de fraudes qui entraînent des pertes importantes par victime. La fraude devenant de plus en plus lucrative, les répercussions du crime organisé dans cette sphère continueront de mettre à l'épreuve les efforts des forces de l'ordre.

Fraude ciblant les aînés

Les aînés (personnes de 60 ans et plus) et les populations vulnérables continuent de représenter les victimes d'une part croissante de l'ensemble des fraudes signalées au CAFC en 2022. En 2021, le CAFC a reçu près de 13 000 signalements d'aînés totalisant 83,6 millions de dollars de pertes. En 2022, le CAFC a reçu environ 17 000 signalements d'aînés totalisant 137,8 millions de dollars de pertes, ce qui montre que ce groupe de Canadiens a continué d'être la cible des fraudeurs et des auteurs de cybermenaces.

En général, les personnes âgées sont particulièrement vulnérables aux formes classiques de fraude, où le premier contact est réalisé par téléphone ou par ligne terrestre et qui comprend des pressions, des menaces et du harcèlement.

Comme en 2021, les aînés continuent d'être victimes d'extorsion, avec 2 194 signalements totalisant des pertes de 7,7 millions de dollars en 2022. L'hameçonnage est également un thème dominant dans les signalements de fraude par les aînés, avec 2 415 signalements d'hameçonnage au CAFC. Les pertes des aînés dues à la fraude à l'investissement ont fortement augmenté en 2022, s'élevant à environ 78,8 millions de dollars comparativement à 38 millions de dollars en 2021. Parmi les autres tendances en progression par rapport à 2021, mentionnons entre autres les fraudes liées aux services, les fraudes du besoin urgent d'argent et les fraudes à l'enquêteur bancaire.

Les autres types de fraudes dominants comme le stratagème de rencontre, le vol de renseignements personnels, la fraude des prix gagnés et la fraude liée aux marchandises sont demeurés relativement stables en 2022. Malgré la reprise des voyages en 2022, la fraude ciblant la multipropriété a continué de diminuer, avec 19 signalements totalisant 783 000 $ de pertes en 2022, comparativement à 30 signalements totalisant 2,1 millions de dollars en 2021.

Aînés (60 ans et plus) – Les 10 principales catégories de fraudes

Type de fraude	Nbre de signalements	% du total général des signalements	Nbre de victimes	% de victimes
Fraude à l'identité	2 510	12,9 %	2 497	99,5 %
Hameçonnage	2 415	12,4 %	601	24,9 %
Extorsion	2 194	11,3 %	475	21,6 %
Service	2 130	11,0 %	1 664	78,1 %
Renseignements personnels	1 808	9,3 %	1 175	65,0 %
Enquêteur bancaire	1 687	8,7 %	512	30,3 %
Besoin urgent d'argent (prison, accident, hôpital, aide)	1 672	8,6 %	750	44,9 %
Investissement	858	4,4 %	824	96,0 %
Prix gagné	743	3,8 %	230	31,0 %
Marchandises	510	2,6 %	395	77,5 %
Total	**16 527**	**85,1 %**	**9 123**	**55,2 %**

Aînés (60 ans et plus) – Les 10 principales catégories de fraude selon les pertes en dollars

Type de fraude	Perte financière	Perte moyenne en dollars par victime
Investissement	78 760 257 $	95 583 $
Stratagème de rencontre	19 524 955 $	67 327 $
Service	8 566 972 $	5 148 $
Extorsion	7 718 495 $	16 249 $
Besoin urgent d'argent (prison, accident, hôpital, aide)	7 134 791 $	9 513 $
Enquêteur bancaire	4 197 111 $	8 197 $
Prix gagné	3 174 427 $	13 802 $
Offre d'argent de l'étranger	2 429 560 $	115 693 $
Subventions	1 653 370 $	10 599 $
Récupération d'argent	974 419 $	15 716 $
Total	**134 134 357 $**	**26 913 $**

Le vol de renseignements personnels et l'hameçonnage continuent de viser les aînés et les Canadiens vulnérables. Le CAFC a observé un nombre très élevé de signalements de fraude à l'identité dans ce groupe d'âge en 2022. Les signalements de fraude du besoin urgent d'argent ont triplé en 2022 par rapport à 2021. Les escroqueries à l'investissement continuent de produire les pertes les plus importantes pour les aînés, ces pertes ayant plus que doublé pour passer de 38 millions de dollars en 2021 à près de 79 millions de dollars en 2022.

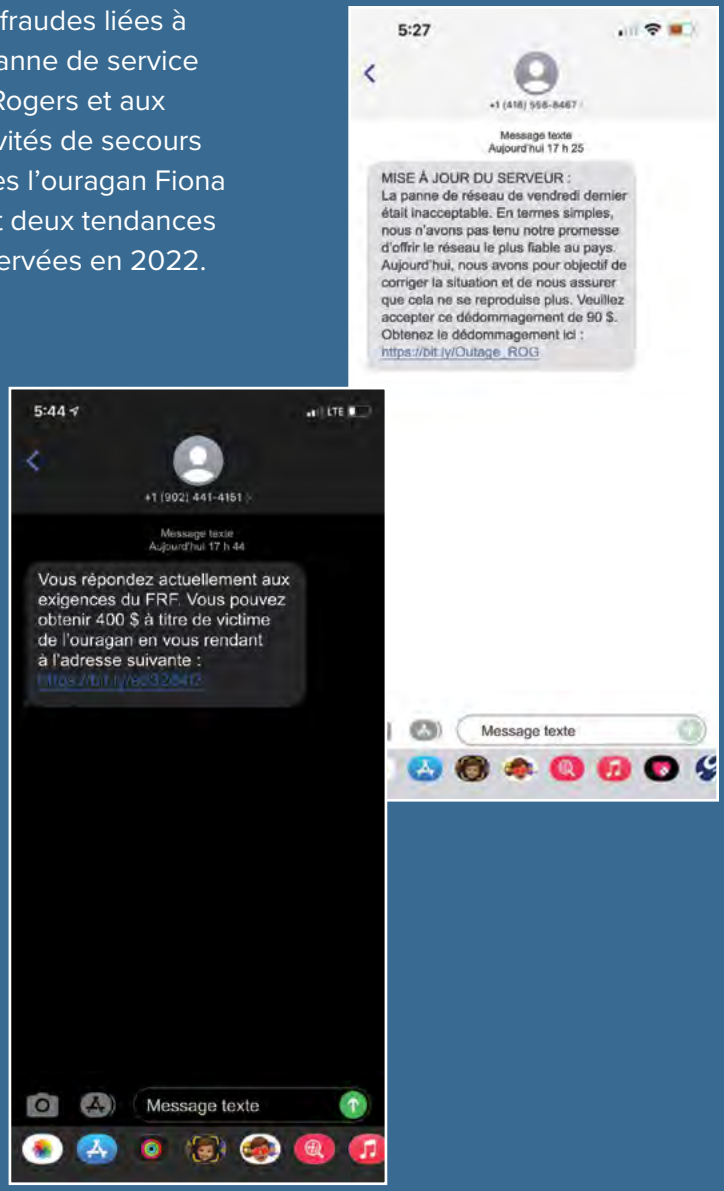
Nouveaux thèmes de fraude

L'environnement de la fraude est extrêmement dynamique. Les opérations de fraude adaptent leurs approches en fonction du succès de leurs tentatives, des tendances socioculturelles et des efforts des forces de l'ordre pour nuire à leur écosystème.

Ainsi, en 2022, le CAFC a observé une diminution de la fraude liée à la COVID-19, qui était très populaire ces dernières années, et une augmentation des fraudes liées aux actualités comme le conflit en cours entre la Russie et l'Ukraine, les efforts de secours après l'ouragan Fiona, les remboursements à la suite des pannes nationales de Rogers, pour citer quelques exemples. Certains types de fraudes, comme les escroqueries liées aux organismes de bienfaisance et l'hameçonnage, ont tiré parti de l'attention portée par les Canadiens sur l'actualité.

La fraude par Internet continue de croître, mais la fraude avec un premier contact au téléphone est le sous-ensemble de fraude le plus signalé au CAFC. Les fraudeurs utilisent également de nouvelles méthodes de prise de contact, notamment ils envoient d'abord un message texte à la victime potentielle contenant une tentative d'hameçonnage et attendent que la victime réponde ou clique sur un lien fourni dans le texte.

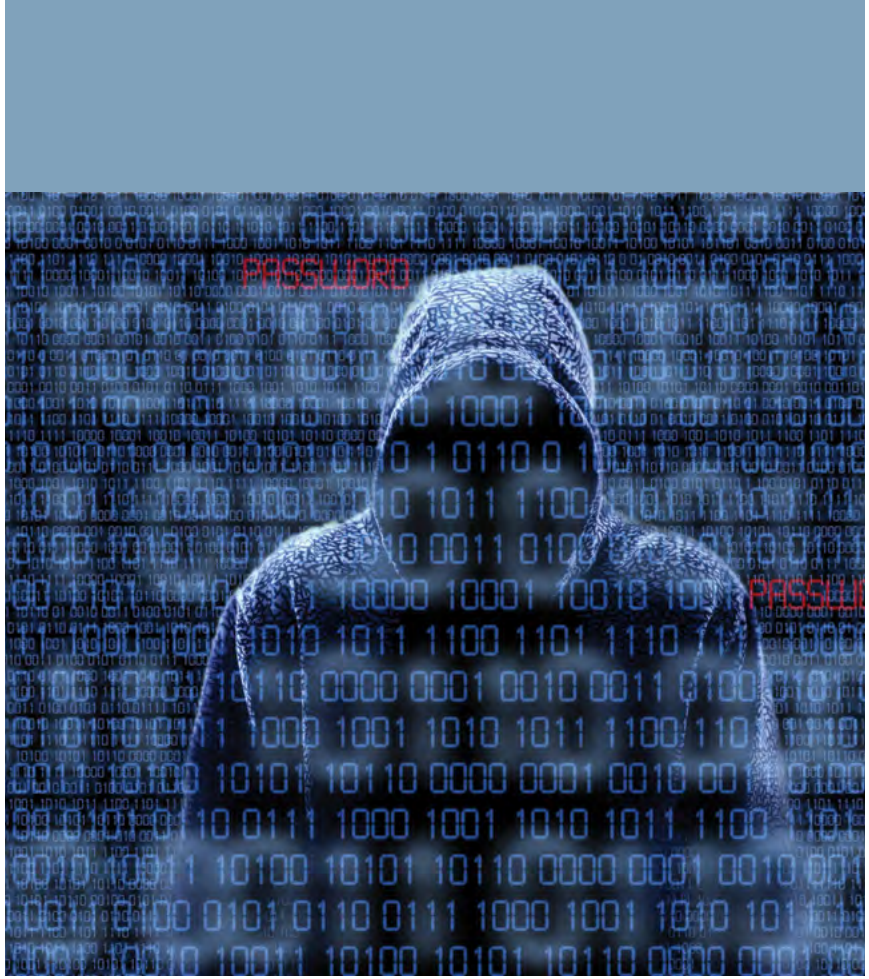
Les fraudes liées à la panne de service de Rogers et aux activités de secours après l'ouragan Fiona sont deux tendances observées en 2022.



Logiciel d’accès à distance

Les logiciels d’accès à distance sont de plus en plus souvent mentionnés dans les signalements de fraude au CAFC, en particulier dans les fraudes à l’enquêteur bancaire et les fraudes au soutien technique. Le fraudeur propose du « soutien » pour des problèmes informatiques ou financiers en cours et demande d’accéder aux appareils de la victime pour les corriger. Les fraudeurs demandent aux victimes d’allumer leur ordinateur ou de cliquer sur des liens envoyés par texto sur les téléphones cellulaires. La fraude qui utilise des outils d’accès à distance est particulièrement efficace lorsque les victimes sont déconcentrées ou désorientées, notamment lorsque le fraudeur crée un sentiment de pression ou d’urgence.

Les outils d’accès à distance sont des logiciels légitimes et propriétaires qui permettent d’accéder à distance à des ordinateurs et de transférer des fichiers virtuellement. En se servant illégalement de cette technologie, les fraudeurs demandent à la victime de télécharger l’application d’accès à distance. Ils la convainquent ensuite de fournir le code d’accès généré par l’outil pour pouvoir accéder à distance à son ordinateur et d’autoriser d’autres fonctions comme le transfert de fichiers et l’occultation de l’écran. Ainsi, le fraudeur peut consulter les comptes bancaires, accéder à des renseignements personnels, créer de nouveaux comptes bancaires et de cryptomonnaies, etc.



Nouvelles technologies favorisant la fraude

Internet permet aux fraudeurs de contacter et de cibler des victimes potentielles à grande échelle. Les publicités, les plateformes de médias sociaux, les courriels, les groupes de clavardage et les forums offrent un accès sans précédent et rapide à des personnes dans le monde entier.

Dans le cyberenvironnement, les fraudeurs peuvent dissimuler leur identité, se faire passer pour des amis, des figures d'autorité ou d'autres personnalités, voire créer d'innombrables comptes gérés par des services ou des programmes automatisés (robots). Le cyberenvironnement permet de réaliser des formes de fraude complexes que les utilisateurs ont de plus en plus de difficulté à reconnaître.

Selon les prévisions du CAFC, les avancées technologiques suivantes auront une forte incidence sur l'environnement de la fraude : intelligence artificielle générative, grands modèles de langage, logiciels de clonage de voix, hypertrucages et robots.

Modèles de langage prédictifs et conversationnels, logiciel de clonage de voix et hypertrucages

L'intelligence artificielle (IA), y compris l'IA générative fondée sur le dialogue comme ChatGPT et l'IA Bard de Google, a été lancée en 2022 et en 2023 et suscite une attention internationale majeure. Facilement accessibles au public, ces outils aident à rédiger des courriels et des documents complexes, font des suggestions en réponse à des questions ou à des problèmes, offrent aux utilisateurs des perspectives différentes sur les questions et fournissent d'autres formes d'aide, comme des traductions rapides et de grande qualité et la rédaction de textes rigoureux et détaillés. Si cette technologie peut être utile, elle crée également une nouvelle dynamique dans l'environnement de la fraude.

En lien avec les outils de clavardage fondés sur l'IA, les nouveaux logiciels de clonage ou d'imitation de la voix permettront de plus en plus de fraudes. Dans ce type de programme, les utilisateurs peuvent entrer des extraits sonores ou des dialogues d'un utilisateur ou utiliser du matériel sonore de personnes célèbres et reconnaissables. Pour un coût minime ou nul, tout le monde peut programmer un modèle de voix pour lui faire dire ce qu'il veut[14]. Les fraudeurs peuvent utiliser des voix célèbres pour présenter des stratagèmes de fraude de plus en plus sophistiqués; le CAFC observe ce phénomène dans les publicités sur les services de diffusion vidéo en continu. Les faux profils de qualité élevée de personnes qui n'existent pas, combinés à l'amélioration permanente du matériel audiovisuel de fraude, continueront de freiner la détection des profils potentiellement faux ou malveillants.

14 Un exemple de cette technologie est **Uberduck**.

Lorsqu'une personne publie du contenu en ligne contenant sa voix, le fraudeur pourra utiliser un logiciel de clonage de voix pour traiter ces échantillons sonores et se faire passer pour la personne. Bien que nous en soyons aux balbutiements de l'application de cette technologie, le CAFC reçoit de plus en plus de signalements de fraudes du besoin urgent d'argent dans lesquelles les victimes reçoivent un coup de téléphone d'une personne en souffrance ou appelant à l'aide dont la voix ressemble à celle de leurs proches ou de leurs propres petits-enfants.

Au-delà du clonage de voix et de l'usurpation d'identité, le CAFC a observé l'utilisation de profils, de vidéos et d'images de personnes générés par l'IA pour commettre des fraudes. Les avancées en IA ont introduit de nouvelles méthodes de création de profils et d'identités factices de plus en plus complexes (hypertrucages)[15]. Par exemple, les programmes d'IA peuvent permettre de créer de faux visages sur les profils des médias sociaux[16].

En combinant toutes les formes mentionnées de voix, d'images et de contenu vidéo, à l'aide d'un logiciel ouvert accessible, les opérations de fraude peuvent complètement usurper l'identité d'une personne et créer une nouvelle identité virtuelle impossible à distinguer de la personne réelle.

Robots

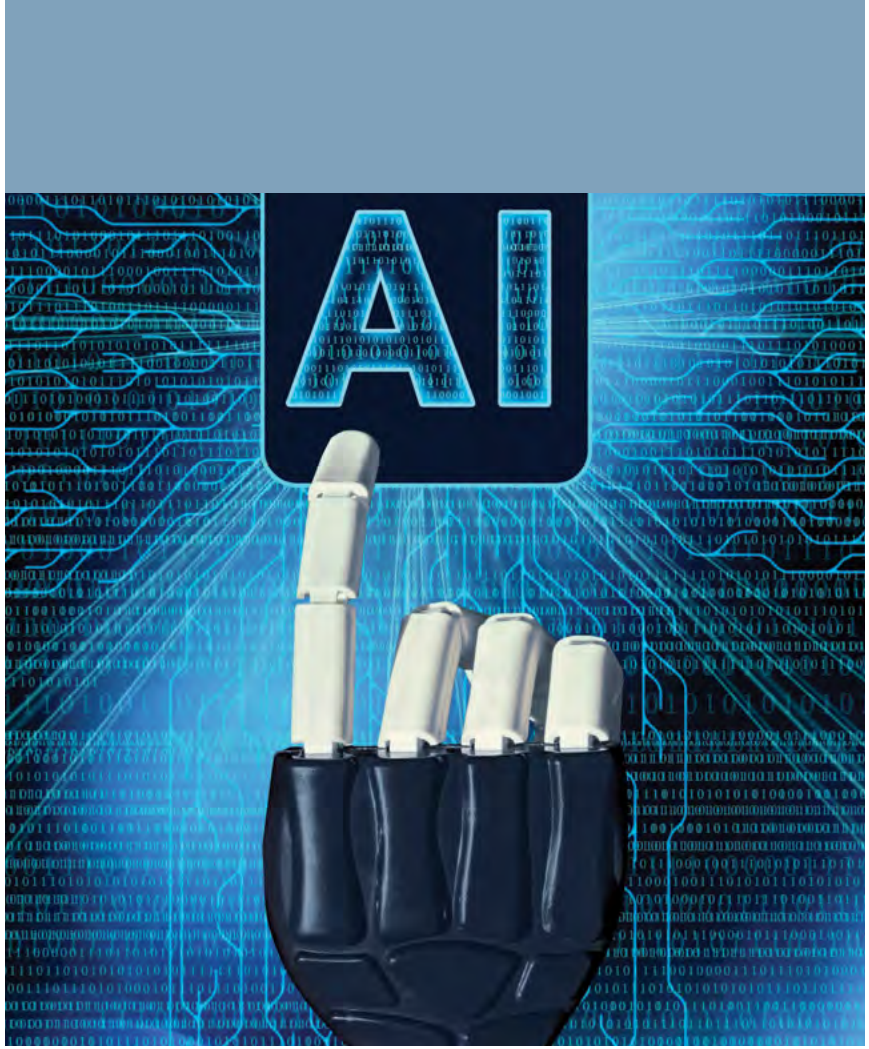
Les robots Internet, ou « bots », sont des applications logicielles qui gèrent des tâches automatisées sur Internet. Les robots peuvent être programmés pour contacter les utilisateurs des sites de médias sociaux dans des messages directs, publier des articles sur les sites Web, engager une conversation entre eux et avec les utilisateurs (robots conversationnels), envoyer des messages texte, etc. Le plus souvent, les robots effectuent des tâches automatisées et simples plus rapidement et à un moindre coût qu'un être humain. Pour ce qui est des activités informatiques malveillantes, les robots peuvent propager des virus et des logiciels malveillants et déclencher des cyberincidents.

Pour ce qui est plus directement lié à la fraude, les personnes peuvent être contactées par d'autres utilisateurs d'un site et ne pas se rendre compte que l'utilisateur avec lequel elles interagissent est en réalité un robot. Les robots peuvent tromper les utilisateurs et leur voler de l'argent ou des renseignements personnels. Les utilisateurs peuvent recevoir un message avec un lien et cliquer accidentellement dessus, ce qui les rend ensuite vulnérables au vol de renseignements personnels, aux virus ou aux logiciels malveillants. Un robot peut rediriger un utilisateur vers d'autres sites pour l'inciter à participer à une fraude. Enfin, un robot peut signaler à un auteur de cybermenaces ou à un fraudeur le moment où il peut communiquer directement avec l'utilisateur.

15 NIGHTINGALE, Sophie J., et Hany FARID. (14 février 2022) **« AI-Synthesized Faces and Indistinguishable from Real Faces and More Trustworthy »**, *Psychological and Cognitive Sciences 119*(8).
16 BOND, Shannon. (27 mars 2022) **« That Smiling LinkedIn Profile Might be a Computer-Generated Fake »**, *NPR*.

Les recherches en cours sur les activités sur les médias sociaux commencent à révéler des niveaux très élevés d'activités sur les sites Web attribuée à des robots malveillants[17]. Si les robots constituent une menace omniprésente et de longue date, facilement observable par les internautes, les tentatives actives de détection et d'élimination des robots au moyen de logiciels antivirus, de tests en ligne comme CAPTCHA et reCAPTCHA et de surveillance de l'activité sur Internet, n'ont fait que conduire à la sophistication et à l'extension des réseaux de zombies. Les robots sont l'un des outils utilisés par les cybercriminels les plus répandus et leur qualité peut être telle qu'ils sont difficiles à détecter par les utilisateurs individuels. Avec les robots, les cybercriminels parviennent à leurs fins, même si les entreprises et le gouvernement du Canada créent de meilleures stratégies pour lutter contre cette menace. Le CAFC remarque que les robots constituent une menace grandissante, qui continuera de nuire aux internautes canadiens dans les années à venir.

Les robots sont l'un des outils utilisés par les cybercriminels les plus répandus pour cibler un nombre important de victimes potentielles. Le succès continu des réseaux de zombies en lien avec la fraude et la cybercriminalité, associé aux efforts durables des entreprises et des gouvernements pour créer des stratégies plus efficaces contre cette menace, laisse penser que les robots gagneront en puissance, se répandront et ressembleront de plus en plus aux utilisateurs humains réels. Le CAFC considère les robots comme une tendance en évolution qui continuera de menacer les internautes canadiens.



17 PFEFFER, Jurgen et coll. (26 janvier 2023). « Just Another Day on Twitter: A Complete 24 Hours of Twitter Data » arXiv preprint arXiv:2301.11429.

Le point sur les efforts actuels

Que vous souhaitiez vous informer activement sur la fraude et les méthodes pour l'éviter, déposer un signalement auprès du CAFC et des services de police locaux, obtenir des conseils et du soutien après avoir été victime de fraude ou prévenir le CAFC d'une tentative de fraude, le CAFC travaille avec diligence pour assurer une présence positive auprès des Canadiens. En tirant parti des efforts des analystes des signalements et de la réception, du personnel du Groupe de soutien aux aînés et des bénévoles, du personnel des communications et des médias et des équipes responsables du renseignement et des enquêtes, le CAFC continuera de soutenir les victimes de fraude.

Le CAFC tient à remercier tous les Canadiens et les personnes à l'extérieur du Canada qui ont communiqué avec lui ou lui ont soumis un signalement. Sans une mobilisation continue, le CAFC ne pourrait pas offrir ses services et coordonner efficacement les efforts de lutte contre la fraude avec les services de police compétents.

Le point sur la Solution nationale en matière de cybercriminalité et le Système national de signalement des incidents de cybercriminalité et de fraude

Depuis la mise à jour de l'année dernière, le CAFC continue de collaborer avec le Centre national de coordination contre la cybercriminalité (CNC3) pour créer la Solution nationale en matière de cybercriminalité (SNC) de la GRC. La SNC sera un dépôt de données centralisé contenant les données d'enquête sur la fraude et la cybercriminalité, les incidents et les renseignements gérés conjointement par le CNC3 et le CAFC.

D'importants progrès ont été réalisés en 2022 par rapport au projet de la SNC. La SNC est passée à la phase de développement complet et a été mise en production pour la première fois en avril 2023. Le lancement intégral est prévu pour le deuxième semestre de 2024.

Comme nous le soulignons dans le Rapport annuel 2022, le Système national de signalement des incidents de cybercriminalité et de fraude se trouve à l'étape de la version bêta et devrait être pleinement opérationnel en 2023-2024.

En 2022, le SNSICF a fait état :

- de 21 238 visiteurs;
- de 5 256 signalements reçus;
- de recherches continues sur les utilisateurs ayant entraîné une diminution de 30 % du temps de chargement du SNSICF.

Tout au long du développement du SNSICF, le CAFC et le CNC3 acceptent les commentaires qui pourraient contribuer au système. Vous pouvez encore participer à nos recherches et devenir bénévole en consultant l'adresse report.antifraudcentre.ca/recruitment.

Conclusion

Selon tous les indicateurs, 2022 a été l'année la plus difficile jamais enregistrée pour la fraude ciblant les Canadiens. Les pertes déclarées ont dépassé le seuil des 500 millions de dollars pour la première fois depuis la fondation du CAFC. Ces pertes ont généré des traumatismes financiers et émotionnels profonds chez des milliers de Canadiens et on estime encore que seulement de 5 à 10 % des victimes signalent les fraudes et les cybercrimes. **La fraude n'est pas un crime sans victime.** D'après notre analyse des signalements, les Canadiens qui continuent d'être les plus touchés par la fraude et le vol d'identité sont les aînés, les populations vulnérables et les personnes qui subissent déjà des pressions financières. Compte tenu de l'augmentation des pertes par victime, le nombre de Canadiens totalement ruinés par les incidents de fraude grandit.

La lutte contre la menace de fraude exige une approche à l'échelle de la société. Le CAFC est un chef de file en matière de sensibilisation et d'information sur la fraude et nous remercions tous les Canadiens de faire passer les messages. Le CAFC tient également à remercier tous les partenaires, y compris les organismes d'application de la loi et les institutions financières, pour leurs efforts visant à aider les victimes et à réduire les méfaits de la fraude.

Le CAFC est le service de police national responsable du signalement des fraudes, de l'harmonisation, de l'échange de renseignements, de l'information et de la sensibilisation, et il s'appuie sur des partenariats solides pour continuer d'assumer ce rôle.

À propos des chiffres

Les statistiques contenues dans le rapport annuel 2022 proviennent de tous les signalements reçus et vérifiés par le CAFC entre le 1er janvier et le 31 décembre 2022. Certains signalements reçus par le CAFC sont incomplets, ne mentionnent pas les sommes perdues et manquent de précisions. Au moment de présenter un signalement, les victimes peuvent donner autant ou aussi peu d'informations qu'elles le souhaitent. Néanmoins, les renseignements détaillés et complets fournis dans les signalements peuvent mieux aider le CAFC à trouver des solutions pour les personnes touchées par la fraude et permettre d'obtenir des renseignements et des statistiques sur la fraude plus fiables.

Les statistiques du rapport annuel comprennent les signalements des tentatives de fraude et les signalements des actes réels de fraude avec victime, et peuvent par conséquent comprendre des signalements n'impliquant pas de perte financière. Le CAFC accorde une grande importance à tous les signalements, y compris les signalements de tentative de fraude ou d'incident de fraude potentielle. Ces signalements sont utiles et offrent de l'information intéressante pour approfondir l'analyse des tendances.

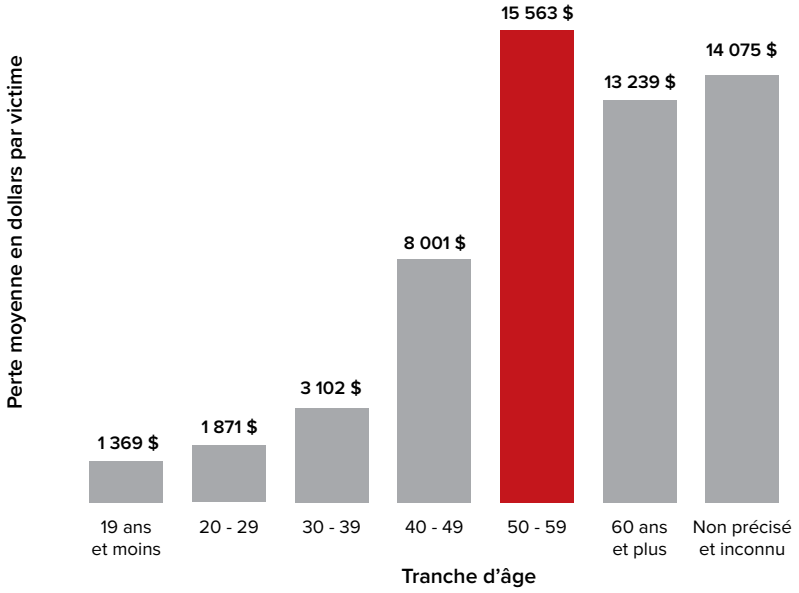
Dans certaines formes de fraude, comme le vol d'identité ou le vol de renseignements personnels, il est difficile d'évaluer les sommes réelles des pertes. À titre d'exemple, un auteur de menaces qui usurpe une identité peut avoir pour but de vendre les données d'identification à d'autres fraudeurs ou de tenter d'obtenir des cartes de crédit en utilisant l'identité de la personne. Les difficultés pour déterminer les pertes en dollars exactes dans ces formes de fraude tiennent à la nature fluide de la fraude.

En raison de la taille de l'ensemble de données et du nombre important de signalements reçus par le CAFC, les chiffres peuvent varier au fil du temps. Le CAFC continue de valider les signalements de l'année précédente, et il est possible de déposer des signalements à une date ultérieure en indiquant que l'incident s'est produit l'année précédente. C'est pourquoi les totaux des signalements et des pertes en dollars pourraient varier au cours de l'année 2023.

Sauf mention explicite, tous les montants exprimés le sont en dollars canadiens.

Statistiques supplémentaires

Perte moyenne en dollars par tranche d'âge

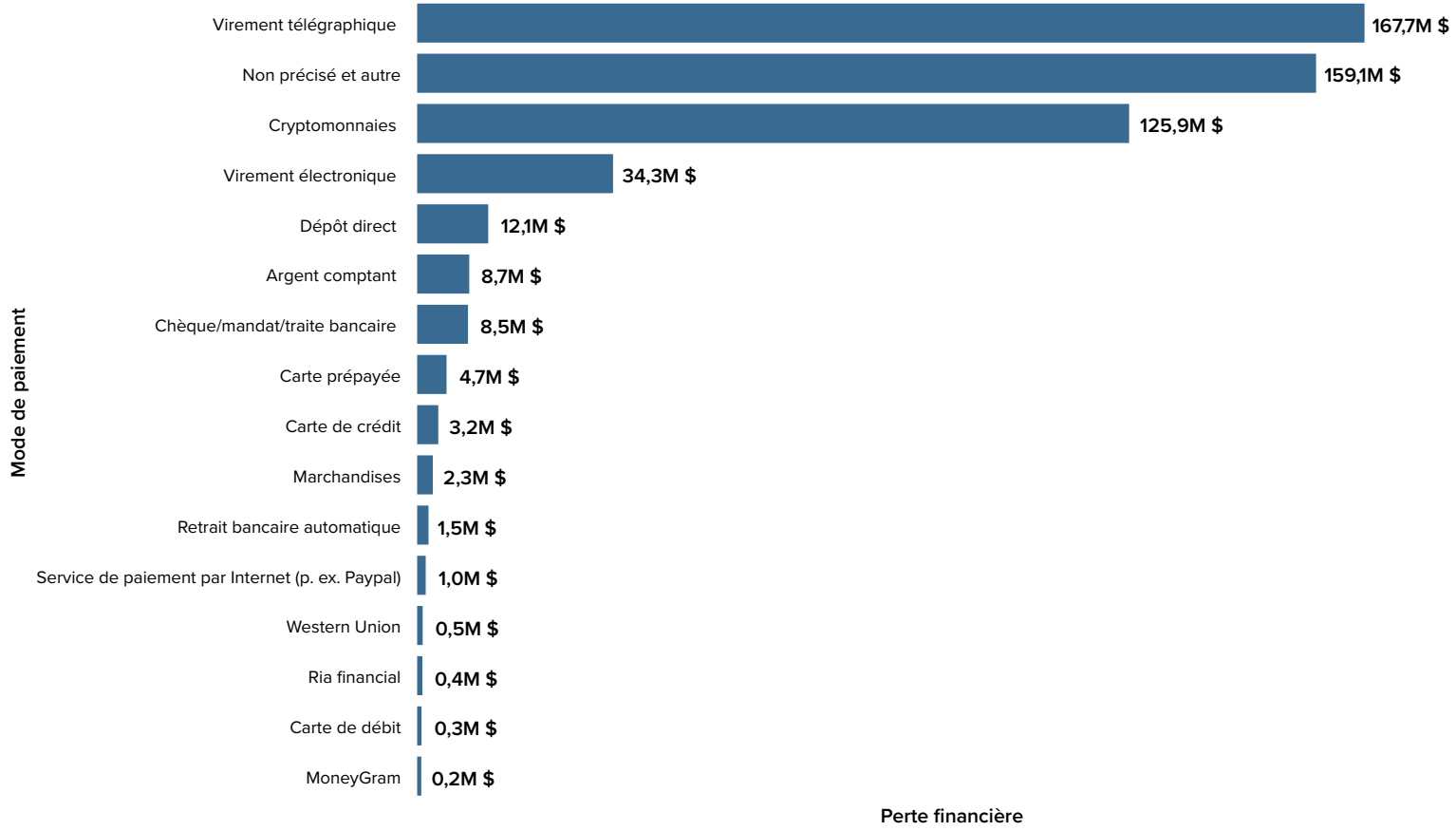


Tranche d'âge	Nbre de signalements	Nbre de victimes	% de victimes	Perte financière	Perte moyenne en dollars par victime
19 ans et moins	1 978	1 730	87,5 %	2 368 433 $	1 369 $
20 - 29	9 569	7 510	78,5 %	14 052 225 $	1 871 $
30 - 39	12 578	9 832	78,2 %	30 500 840 $	3 102 $
40 - 49	10 679	7 759	72,7 %	62 080 599 $	8 001 $
50 - 59	9 291	5 860	63,1 %	91 196 944 $	15 563 $
60 ans et plus	19 424	10 419	53,6 %	137 935 844 $	13 239 $
Entreprises et personnes décédées	43	35	81,4 %	641 092 $	18 317 $
Non précisé et inconnu	27 359	13 617	49,8 %	191 661 990 $	14 075 $
Total	**90 921**	**56 762**	**62,4 %**	**530 437 966 $**	**9 345 $**

Les personnes âgées de 50 à 59 ans et plus continuent de déclarer des pertes plus élevées que les autres groupes d'âge, comme en 2021.

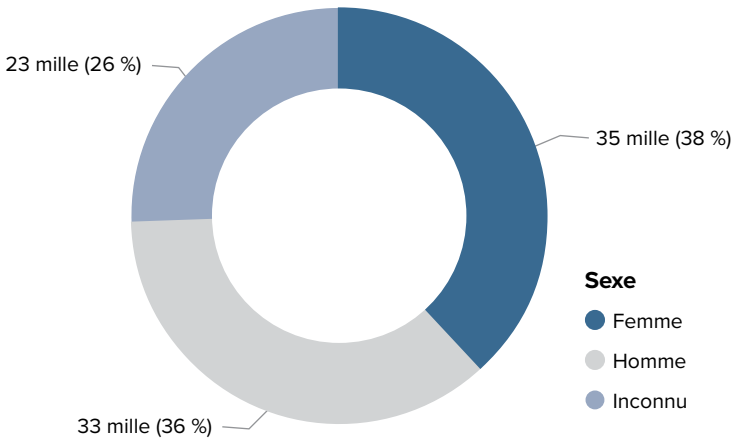
Les entreprises ont également déclaré des pertes élevées par victime, qui peuvent être reliées à des formes de fraude comme le harponnage et la fraude ciblée pour les pertes les plus importantes.

Pertes en dollars par mode de paiement

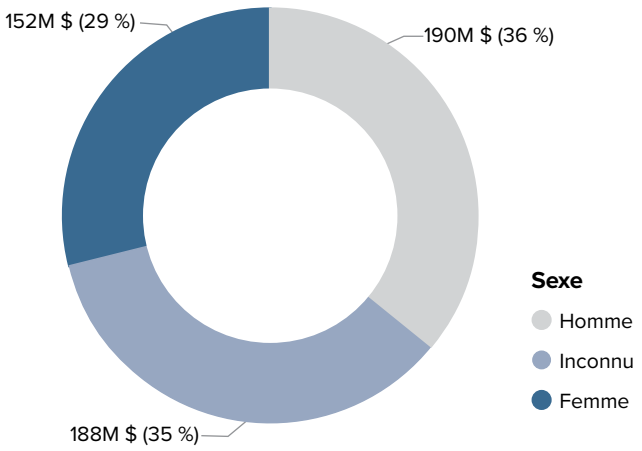


Les virements télégraphiques continuent de générer les pertes les plus élevées en 2022. Les pertes en cryptomonnaies sont passées d'environ 78 millions $ en 2021 à près de 126 millions $ en 2022. Il convient de noter que le transfert électronique Interac est un service exclusivement canadien, ce qui montre que, dans les signalements au CAFC, 34,3 millions de dollars ont été envoyés par ce mode à des fraudeurs se trouvant potentiellement au Canada.

Nombre de signalements selon le sexe



Perte en dollars selon le sexe



En tenant compte des signalements des personnes ne précisant pas leur sexe, les hommes ont présenté un nombre de signalements légèrement plus élevé que les femmes et ont également enregistré des pertes légèrement plus importantes.

Aînés (60 ans et plus) – Méthode de sollicitation selon le sexe pour la fraude à l'identité

Sexe	Nbre de signalements	Nbre de victimes	% de victimes
Femme	**1 196**	**1 190**	**99,5 %**
Fraude classique	1 182	1 176	99,5 %
Cyberfraude	14	14	100,0 %
Homme	**1 288**	**1 281**	**99,5 %**
Fraude classique	1 274	1 269	99,6 %
Cyberfraude	14	12	85,7 %
Préfère ne pas répondre/ inconnu	**26**	**26**	**100,0 %**
Fraude classique	26	26	100,0 %
Total	**2 510**	**2 497**	**99,5 %**

Aînés (60 ans et plus) – Méthode de sollicitation selon le sexe

Sexe	Nbre de signalements	Nbre de victimes	% de victimes
Femme	**10 132**	**5 403**	**53,3 %**
Fraude classique	7 089	3 634	51,3 %
Cyberfraude	3 043	1 769	58,1 %
Homme	**8 893**	**4 761**	**53,5 %**
Fraude classique	5 873	3 045	51,8 %
Cyberfraude	3 020	1 716	56,8 %
Préfère ne pas répondre/ inconnu	**399**	**255**	**63,9 %**
Fraude classique	332	214	64,5 %
Cyberfraude	67	41	61,2 %
Total	**19 424**	**10 419**	**53,6 %**

Les aînés ont été largement touchés par les méthodes classiques de sollicitation, y compris les appels téléphoniques directs. Les deux sexes ont affiché des niveaux comparables de victimisation dans les signalements. En particulier, dans les signalements des hommes, la cyberfraude continue de toucher les aînés de manière accrue. Les escroqueries classiques ont dominé dans les crimes liés à l'identité à l'encontre des aînés.

Aînés (60 ans et plus) – Méthode de sollicitation selon le sexe pour la fraude à l'investissement

Sexe	Nbre de signalements	Nbre de victimes	% de victimes	Perte financière	Perte moyenne en dollars par victime
Femme	**248**	**236**	**95,2 %**	**17 805 296 $**	**75 446 $**
Fraude classique	47	43	91,5 %	3 092 116 $	71 910 $
Cyberfraude	201	193	96,0 %	14 713 181 $	76 234 $
Homme	**597**	**575**	**96,3 %**	**57 775 076 $**	**100 478 $**
Fraude classique	122	113	92,6 %	22 625 785 $	200 228 $
Cyberfraude	475	462	97,3 %	35 149 291 $	76 081 $
Préfère ne pas répondre/ inconnu	**13**	**13**	**100,0 %**	**3 179 885 $**	**244 607 $**
Fraude classique	6	6	100,0 %	436 585 $	72 764 $
Cyberfraude	7	7	100,0 %	2 743 300 $	391 900 $
Total	**858**	**824**	**96,0 %**	**78 760 257 $**	**95 583 $**

La fraude à l'investissement commence souvent par une publicité sur les médias sociaux ou un message direct. Selon les statistiques de 2022, la fraude à l'investissement a entraîné des pertes considérables, et la plupart des pertes ont commencé par une cyberarnaque.

Aînés (60 ans et plus) – Modes de paiement pour la fraude à l'investissement

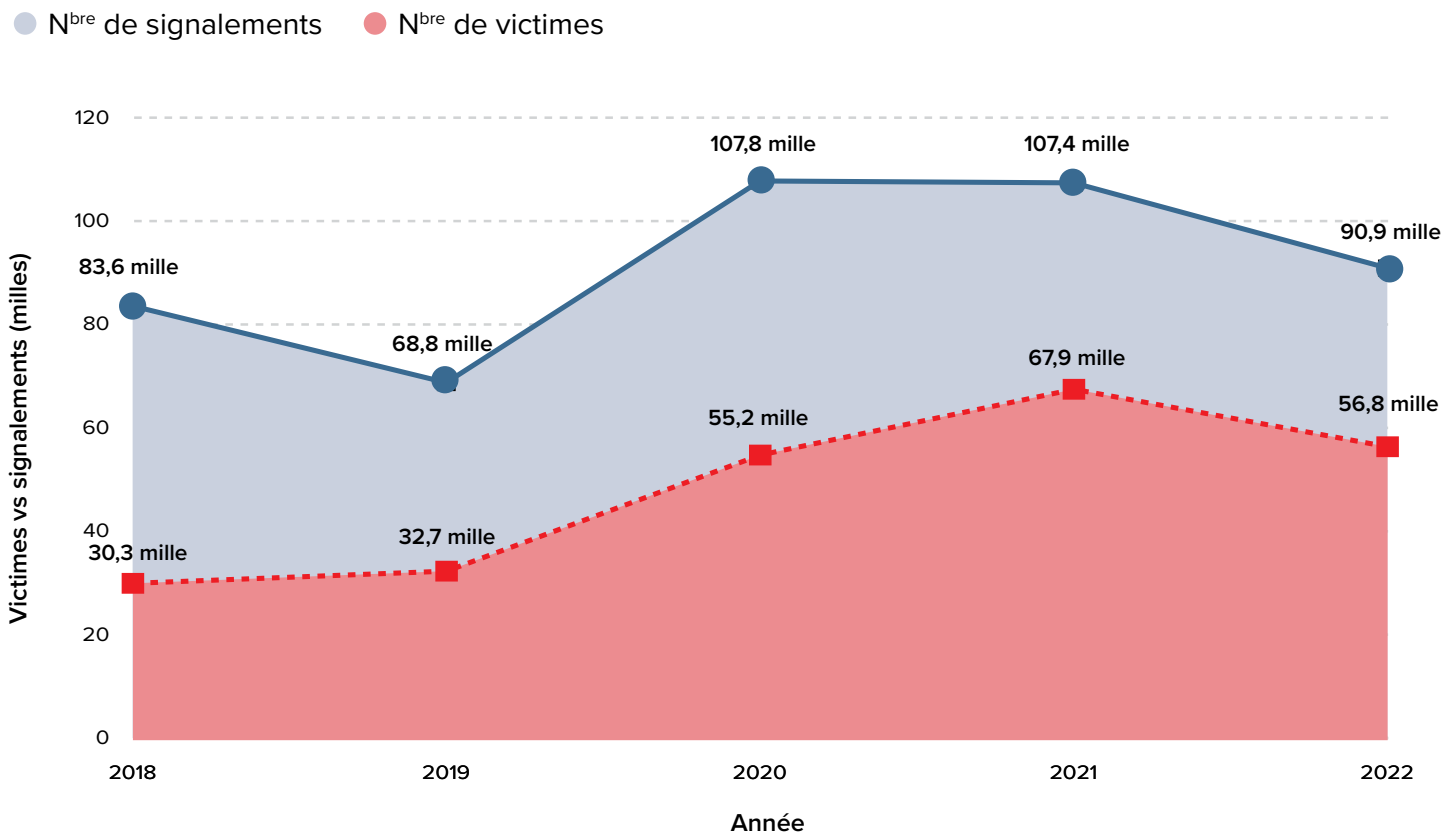
Type de fraude Modes de paiement	Investissement	
	N^bre du mode de paiement*	Perte financière
Cryptomonnaies	458	23 456 840 $
Non précisé et autre	355	29 976 874 $
Virement électronique	305	3 351 867 $
Virement télégraphique	154	19 011 904 $
Carte de crédit	127	273 543 $
Retrait bancaire automatique	20	74 943 $
Chèque/mandat/traite bancaire	18	2 396 688 $
Carte de débit	17	2 625 $
Argent comptant	11	50 000 $
Service de paiement par Internet (p. ex. Paypal)	11	53 465 $
Dépôt direct	9	59 823 $
Carte prépayée	5	500 $
MoneyGram	2	17 350 $
Ria financial	2	33 834 $
Transfert d'argent par Vigo	1	0 $
Western Union	1	0 $
Total	**1 496**	**78 760 257 $**

*Veuillez prendre note que chaque signalement reçu peut impliquer plus d'un mode de paiement.

Les cryptomonnaies continuent d'être une monnaie dominante dans la fraude à l'investissement en raison de la facilité des transferts internationaux et de la difficulté à récupérer les fonds volés avec cette monnaie.

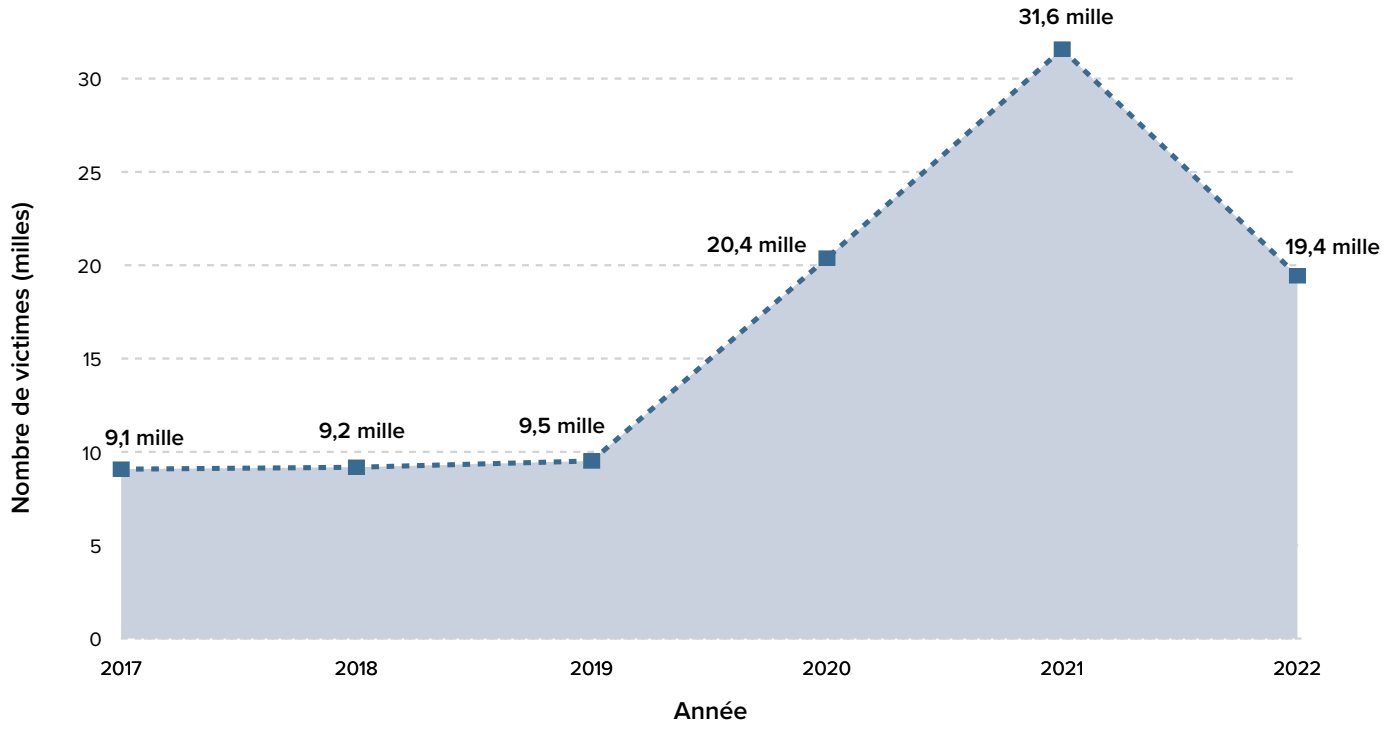
De plus, une partie des pertes par transfert télégraphique liées à la fraude à l'investissement peut être attribuée à la victime qui envoie des virements télégraphiques à l'opération de fraude dans l'espoir que le fraudeur investisse l'argent pour elle.

Nombre de signalements et de victimes par année



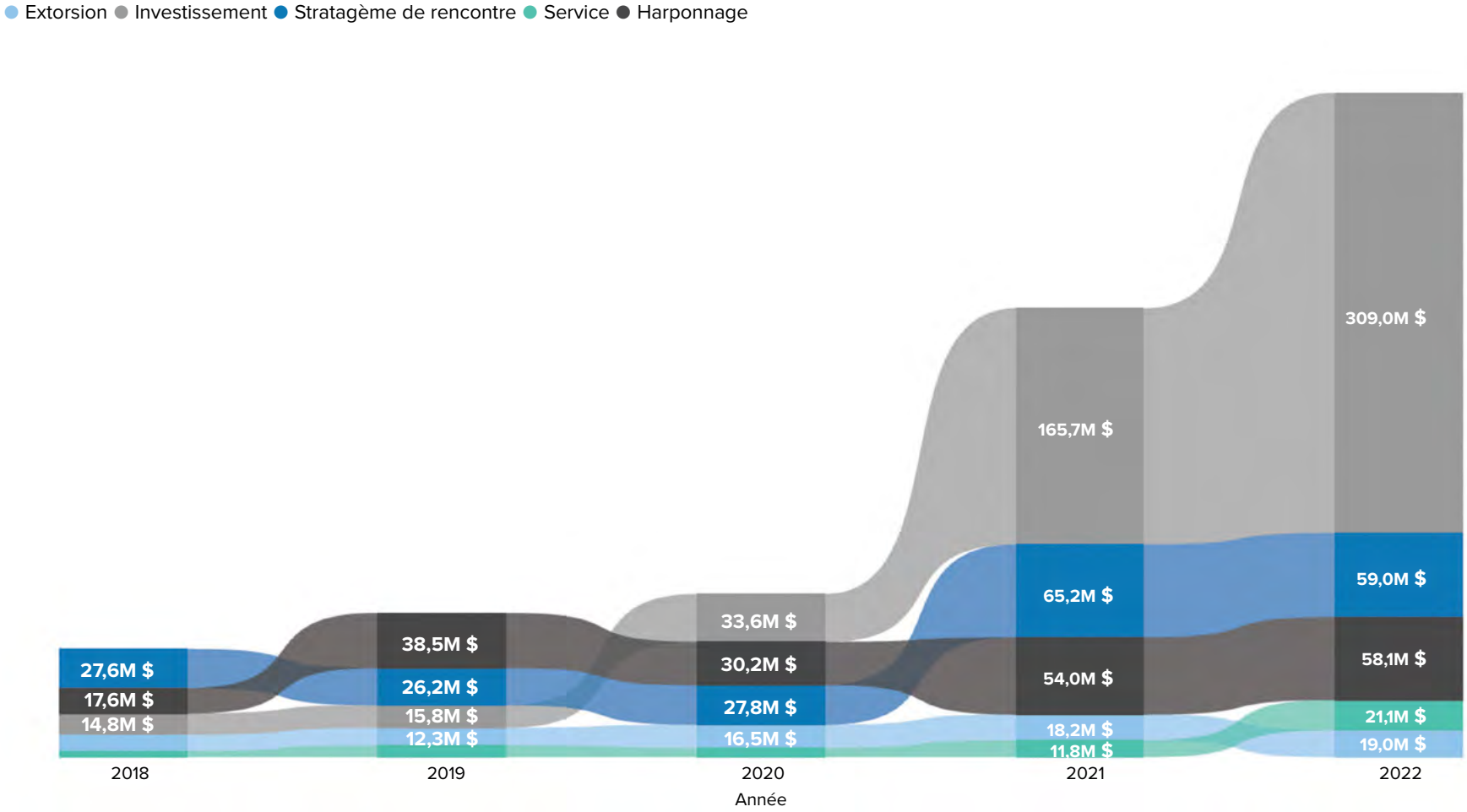
Le nombre de signalements et de victimes déclarées est demeuré relativement stable en 2022. Toutefois, le CAFC est limité par la capacité globale à recueillir les signalements. Le signalement des fraudes continue de se complexifier, ce qui entraîne une augmentation du temps consacré à la réception et à l'examen des signalements. Le SNSICF aidera à améliorer le traitement global des signalements.

Fraude à l'identité – Nombre de victimes par année



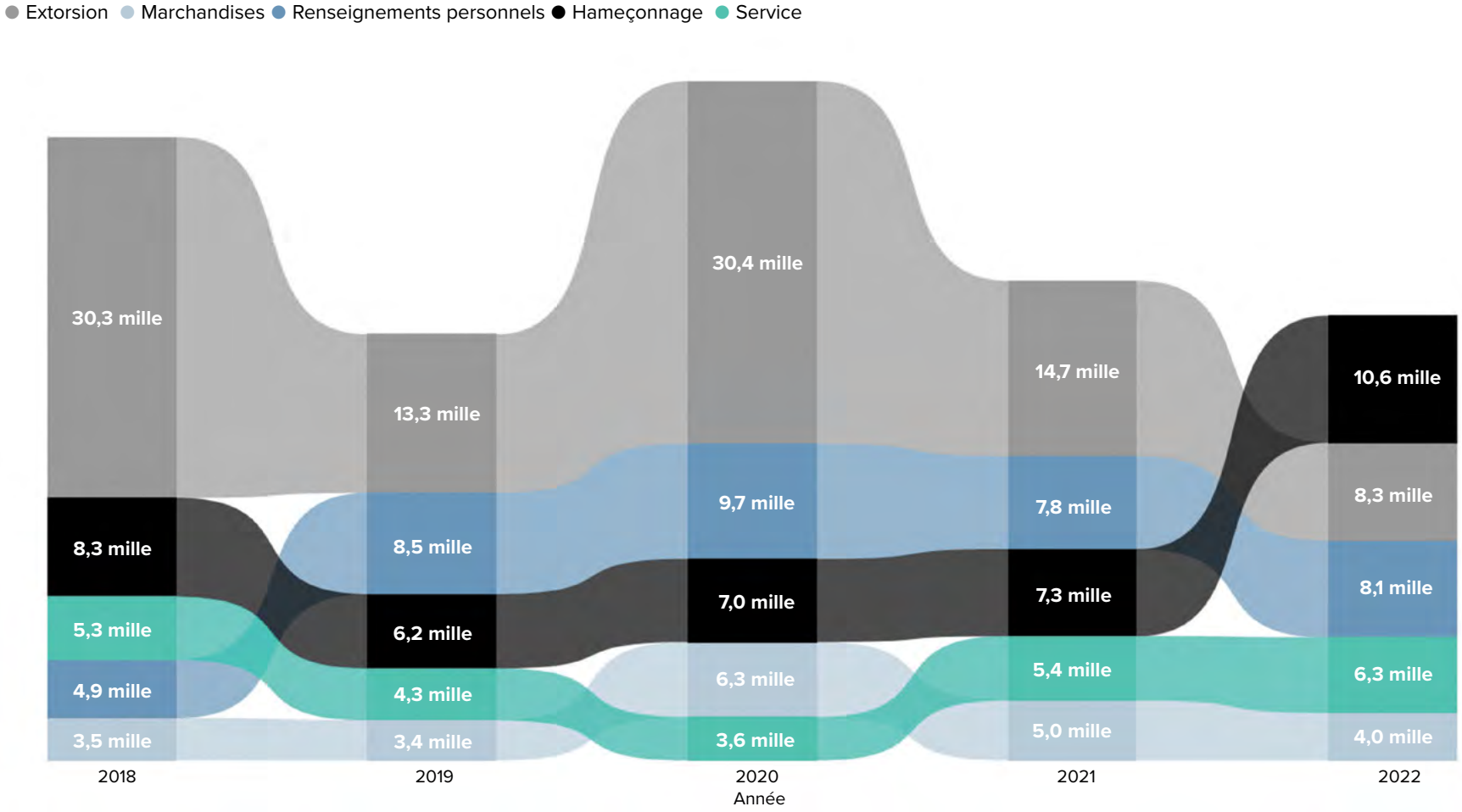
Le CAFC a continué de recevoir un nombre élevé de signalements de fraude à l'identité en 2022.

Les cinq principales des pertes en dollars par année et par type de fraude



L'une des tendances dominantes observées par le CAFC est la croissance rapide des pertes élevées et des pertes élevées dans plusieurs grands types de fraudes. Une part importante des pertes dues à la fraude est attribuable à la fraude à l'investissement, au cours des deux dernières années, ainsi qu'au stratagème de rencontre et au harponnage.

Les cinq principaux signalements par année et par type de fraude



Bien que l'extorsion entraîne davantage de pertes globales, le CAFC a reçu un nombre inférieur de signalements d'extorsion. Cela peut signifier que les opérations de fraude concentrent leurs efforts sur des cibles à impact élevé. L'hameçonnage continue de progresser, étant directement lié aux crimes liés à l'identité et au vol de renseignements personnels. Les signalements de fraudes liées aux marchandises et aux services sont demeurés relativement stables en 2022.

Les cinq principaux modes de paiement utilisés dans la fraude

Modes de paiement	2018	2019	2020	2021	2022	Total
Virement télégraphique	56 924 372 $	84 599 095 $	83 190 511 $	150 480 009 $	167 709 188 $	**542 903 175 $**
Non précisé et autre	27 386 413 $	17 019 999 $	25 480 764 $	107 038 806 $	159 104 694 $	**336 030 677 $**
Cryptomonnaies	8 643 554 $	8 248 482 $	22 540 247 $	77 564 511 $	125 911 221 $	**242 908 014 $**
Virement électronique	1 787 178 $	2 959 583 $	4 952 030 $	9 956 857 $	34 270 576 $	**53 926 225 $**
Dépôt direct	3 115 398 $	3 308 154 $	4 404 216 $	9 166 841 $	12 102 988 $	**32 097 597 $**
Total	**97 856 915 $**	**116 135 312 $**	**140 567 769 $**	**354 207 025 $**	**499 098 668 $**	**1 207 865 688 $**

Les cinq principaux signalements par province ou territoire

Province ou territoire	2018	2019	2020	2021	2022	Total
Ontario	28 257	23 166	27 345	29 962	25 595	**134 325**
Québec	15 488	14 398	18 350	21 120	20 078	**89 434**
Colombie-Britannique	8 896	6 605	9 394	9 245	8 611	**42 751**
Alberta	8 249	6 341	7 386	7 779	7 184	**36 939**
Manitoba	3 025	2 230	2 717	2 654	2 291	**12 917**
Saskatchewan	1 942	1 573	2 279	1 709	1 643	**9 146**
Nouvelle-Écosse	1 312	1 075	1 503	1 451	1 480	**6 821**
Nouveau-Brunswick	1 105	858	1 086	1 265	1 239	**5 553**
Terre-Neuve-et-Labrador	543	355	481	545	516	**2 440**
Île-du-Prince-Édouard	209	128	227	295	243	**1 102**
Yukon	66	68	68	76	105	**383**
Territoires du Nord-Ouest	42	53	60	56	37	**248**
Nunavut	29	16	30	41	22	**138**
Total	**69 163**	**56 866**	**70 926**	**76 198**	**69 044**	**342 197**

Les tendances sur cinq ans montrent que si les pertes par virement télégraphique ont connu un pic en 2021 et une baisse en 2022, les pertes en cryptomonnaies continuent de croître à un rythme très rapide, puisqu'elles sont passées de 8,2 millions de dollars en 2019 à 22,5 millions de dollars en 2020 et à près de 126 millions de dollars en 2022. Le transfert électronique est également en pleine croissance parmi les modes de paiement les plus populaires.

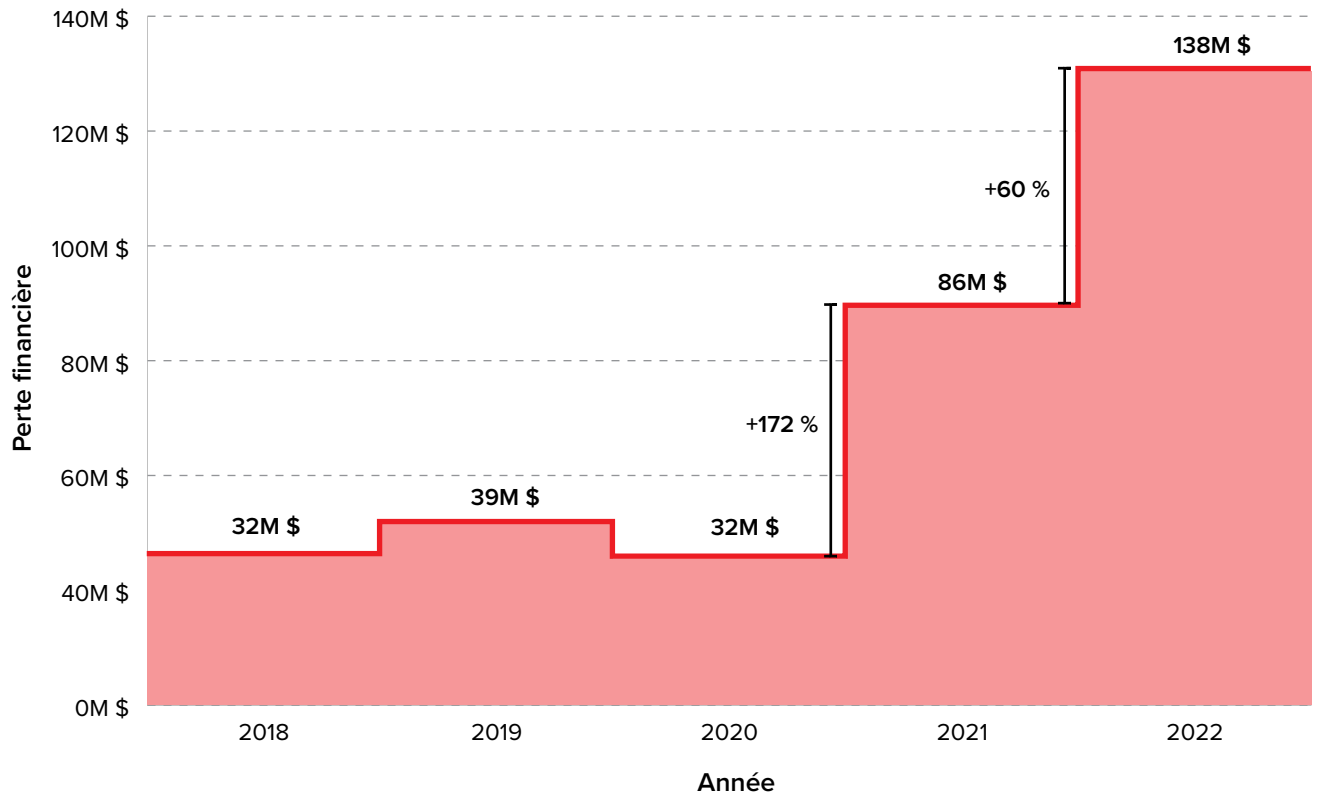
Le CAFC reçoit toujours une majorité de signalements en provenance de l'Ontario et du Québec, juste devant la Colombie-Britannique et l'Alberta.

Différence de pertes en dollars d'une année à l'autre par mode de paiement

Mode de paiement	Nbre du mode de paiement	% d'une année à l'autre – Nbre du mode de paiement	Perte financière	% d'une année à l'autre – Perte en dollars
Virement télégraphique	2 132	21,83 % ▲	$167 709 188	11,45 % ▲
Autre/inconnu	3 349	10,35 % ▲	$159 104 694	48,64 % ▲
Cryptomonnaies	5 281	-0,13 % ▼	$125 911 221	62,33 % ▲
Virement électronique	5 108	27,38 % ▲	$34 270 576	244,19 % ▲
Dépôt direct	4 954	-69,55 % ▼	$12 102 988	32,03 % ▲
Argent comptant	1 189	106,42 % ▲	$8 734 765	116,79 % ▲
Chèque/mandat/traite bancaire	424	1,92 % ▲	$8 510 772	41,85 % ▲
Carte prépayée	2 377	-13,60 % ▼	$4 702 159	20,99 % ▲
Carte de crédit	6 324	-18,05 % ▼	$3 236 031	-26,63 % ▼
Marchandises	1 337	-25,72 % ▼	$2 261 937	-60,21 % ▼
Retrait bancaire automatique	354	25,09 % ▲	$1 500 186	41,55 % ▲
Service de paiement par Internet (p. ex. Paypal)	734	-22,90 % ▼	$999 827	-35,98 % ▼
Western Union	250	-23,78 % ▼	$462 511	-23,59 % ▼
Ria financial	183	50,00 % ▲	$408 592	41,69 % ▲
Carte de débit	494	6,01 % ▲	$258 468	-74,68 % ▼
MoneyGram	137	-33,50 % ▼	$217 909	-57,54 % ▼
Transfast	11	-15,38 % ▼	$46 141	384,93 % ▲
Non disponible	62 127	-4,30 % ▼	$0	NaN
Transfert d'argent par Vigo	4	0,00 % ▬	$0	NaN

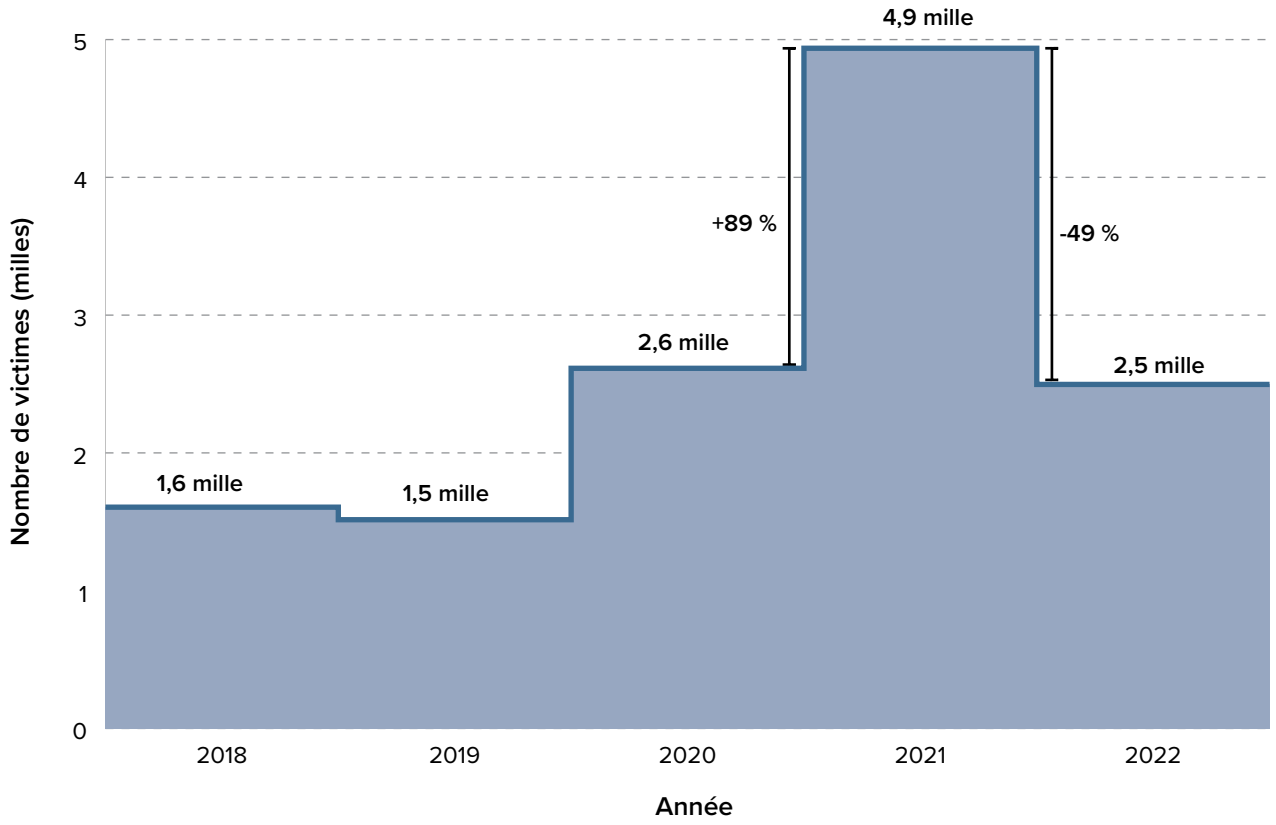
En comparant 2021 à 2022, les pertes par virement électronique et en espèces ont augmenté de manière importante, suivies par les pertes en cryptomonnaies qui ont augmenté de manière notable comme d'autres modes. Les pertes financières sont souvent associées à l'envoi de colis contenant de l'argent par des personnes âgées et des victimes vulnérables par l'entremise de services de messagerie ou de mules ou de collecteurs de fonds se présentant à leur domicile.

Aînés (60 ans et plus) – Perte en dollars par année



Sur une période de cinq ans, les aînés sont ciblés par les deux types de fraudes : la fraude classique et la cyberfraude. Le CAFC a continué d'enregistrer des pertes élevées en 2022 pour ce groupe d'âge.

Aînés (60 ans et plus) – Nombre de fraudes d'identité par année



Le CAFC a reçu un nombre inférieur de signalements de fraude à l'identité de la part des aînés en 2022 par rapport à l'année précédente, ce nombre de signalements étant comparable à celui de 2020.

www.antifraudcentre-centreantifraude.ca