



Canadian Anti-Fraud Centre

ANNUAL REPORT 2022





Royal Canadian
Mounted Police

Gendarmerie royale
du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

© His Majesty the King in Right of Canada,
as represented by the Royal Canadian Mounted Police, 2023.

ISSN: 2816-8348

PS61-46E-PDF

Connect with us at

antifraudcentre-centreantifraude.ca



[Canadian Anti-Fraud Centre | Facebook](#)



[Canadian Anti-Fraud Centre \(@canantifraud\) | Twitter](#)

Contents

Executive Foreword	2	Spear Phishing.....	31
Executive Summary	3	Extortion	33
About the CAFC	6	Sextortion.....	34
The CAFC's Core Responsibilities.....	7	Extortion Targeting Specific Ethnic Groups	36
The CAFC's Role in Enabling Investigations and Preventing Fraud	8	Emergency-Grandparent Fraud	36
Victimization and Dollar Loss	10	Romance Fraud	39
Operational Successes in 2022.....	12	Impersonation of Government Organizations	42
Coordinating Wellness Checks with Local Police Services .	13	Merchandise and Counterfeit Merchandise Fraud	43
Operational Support Efforts in 2022	13	Identity Fraud, Identity Theft, and Personal Information Theft Trends.....	44
Coordination and Deconfliction Support	13	Fraud and Organized Crime	45
Fraud Recoveries in 2022.....	13	Money Mules	46
Money Mules	15	Fraud Targeting Seniors	47
Fraud Prevention Efforts	16	New Fraud Themes	49
Senior Support Unit	17	Remote Access Software	50
Disruption Efforts	18	New Technologies Enabling Fraud	51
Examples of Operational Successes in Collaboration with Police Partners	19	Predictive and Conversational Language Models, Voice Cloning Software, and Deepfakes	51
Fraud Trends in 2022	20	Bots	52
The Digital Environment Continues to Enable Fraud	21	Update on Current Efforts.....	54
Solicitation Methods.....	22	An Update on the National Cybercrime Solution and National Cybercrime and Fraud Reporting System	54
Social Media Fraud	24	Conclusion	55
Cryptocurrency and Investment Fraud	27	About the Numbers	56
Recovery Fraud	29	Additional Statistics	57
Phishing, Identity Fraud and Identity Theft.....	30		

Executive Foreword

I am pleased to introduce the CAFC's Annual Report 2022 (the Report). This report provides in-depth trend analysis, statistics and guidance based on our observations over the past year. As part of a new CAFC partnership with the Government of Canada's Open Government Initiative, the dataset used in this report is also [published online for transparent viewing, research, and consideration](#). These datasets mark the first RCMP contribution to the Open Government Initiative.

Fraud occurs when intentional deception is used to steal money, property or information. While fraud's aim of personal or financial gain has remained the same over the years, fraudsters often change their tactics, tools, and targets to improve the potential for success. Advancements in technology are a catalyst for advancements in fraud techniques.

Canadians continue to be victimized by cyber-related fraud. In 2022, the Canadian Anti-Fraud Centre (CAFC) received over 91,000 reports totalling approximately \$530 million in losses, the highest fraud losses on record. Unfortunately, there are no signs that this trend will change.

While the past few years saw the popularity of COVID-19-themed frauds, new trends are emerging. For example, we're seeing an increase in fraudulent advertisements on social media and websites. Ads on these platforms trick users into clicking a deceptive link or contacting a fraudster, and are proving to be quite successful at victimizing Canadians. This trend is expected to continue, amongst others.

We are also seeing how emerging technology and the cyber environment are allowing for more complex forms of scams that are becoming increasingly challenging for users to recognize as fraud. Within the cyber environment, fraudsters can also more easily obfuscate their identities, impersonate friends, authority figures, or other personalities, and even create countless accounts managed by automated accounts or programs (bots).

The ever-changing fraud and cybercrime environment and increase in losses emphasizes the importance of the CAFC as a National Police Service. The CAFC provides direct assistance to Canadians and Canadian organizations impacted by fraud, deconflicts and coordinates fraud efforts with domestic and international police agencies, and engages in comprehensive fraud education and awareness efforts across Canada.

While the CAFC works tirelessly with partners to target fraud, every Canadian has a part to play. It's still estimated that only 5-10 per cent of fraud and cybercrime are reported. We need anyone targeted by a fraud to submit a report to the CAFC. Reports are essential for our efforts in prevention, awareness and disruption.

Chris Lynam

Director General

National Cybercrime Coordination Centre (NC3)

and Canadian Anti-Fraud Centre (CAFC)

Royal Canadian Mounted Police

Executive Summary

The CAFC Annual Report 2022 provides an overview of fraud reported to the CAFC between January 1 and December 31, 2022. The Report highlights significant fraud and cybercrime trends and an overview of the CAFC's ongoing efforts and responses to the current fraud environment.

The CAFC receives reports from Canadians, Canadian businesses and organizations, and international reports with a Canadian connection. These reports are stored on the CAFC-managed Fraud Reporting System (FRS) database. The CAFC analyzes reports to distinguish trends, gather intelligence, and further inform law enforcement investigations.

2022 was a significant year for Canadian fraud victimization and losses. The CAFC observed four ongoing and overarching trends during this time:

1. Fraud is leading to larger losses

The CAFC continued to observe steadily increasing fraud losses in 2022. The CAFC received nearly 91,000 conventional and cyber-fraud reports through both the Call Centre and online reporting system, totalling losses of \$530.4 million. For reference, in 2021 the CAFC observed total losses of approximately \$383 million in a comparable number of reports to 2022. Fraud losses are in addition

to the growing number of reports of personal information and identity fraud and theft, as monetary value cannot be accurately obtained in these instances.¹ Cryptocurrency-related fraud and investment fraud is also becoming increasingly impactful, with approximately \$97 million in reported losses to cryptocurrency investment fraud.

2. Fraud is becoming more personal

A common assumption is that most fraud is a distant form of crime, perpetrated by fraud operations located in other countries. Most people mistakenly believe that money is simply transferred from the victim to the fraud operation in a straightforward and simple fashion.

Domestic and international fraud operations are increasingly recruiting people located in Canada to assist in fraud. Money mules and fraud assistants visit the homes of victims and directly contact potential targets. This was a rapidly growing trend in 2022. The CAFC received many reports of fraudsters and cybercriminals openly threatening victims, and using explicit content and personal and financial information to extort victims and their families. Victims are not just losing money or information, but are also exposed to situations of psychological and emotional harm.

¹ Please see "[About the Numbers](#)" on page 56 for further explanation on why the CAFC does not produce monetary loss evaluations of identity crimes.

3. Fraud and cybercrime is targeting every age demographic

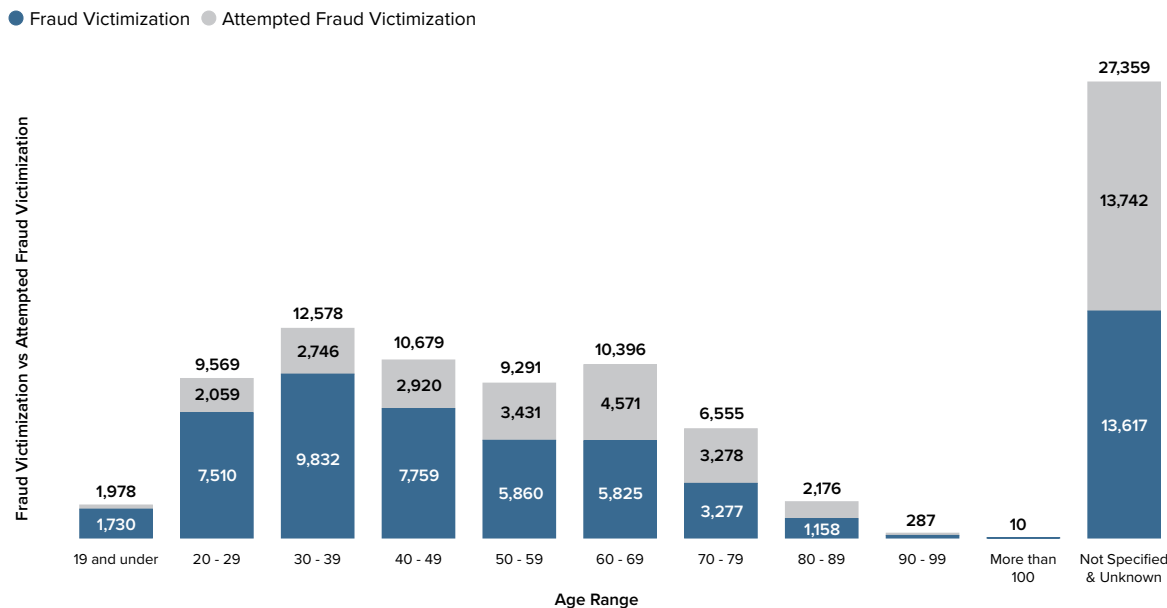
Another mistaken assumption is that fraud only victimizes seniors and vulnerable populations. Although reports by individuals aged 60+ outnumbered all other age groups in 2021, there was a drastic shift in reporting by age range in 2022. All age demographics are becoming targeted by fraud in 2022. Younger age groups are increasingly being victimized by nuanced and age-specific forms of fraud.

Fraud operations are using social media and other applications to target younger Canadians. In 2022, the CAFC received 7,510 reports of victimization from individuals aged

20 to 29, 9,832 reports from those aged 30 to 39, and 7,759 from individuals aged 40 to 49. Reports by individuals aged 20 to 49 outweighed reports by individuals aged 50-89, with this age group submitting a total of 16,120 reports of victimization in 2022.

Fraud operations are developing capacity to target all Internet users with creative forms of fraud. Since younger age demographics are most likely to be engaged online and may not have a strong understanding of fraud as a threat, they become a primary target for Internet-based fraud operations.

Number of Attempted Fraud Victimization vs Fraud Victimization by Age Range



Differing greatly from 2021, in 2022 the majority of reports of victimization received were from reporting individuals aged 20-29, 30-39, and 40-49. This demonstrates the shift towards new and successful fraud techniques through social media platforms and online applications, targeting younger Canadians.

4. Fraud is enabled by easier access to personal information

With Canadians posting more personal or specific information on accessible sites like LinkedIn, Facebook, Instagram, and Twitter, fraud operations are using this public information to create targeted and more believable fraud scenarios. Fraudsters can learn about someone's friend groups, work, career aspirations, hobbies and interests, and financial situations through these mediums. Information stolen through cybercrime can also be obtained by fraudsters. This trend leads to specific, advanced and believable fraud attempts, increasing the potential for victimization.

Furthermore, fraud schemes sent through stolen or hacked accounts to online friends and followers became more prevalent in 2022. Because of these information-sharing trends, fraudsters are more likely to have a stronger understanding about the individual prior to targeting them with more nuanced forms of fraud. In this development, identity fraud and personal information theft continue to be highly represented across all age groups, accounting for approximately 27,600 reports to the CAFC in 2022.



About the CAFC






Located in North Bay, Ontario, the CAFC was originally established in 1993 as PhoneBusters, in response to the growing threat of deceptive telemarketing practices. Today, the CAFC is the central repository for fraud information and intelligence in Canada, and is jointly operated by the Royal Canadian Mounted Police (RCMP), the Ontario Provincial Police (OPP) and the Competition Bureau of Canada.

The CAFC creates and shares timely, accurate, and useful fraud-related intelligence and information to educate and assist citizens, businesses, law enforcement, and government institutions in Canada and around the world.

As a National Police Service stewarded by the RCMP, the CAFC offers support to all law enforcement agencies across Canada. The RCMP National Cybercrime Coordination Centre (NC3) are CAFC aligned organizations under the same operational branch of the RCMP.



The CAFC's Core Responsibilities

PREVENTION	DISRUPTION	INTELLIGENCE	SUPPORT	PARTNERSHIPS
				
<p>The CAFC delivers fraud awareness campaigns, such as Fraud Prevention Month, and presentations to communities and organizations.</p> <p>The CAFC is the primary national source for fraud and identity crime material and education. Fraud alerts, advisories and prevention toolkits are posted to the CAFC website and distributed to partners regularly.</p>	<p>The CAFC works with partners, including financial institutions, credit card companies, telecommunications and Internet providers to disrupt fraud.</p> <p>Fraud disruptions serve to dismantle the tools used by fraud operations, preventing fraud before it happens.</p> <p>In some cases, the CAFC is able to help intercept fraudulent transfers before the victim loses all their money.</p>	<p>By receiving fraud and identity crime reports through the Fraud Reporting System, the CAFC can aggregate reports and provide actionable intelligence and information. This work is distributed to police of jurisdiction to enrich investigative efforts in Canada and abroad.</p> <p>The CAFC also aggregates statistics and completes reporting analyses to warn Canadians and partners of ongoing fraud trends.</p>	<p>The CAFC provides direct support to victims of fraud. Through the CAFC Call Centre, Intake Analysts provide guidance to victims of fraud and refer reporting individuals to additional services.</p> <p>The CAFC's Senior Support Unit (SSU) provides targeted support and guidance for seniors and vulnerable victims of fraud.</p>	<p>Fraud requires a whole-of-society approach, with all impacted groups, including individuals, private sector organizations, and police services, to work together in preventing fraud.</p> <p>The CAFC maintains strong partnerships with organizations like courier companies, telecommunications companies, financial organizations, and the wider police community to prevent fraud and assist in investigations.</p> <p>The CAFC manages the National Financial Crime Intelligence Sharing Group and coordinates fraud-related communication between police of jurisdiction.</p> <p>The CAFC is now partnered with the National Cybercrime Coordination Centre (NC3), working in collaboration to create the new National Cybercrime and Fraud Reporting System (NCFRS).</p>

The CAFC's Role in Enabling Investigations and Preventing Fraud



CAFC Annual Report 2022

\$530M

Reported losses to the CAFC in 2022

91,000

Reports received in 2022 through the CAFC Call Center and Website

SOLICITATION METHOD

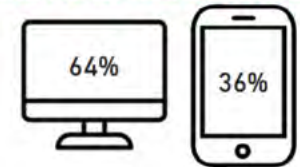
Cybercriminals are adjusting the ways they reach their victims.



In 2022, 62.4% of individuals who reported a scam to the CAFC also reported that they were victimized. Compared to 2021, the average dollar loss by victims increased by 34.6%, and totaled \$14,000 per victim.

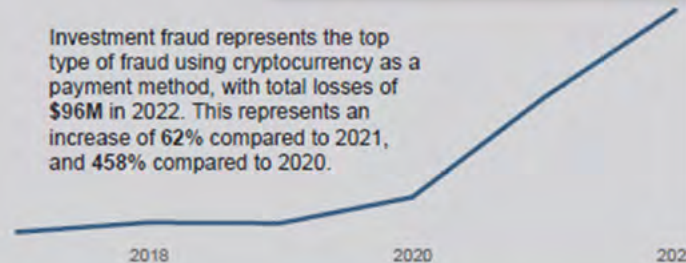


ABOUT 3 IN 5 REPORTS TO THE CAFC WERE THROUGH THE CAFC'S ONLINE FRAUD REPORTING SYSTEM.



EVOLUTION OF CRYPTOCURRENCY

Investment fraud represents the top type of fraud using cryptocurrency as a payment method, with total losses of \$96M in 2022. This represents an increase of 62% compared to 2021, and 458% compared to 2020.



Royal Canadian Mounted Police / Gendarmerie royale du Canada



Canada

Report fraud
1-888-495-8501

Victimization and Dollar Loss

Following the upward trend, 2022 continued to see unprecedented losses to fraud. The CAFC received reports of over \$530 million in losses, a historic record in CAFC reporting. For comparison, in 2021 the CAFC observed \$380 million in reported losses and \$165 million 2020.

Top 10 Fraud – Number of Fraud Reports

Fraud Type	# of Reports	% of all Reports	# of Victims	% Victimized
Identity Fraud	19,543	21.5%	19,435	99.4%
Phishing	10,647	11.7%	2,584	24.3%
Extortion	8,266	9.1%	2,330	28.2%
Personal Info	8,086	8.9%	6,155	76.1%
Service	6,309	6.9%	4,571	72.5%
Investment	4,671	5.1%	4,283	91.7%
Bank Investigator	4,255	4.7%	974	22.9%
Merchandise	4,001	4.4%	3,190	79.7%
Counterfeit Merchandise	3,993	4.4%	3,943	98.7%
Other	3,302	3.6%	673	20.4%
Total	73,073	80.4%	48,138	65.9%

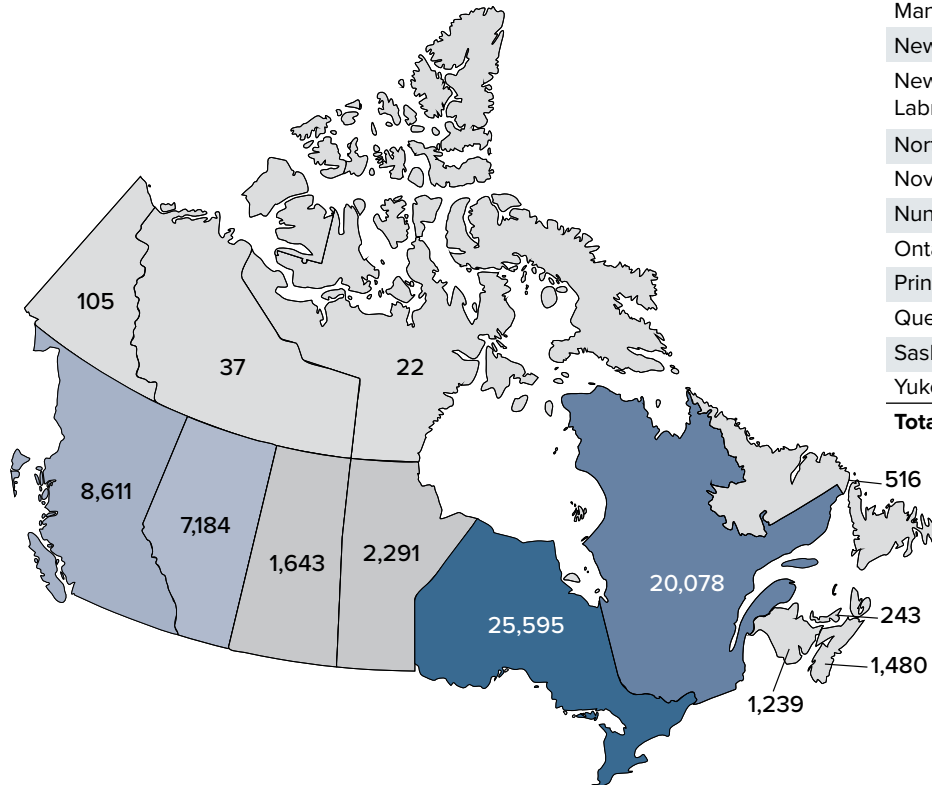
Extortion, personal information theft, phishing and identity fraud continued to be highly reported in 2022. Merchandise-related fraud was also highly reported, primarily connected to online shopping trends.

The CAFC received more than twice the total reports of investment fraud in 2022 compared to the previous year, also producing the largest losses. Romance scams and spear phishing targeting organizations also created significant losses per victimization.

Top 10 Fraud – Dollar Loss

Fraud Type	Dollar Loss	Average Dollar Loss per Victimization
Investment	\$308,977,217	\$72,140
Romance	\$59,017,857	\$55,835
Spear Phishing	\$58,090,488	\$77,765
Service	\$21,090,880	\$4,614
Extortion	\$19,049,210	\$8,176
Emergency (Jail, Accident, Hospital, Help)	\$9,424,134	\$8,513
Merchandise	\$8,787,475	\$2,755
Other	\$7,262,565	\$10,791
Job	\$7,115,019	\$4,253
Bank Investigator	\$6,743,980	\$6,924
Total	\$505,558,825	\$24,536

Number of Reports by Province/Territory



Province/Territory	# of Reports	# of Reports per Capita (100,000)	% Victimized	Dollar Loss
Alberta	7,184	169	62.7%	\$52,052,868
British Columbia	8,611	172	65.6%	\$77,029,243
Manitoba	2,291	171	63.1%	\$10,405,018
New Brunswick	1,239	160	55.6%	\$3,163,724
Newfoundland and Labrador	516	101	59.5%	\$1,415,861
Northwest Territories	37	90	54.1%	\$200,392
Nova Scotia	1,480	153	54.7%	\$3,792,630
Nunavut	22	60	63.6%	\$122,610
Ontario	25,595	180	63.9%	\$213,501,876
Prince Edward Island	243	157	60.9%	\$1,020,967
Quebec	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

Ontario and Quebec continued to submit the most reports to the CAFC. While most provinces and territories held steady reporting numbers in 2022, reports from Quebec nearly doubled from 10,479 in 2021 to over 20,000 in 2022. Ontario reporting numbers grew from 19,084 in 2021 to 25,595 in 2022. Residents of Alberta and British Columbia also submitted approximately 2,000 more reports in 2022 than 2021. “% victimized” serves to outline the total percentage of reports to the CAFC that includes a fraud victimization, as opposed to a reported fraud attempt.

Operational Successes in 2022

Coordinating Wellness Checks with Local Police Services

Being defrauded can be an extremely traumatic and life-changing event. Individuals may report fraud to the CAFC only after losing their entire savings without their family's knowledge, after selling or mortgaging their homes, or borrowing from friends and family. In some situations, people may report suicidal ideation or threaten to harm themselves when contacting the CAFC. In other types of fraud, like extortion, reporting individuals may be fearful for their lives after the fraudster threatens to harm them or their families.

When this takes place, CAFC analysts flag the files and immediately contact local police to initiate wellness checks at the identified residence. The CAFC requested local police to conduct 85 wellness checks in 2022.

Operational Support Efforts in 2022

The CAFC provides operational support to assist investigative efforts in collaboration with local police services in Canada and abroad. In 2022, the CAFC offered operational support to police services and other partners in 811 instances. Among many others, key external partners in 2022 included the Ontario Provincial Police, Winnipeg Police Service, Canada Post, EUROPOL, and the Sûreté du Québec.

Coordination and Deconfliction Support

Fraud investigations are often spread across multiple jurisdictions and borders, and individual fraud operations can target Canadians in every province and territory. To better coordinate national fraud investigations, the CAFC manages the National Financial Crime Intelligence Sharing Group (FCISG). The FCISG supports information sharing among police services and acts as a central point of contact in coordinating police investigations. In 2022, the CAFC disseminated 370 articles of intelligence to FCISG members.

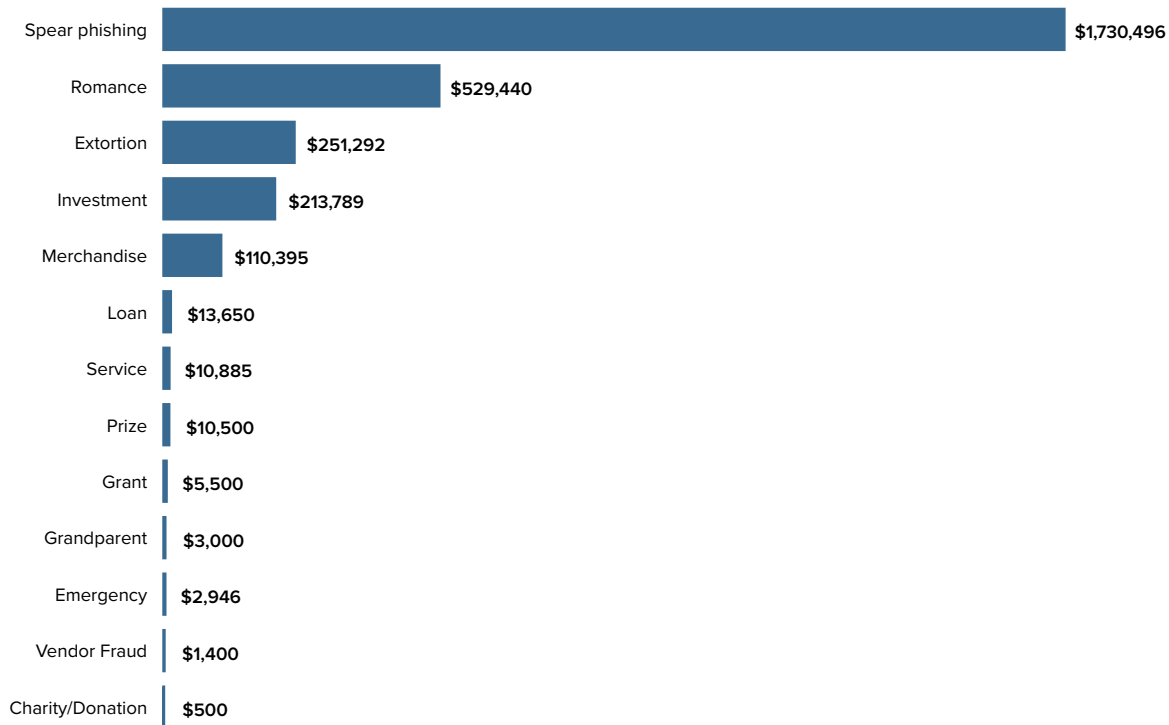
Fraud Recoveries in 2022

When someone or an organization reports a fraud occurrence, the CAFC can work with financial partners to freeze and recover fraudulently stolen money. In 2022, the CAFC assisted in 40 instances of freezing and recovering funds, leading to the recovery of \$2.9 million for victims of fraud. This includes 12 recoveries over \$100,000, and one instance of recovering \$776,000 connected to a spear phishing incident.²

The CAFC is also beginning to see positive results associated to cryptocurrency tracing services. In 2022, the CAFC successfully traced the movement of fraudulently stolen cryptocurrency to a specific exchange, and assisted in the recovery of approximately \$17,000 in Bitcoin.

² The CAFC provides actionable intelligence for law enforcement and financial partners, who then complete fraud recoveries when it is possible to do so. Although this statistic is valuable for reference, recoveries assisted by the CAFC require partners to report back on the final outcome of files. Partners may not report back to the CAFC, and this statistic is likely undervalued.

Total Amount Recovered by Fraud Type



* Amounts are converted to CAD

Spear phishing losses accounted for the majority of recovered money in 2022. Spear phishing attacks continue to produce larger losses, with fraudsters targeting businesses and organizations with nuanced email pitches and impersonation scams.

Money Mules

Fraud operations rely on money mules to transfer stolen funds. Money mules can challenge financial institutions and law enforcement efforts to track the movement of money, allowing fraud operations to transfer money to other jurisdictions or countries.

In April 2022, the CAFC was contacted by a North American courier company reporting the interception of a suspected fraudulent parcel containing \$4,500. The package was sent from an individual in Ontario to an address in Minneapolis, Minnesota. Further analysis found that a total of \$50,000 was transferred from the Ontario resident to this Minnesotan address in additional parcels.

The CAFC contacted the local police department corresponding with the American address. Local police arrived at the home, and discovered that the resident was being victimized by a romance scam. The Minneapolis victim told police that they were receiving packages on behalf of their romantic partner, an investor working in Russia. Their romantic partner requested that she deposit and transfer the money into a Bitcoin ATM. In reality, the Minneapolis victim was acting as an unwitting money mule for the suspect, their romantic partner.

The CAFC also contacted the Ontario victim's local police department. From further investigation, local police found that the Ontario victim was in an intimate online relationship with the same suspect as the victim in Minneapolis.

The Ontario victim was convinced by the fraudster that the Minneapolis victim was the suspect's "nanny," and was told to send the money to the Minneapolis address to assist with

medical bills. The Ontario victim had sent thirteen separate packages of cash to the individual located in Minneapolis. This money was then received by the Minneapolis victim, and deposited into the suspect's wallet through a Bitcoin ATM.

From further investigation, it was estimated that the Minneapolis victim accepted and deposited over \$300,000 from eleven other victims over two years.

Realizing that they were actively participating in a fraud operation, the Minneapolis victim told the CAFC they would cease all communication with the suspect and stop accepting parcels. Soon after, the suspect contacted both victims and convinced them that the CAFC was trying to break up the relationships, and that the relationships should continue.

The suspect used different names with both victims, and encouraged the victims to regularly communicate with each other to ensure the success of the money transfers. Until the CAFC and local police engaged the victims, neither had realized that they were victims of romance fraud, and were unaware that their experiences were connected to the same fraudster. This example shows that victims of fraud require consistent engagement, education and support; services led by the CAFC in partnership with local police services.

The following narrative from a CAFC file in 2022 demonstrates the interesting qualities of money mule activity:

Fraud Prevention Efforts

The CAFC is a co-chair of Fraud Prevention Month (FPM) every March, working with key partners like Competition Bureau Canada and Ontario Provincial Police (OPP) to educate Canadians on fraud. In the 2022 Fraud Prevention Month, the CAFC provided:

- 24 presentations to community groups and partners, including multiple presentations to Ukrainian refugees in Quebec on fraud prevention
- Educational material through Facebook and Twitter posts
- Material posted through the CAFC website
- Bulletins and toolkits to over 700 partners
- 421 responses to media requests

Demonstrating the value of the FPM campaign, the CAFC's official hashtags #FPM2022 (English) and #MPF2022 (French) reached approximately 30 million Twitter accounts and 11.5 million Facebook accounts.

While Fraud Prevention Month is one of the CAFC's larger awareness campaigns, the organization also led a Money Mule Awareness Campaign in partnership with the OPP and RCMP, participated in Cyber Security Awareness Month, led a Holiday Scams campaign, among other campaigns.

Through our Facebook and Twitter accounts and website, the CAFC regularly shares fraud awareness and educational material to thousands of followers.



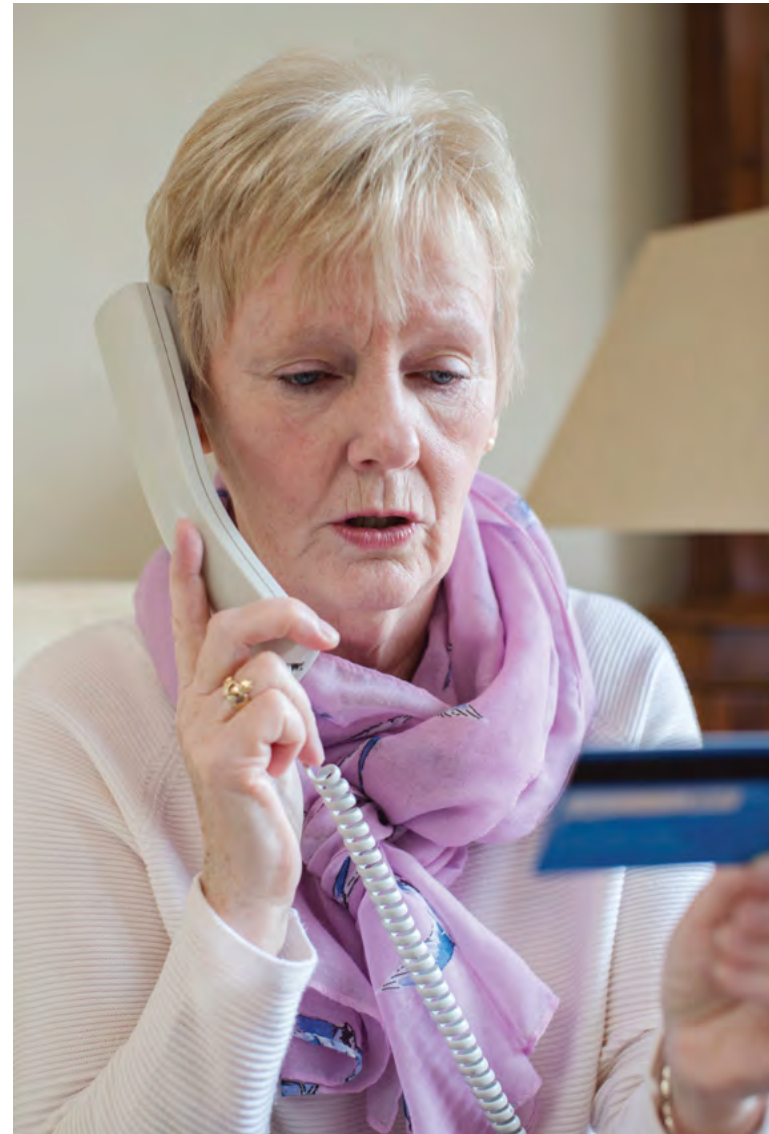
Connected to fraud trends, the CAFC provides key perspectives to media articles in advancing public awareness of fraud. Some examples from 2022 include:

- [Grandparent scams are on the rise. Here's how you can protect yourself \(CTV News\)](#)
- [10 common crypto scams and how to avoid them \(MoneySense\)](#)
- ['Protect your wallet and your heart,' warns woman after finding Ontario beau's romance scam links \(CBC News\)](#)

Senior Support Unit

The CAFC Senior Support Unit (SSU) is supported entirely by volunteers dedicated to reducing the impact of fraud across Canada. The SSU is a critical component of the CAFC, providing advice, education and reassurance to vulnerable Canadians targeted by fraudsters. The SSU receives reports referred by the Intake Unit, after identifying that further assistance for a senior or vulnerable individual is needed.

In 2022, the SSU managed 698 reports and gave 80 presentations, providing direct outreach and engagement across Canada.

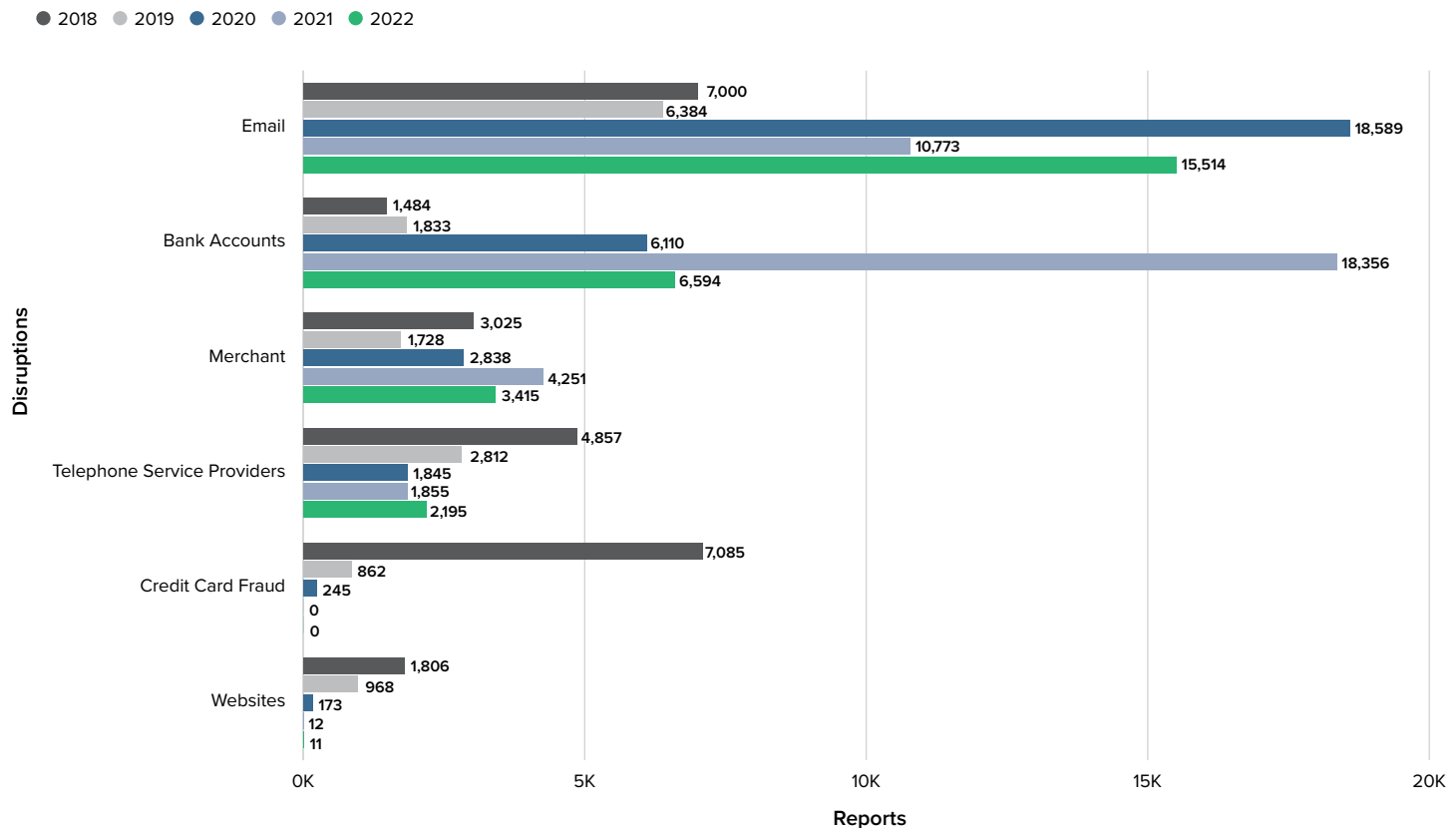


Disruption Efforts

The CAFC works closely with law enforcement, federal partners and industry to disrupt fraudulent activity. To disrupt fraud, the CAFC receives and shares critical information from fraud reports, works with partners to remove fraudulent addresses, bank and credit accounts, business accounts and telephone numbers from their respective systems. In 2022,

the CAFC’s operational focus was the disruption of fraudulent email addresses, bank accounts, merchant accounts, and telephone numbers through collaboration with telephone service providers. These efforts are significant due to their ability to disrupt criminal infrastructure that may get reused for several victims. This disruption creates friction for the fraudster, making it more difficult to conduct criminal activity.

Number of Disruptions by Year



Examples of Operational Successes in Collaboration with Police Partners

Operation Eagle Sweep

Domestic and international police partners frequently ask the CAFC for investigational support through information and intelligence sharing from their repository of reports. The CAFC's information can be included in wider investigations, potentially leading to the arrest of fraudsters and the termination of fraud operations.

In one example, the CAFC led coordination efforts related to Operation Eagle Sweep, an international investigation of a global Business Email Compromise (BEC) operation led by the United States Federal Bureau of Investigation (U.S. FBI). In this role, the CAFC coordinated assistance efforts by Canadian police services and shared information connected to Canadian victimizations. The investigation led to the arrest of two individuals located in Canada.³

Transnational Tech Support Fraud Arrests

Canadians continue to be impacted by tech support fraud. In this scam, fraudsters will contact victims by telephone, through online advertisements, or email, to warn that there are issues with their computer. These coordinated fraud operations frequently target seniors or vulnerable victims who have limited digital literacy.

As law enforcement is observing, instances of fraud are often connected to international fraud operations targeting Canadians. To address this, law enforcement and partners need to coordinate, share information and work together. In an example from 2022, the CAFC assisted in a tech support fraud investigation led by Peel Regional Police, United States and Indian law enforcement, which led to the arrest of one individual located in Canada, one in the United States, and three individuals located in India.⁴



³ [Coordinated Global Operation Disrupted BEC Schemes — FBI](#)

⁴ [Search Warrant Executed in International Fraud Investigation](#)

Fraud Trends in 2022

The Digital Environment Continues to Enable Fraud

Canadians continue to spend more time online. In 2022, 54% of Canadians spent more than five hours per day online, and an additional 24% spent between three and four hours per day online.⁵ More than ever before, the Canadian life is intrinsically connected to the digital world.

Canadians are increasingly using the Internet to shop, with online purchasing of goods and services rising from \$57.4 billion in 2018 to \$84.4 billion in 2020.⁶

Canadians are using the Internet for communicating and connecting with each other. Over 70% of Canadians are using social media and a further 76% of Canadians communicate through instant messaging apps.⁷

Furthermore, working from home is quickly becoming a permanent reality for many Canadian workers. A third of Canadian businesses offered employees the opportunity to telework during the COVID-19 pandemic, and there is the potential for this to continue as we move beyond the pandemic.⁸

While Canadians continue to develop a strong link to the cyber environment, it is understandable that more Canadians are, and will continue to be, targeted by malicious cyber threats, including fraud and identity crimes.

Phishing and spear phishing, which targets both business/corporate and personal email addresses, is one of the primary methods for malicious cyber actors to access corporate systems, steal corporate and personal information, and engage in fraud. Phishing was the most-reported type of fraud reported to the CAFC in 2022, with over 10,600 reports. Spear phishing is also strongly represented in 2022, with over 1,500 reports totalling over \$58 million in reported losses.

Fraudsters engaging in counterfeit merchandise and merchandise fraud are using Canadians' online shopping habits to their advantage and adapting their lures to align with emerging trends. Social media is also strongly represented as a dominant platform for distributing fraud schemes to a wide subset of the Canadian population.

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

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*.

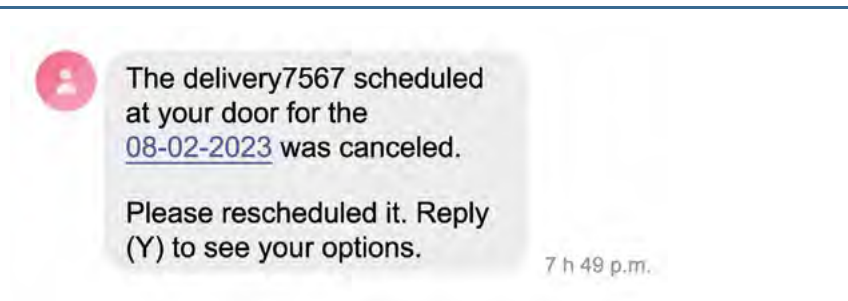
7 Ibid.

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*.

Solicitation Methods

The CAFC observed similar numbers of reporting by solicitation method (how the fraudster first contacts victims) from 2021 to 2022. Telephone and telecommunications continued to be the most popular form of initial solicitation by a small margin, although reports with the Internet as the solicitation method led to far more victimizations.

Within telecommunication technology as the solicitation method, the CAFC continues to see texting become a more popular method of fraudsters reaching out to potential victims.

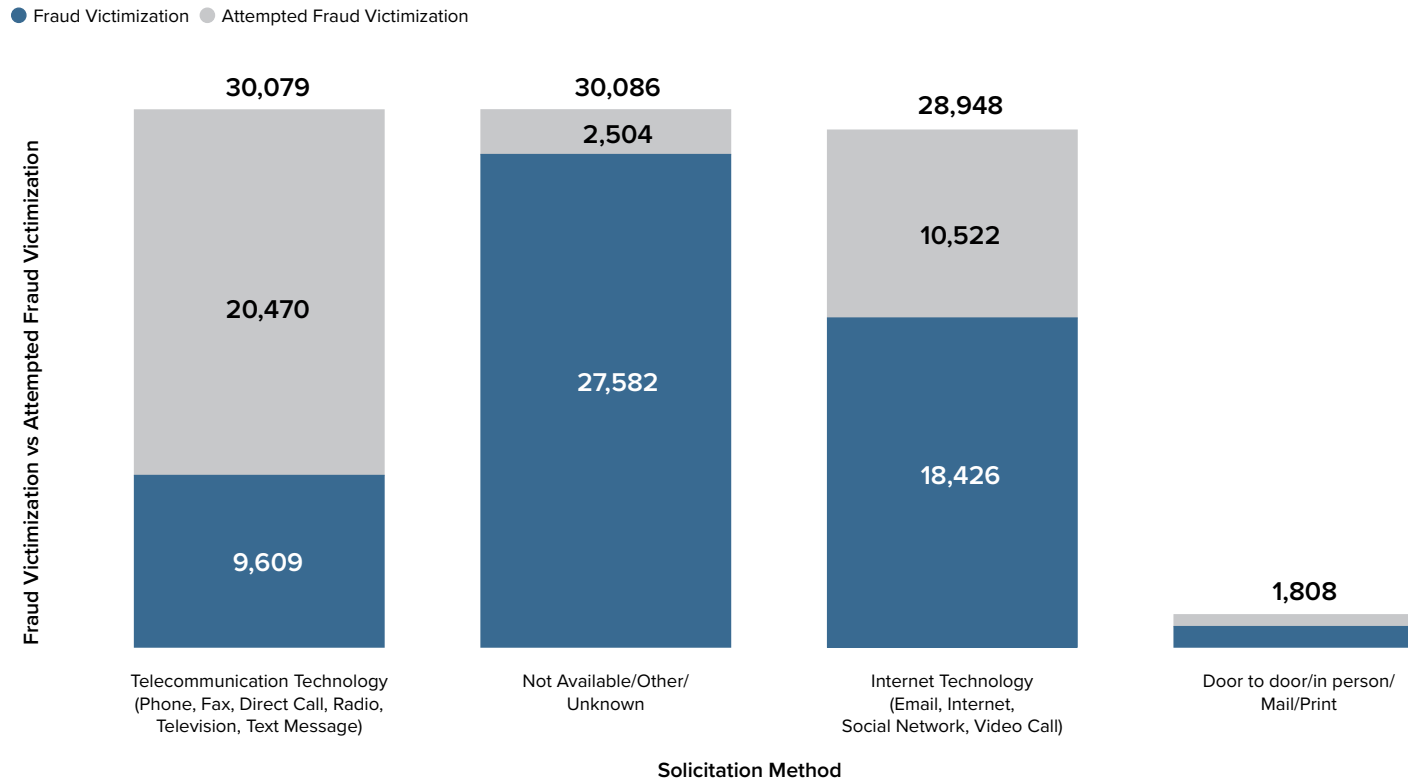


Fraud operations are using automated text messaging services and technology to distribute fraud pitches to a large number of Canadians, with extremely low operational costs.

From the example, if the recipient replies to the message (usually can be any form of reply), the text will be followed up with a fraudster calling the number and continuing the pitch.



Attempted Fraud Victimization vs Fraud Victimization by Solicitation Method



Solicitation method statistics were largely similar from 2021 to 2022. However, reports of Internet technology as the initial pitch were connected to significantly more victimizations. Telephone scams are often more intrusive and annoying than Internet scams, so individuals are therefore more inclined to report attempted telephone scams than attempted Internet scams.

Social Media Fraud

With Canadians spending a large amount of time on sites like Facebook, Twitter, Instagram and TikTok, fraudsters and malicious cyber actors are also using these sites to initiate many forms of fraud. With the massive amounts of information regularly posted on these sites, users are increasingly challenged with differentiating between legitimate and fraudulent accounts, pages, advertisements, and conversations. As most social media platforms are free to use, they are an inexpensive method for fraudsters to target Canadians with fraud.

As Canadians are putting more personal information online and are connecting to their personal friend groups through social media sites, fraudsters and threat actors can find detailed information to customize fraud attempts against them.

With likes, follows, retweets and comments being public knowledge, fraudsters can develop an understanding of individual social patterns and habits. Fraudsters can find a user's close friends and learn about their relationships and interests. This includes past jobs, schools attended, hometowns and places of residence, among other detailed information. This information is the perfect background for fraudsters to begin complex and sophisticated forms of fraud.

For instance, Canadians use sites like LinkedIn to display their career development and search for jobs. Taking advantage of this opportunity, fraudsters build fake LinkedIn profiles that appear like a hiring manager or employee within a company, and send unsolicited direct messages and engage with users. This creates the opportunity for job scams, other forms of fraud, and money mule recruitment.⁹ In another example, fraudsters can easily impersonate friends, coworkers and acquaintances online, particularly if personal information is accessible. Impersonating someone can create an illusion of trust, and further exploit the wider friend group.

Younger Canadians tend to engage with social media far more than any other age demographic. In 2022, the CAFC observed an alarming trend of fraud enabled by these platforms, particularly against individuals younger than 30. The CAFC encourages Canadians to develop a strong awareness of potential threats online, and for parents to discuss potential online threats with their children.

⁹ Bond, Shannon. (March 27, 2022). ["That Smiling LinkedIn Profile Face Might be a Computer Generated Fake."](#) *NPR*.

NARRATIVE OF A SOCIAL MEDIA FRAUD REPORT

“A friend on Instagram messaged me directly to ask if I am interested in Bitcoin investing, and that she has a friend who can mentor me. I created a Shakepay account to send the funds from my personal bank accounts to invest on a trading website.

They showed me how I can purchase fractions of Bitcoin and submit it to my trading account, and I transferred some money from my personal account on Shakepay to a cryptocurrency wallet address. The person said that I made a profit, so I requested to withdraw to see. They said that I needed a PIN which would require a fee. Using the same process, I sent money to obtain the PIN.

Then they said to withdraw the amount I wanted, I would need to upgrade my trading account. So I used the same process using Shakepay to send the funds. I sent money from both my chequing accounts and a line of credit.

Soon after, I realized there was something off when they said that they are unable to send the funds as there was a commissions fee to be paid.

This morning, they messaged me again saying that they have a way to get my funds without paying the \$4,500 fee. They sent a link to me via text which I saw right away that they were trying to access my phone. I denied the request and changed my password. I contacted the friend that referred this account manager, and she had posted a story on her Instagram saying that she was hacked.”



How to protect yourself from social media fraud

- ▶ Frequently review and update your privacy and account settings, to limit the amount of information accessible to the open Internet.
 - ▶ Do not respond to unsolicited contact by a stranger, and when possible, ensure that you can verify the identity of the person you are talking.
 - ▶ Never share personal information or send money to someone you do not know online, and when possible verify the authenticity of products or services you are exchanging money for online.
 - ▶ Search for duplicate accounts to ensure that your account is not being impersonated.
 - ▶ Stay up-to-date on new social media fraud pitches, shared on the [CAFC website](#).
-

How fraudsters leverage social media

- ▶ Posting fraudulent advertisements, attracting users to contact them or click on links to fraudulent websites.
 - ▶ Running fake or bot accounts, using automated processes to contact users through direct messages.
 - ▶ Managing fraudulent groups or web pages on social media platforms.
 - ▶ Selling fake or nonexistent goods and services, facilitating merchandise fraud.
 - ▶ Initiating contact with users with specific fraud pitches and themes (e.g. engaging in romance fraud on dating sites).
 - ▶ Using social media as a platform to begin initial contact with potential victims.
-

Cryptocurrency and Investment Fraud

Cryptocurrency is a fast, easy, and efficient way to transfer currency around the world. Canadian and international cryptocurrency exchanges, as well as cryptocurrency Automated Teller Machines (ATMs), are making it easier to exchange and transfer cryptocurrency and cash.

While this is beneficial for law-abiding users, cryptocurrency continued to be a strong fraud enabler in 2022.

Cryptocurrency was the second-most common form of payment method used in fraud in 2022, and it continues to quickly grow at a faster pace than other payment methods. In 2022, the CAFC received 5,281 cryptocurrency-related reports totalling \$125.9 million in losses, and was particularly prevalent in instances of fraud with high losses.

Cryptocurrency can often be used in a more anonymous manner, and the likelihood that cryptocurrency lost to fraud will be recovered is significantly lower than other forms of payment methods. Additionally, unusual cash-based transactions or wire transfers are more likely to be flagged as potentially fraudulent and frozen, than when exchanging large amounts of cryptocurrency.

The CAFC continues to observe the ongoing trend of cryptocurrency investment fraud. In 2021, the CAFC noted that cryptocurrency investment fraud became a dominant reported fraud type, leading to significant reported losses and victimizations. In 2022, the CAFC received a total of 2,851 cryptocurrency investment fraud reports, and this is by far the most prevalent type of investment scam. The average loss per investment fraud victimization was also higher than most forms of fraud impacting individuals, with an average reported loss of over \$72,000.

Cryptocurrency was by far the most significant form of payment method for investment fraud.

Payment Methods for Investment Fraud

Fraud Type Payment Methods	Investment	
	# of Payment Methods*	Dollar Loss
Cryptocurrency	2851	\$96,731,847
Not Specified & Other	1898	\$115,620,554
e-Transfer	1430	\$24,556,346
Wire transfer	579	\$63,739,890
Credit card	438	\$571,200
Debit card	114	\$107,497
Automatic Bank Withdrawal	88	\$827,591
IPS - Internet Payment Service (ex. Paypal)	80	\$257,819
Direct deposit	71	\$1,868,791
Cheque / Money Order / Bank Draft	59	\$4,029,386
Cash	38	\$576,972
Prepaid Card	17	\$1,550
Western Union	11	\$33,078
Ria financial	7	\$36,680
Moneygram	5	\$17,950
Merchandise	2	\$0
Transfast	2	\$66
Vigo money transfer	1	\$0
Total	7691	\$308,977,217

* Note that each report received can have more than one payment method.

With the growth of decentralized finance and accessible investment apps and platforms, Canadians are becoming more comfortable with investing online. Combined with the promise of high returns and the appearance of legitimacy, Canadians are losing more money to investment fraud than ever before. In 2022, the CAFC received a total of 4,671 investment fraud reports, leading to approximately \$309 million in total losses.

Investment fraud is frequently initiated through advertisements on social media, in video or website conversations. Fake online reviews are also used to create the appearance of legitimacy.

While cryptocurrency investment scams frequently use generalized names like “Bitcoin-Unlocked-Financial,” investment fraud is also impersonating well-known and reputable Canadian financial institutions and companies to create a sense of trust. This can include spoofing or impersonating websites and contact information, and building websites the look similar to authentic websites.

NARRATIVE OF AN INVESTMENT FRAUD REPORT

“I heard an advertisement on a podcast that I receive regularly via email. A new form of trading has been created, and you can buy in countries with high speed Internet and sell in countries with lower speed Internet before price changes on the chart.

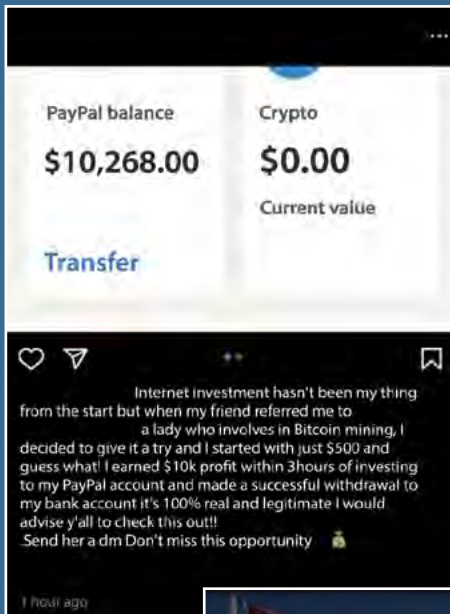
I contacted the business on August 22, signed up with \$250.00 via credit card. My account started showing good percentages so I invested more.

The Personal Advisor kept suggesting daily to invest more money for bigger gains. I have been day trading 22 months on my own, and his trades seemed legitimate. I could see them when looking back over the chart. So I eventually invested a total of \$8,500 in the account.

Later, the Advisor repeatedly called me and told me to borrow money to invest. At this point, I realized that this could be a scam.

I have been requesting account closure with my money returned. No one will answer my calls or emails. If I call from another phone, the call is picked up and immediately disconnected.”

Investment fraudsters are using streaming advertisements and social media to distribute fraud attempts. This includes hacking into and impersonating real user accounts to send fraud attempts to friends and followers.



Recovery Fraud

Closely linked to investment scams and cryptocurrency fraud, recovery fraud takes place after someone has already been defrauded. A victim will be contacted by a fraudster promising to recover the lost money for a fee. In some cases, they will state that they noticed a “dormant unused account,” and will offer assistance to return money. Victims will likely be asked to pay a fee before receiving any service. In 2022, the CAFC received 221 recovery fraud reports totalling \$2.5 million in losses.

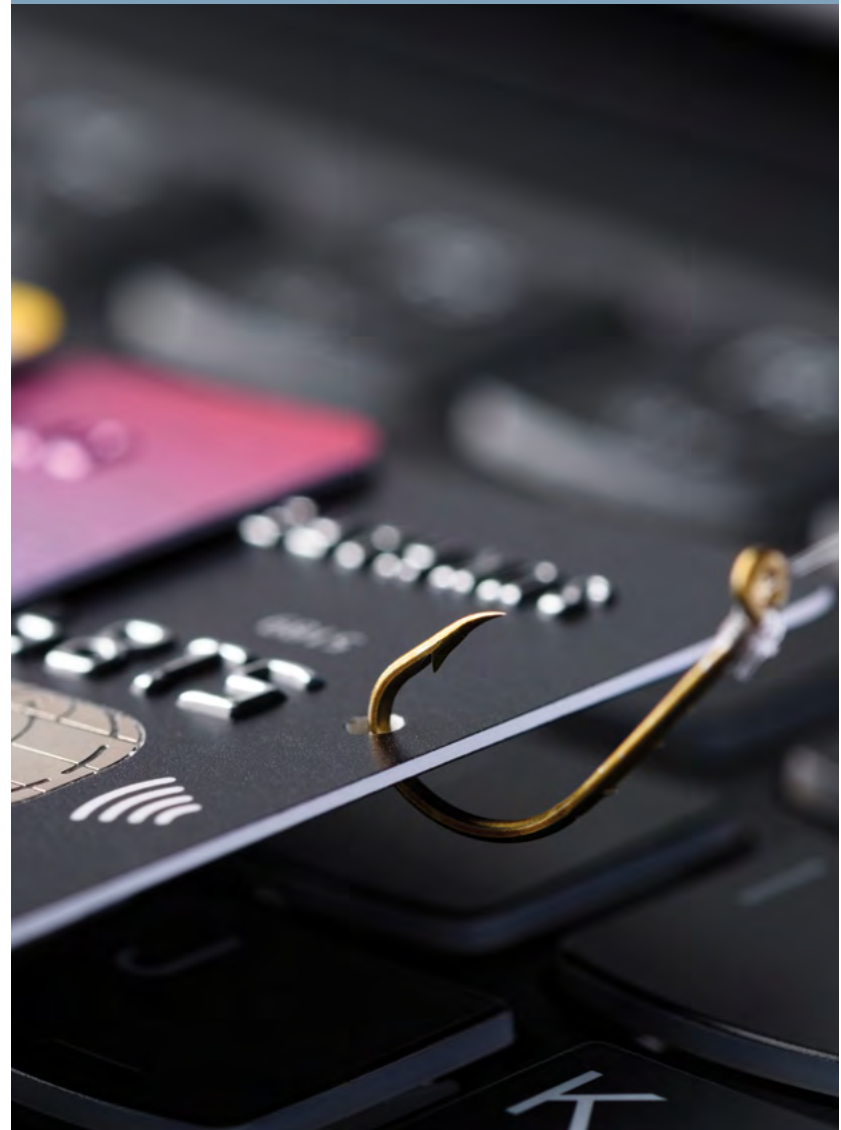
In many circumstances, the recovery fraud is linked to the original fraud, and this is an attempt to continue the victimization. The fraudster may know about the amount of money lost and additional personal information. Fraudsters frequently contact victims with alternative types of fraud and recovery scams in an attempt to continue the victimization. They will also use new contact information to appear unrelated to the previous fraud.

Phishing, Identity Fraud and Identity Theft

Phishing is one of the highest reported types of fraud. Whether receiving text messages or emails asking to respond or click on a link, these attempts serve to initiate other forms of fraud, steal personal information, or install malware and viruses. In 2022, the CAFC received 10,647 phishing reports.

Through phishing attempts, the fraudster can obtain personal information such as copies of driver's licences, health cards and Social Insurance Numbers (SINs), and financial information such as credit card and bank account details. As such, phishing is closely linked to identity theft and fraud. Alternatively, phishing resulting in malware installation on electronic devices may also lead to the theft of personal information without the victim's direct knowledge.

In 2022, a growing trend is the widespread distribution of automated texts, with fraud operations waiting for a response prior to calling the victim back. The CAFC observed an increase in identity theft and fraud reports, receiving 19,543 reports in 2022. Seniors and vulnerable populations are especially susceptible to identity theft and fraud. In 2022, the CAFC received 2,510 reports from victims over the age of 60.



NARRATIVE OF A PHISHING REPORT

“I was emailed by a phishing scam posing as my credit card company. The banner and overall email appeared 100% legitimate, including the banners, logos, and typeface.

I have received emails from them before, but don't recall it appearing this way. The company stated that they just upgraded our cards and branding, so I thought it was part of that. It also was marked as time-sensitive, so I clicked on the attached link, and it redirected me to an Amazon link. I wasn't sure if this was a mistake on my part somehow, so I clicked it again, and it redirected me to the same Amazon link.

On 2 December 2022, my credit card company called me to let me know my card had been used and the charge is uncharacteristic. We then discovered that my credit card had been used, discussed how this may have happened, and realized that it was through the email I had received.”

Spear Phishing

Spear phishing is the targeted version of phishing. In spear phishing, fraudsters and cybercriminals targets specific victims with detailed phishing attempts. While phishing often entails distributing generalized phishing lures to many potential victims, spear phishing includes sending customized information to a specific audience for greater potential gains.

Targeting businesses, governmental and public organizations, and individuals, spear phishing is becoming an increasingly prevalent and significant form of financial crime. In 2022, the CAFC received 1,548 reports totaling \$58.1 million in losses, compared to 1,852 reports and \$54 million in losses in 2021.

Spear phishing is a threat that can lead to significant losses by organizations and individuals. Most businesses, especially small-and-medium sized companies (SMEs), publish accessible information about their mandate, business practices, services offered, and management names, titles, email addresses and responsibilities. Fraud operations can also pull information about specific employees from their social media pages or blogs. All of this key information can be lifted to create detailed spear phishing attempts.

Although nuanced and detailed information may lead to a greater chance of spear phishing victimization, reporting trends show that spear phishing attacks can be successfully completed with limited and basic information found online.

Businesses rely on other businesses to support their respective organizations, from providing supplies and logistical support, to software and hardware implementation.

Businesses often share contacts, financial information and other specific details to a variety of associated companies and suppliers.

A spear phishing attack can begin with a malicious cyber incident against one of these connected businesses, leading to the theft of client or partner information. After this

information is stolen, it can be used to create a sophisticated spear phishing attempt against associated businesses, especially if the company did not know that their information was previously stolen. Spear phishing attempts targeting organizations, particularly in connection to corporate functioning or the payment of invoices, is also known as Business Email Compromise (BEC).

NARRATIVE OF A SPEAR PHISHING REPORT

“I received an email from our supplier with an invoice attached and I replied with a “thank-you.” This is a normal and frequent occurrence. Several days later, we received a reply to that email from the same person asking when the payment would be made. I responded by stating that the invoice would be paid next week, and we would also follow up when it was paid.

A week later, we received an email from our supplier, stating that they have recently switched their banking details and need all future payments made to the new account. There was a signature in the email which was from the person we normally deal with and it contained identical information that the person normally has in their signature.

We sent a form back to the correct email address, requiring a signature from an authorized official. The form was completed with all the details and sent back with the authorized signature and a void cheque, which is also required. We updated our banking details and paid the most recent invoice to this company via direct deposit.

I received another invoice via email seven days later from the same email address and I responded with another “thank-you.” Both invoices were correct and from the right person. Later that week, I received a reply to the email with the invoice, from the same email address asking when payment would be made for this invoice. This correspondence also contained the right email address, correct invoice number and signature details of the person we frequently worked with. I responded saying, “You will receive a payment notice, should be tomorrow.” We then paid this invoice as well.

A week later, we received an email from same email address saying they just found out their corporate email accounts were hacked, and did not send emails saying their banking details changed.”

Extortion

Extortion is the practice of obtaining money through threats or intimidation. It continued to be one of the most reported forms of fraud to the CAFC. In 2022, the CAFC received 8,266 reports of extortion, totalling approximately \$19 million in losses. Although total extortion reports to the CAFC have been declining since 2018, dollar loss and loss-per-victimization have consistently increased into 2022.

In 2022, the CAFC observed the ongoing trend of extortion targeting specific groups of Canadians. For instance, seniors are being targeted with direct threats to harm them and their family members.

In other situations, the fraudster may resort to threatening the individual when they do not comply with the initial fraud attempt. Information like personal addresses, family member names, or other personal information to scare potential victims is being used in extortion.



Sextortion

Online extortion and sextortion continued to be impactful in 2022. Sextortion, or online sexual exploitation, is when a victim is tricked or encouraged to participate in or observe online situations of a sexual nature. These encounters are then recorded or captured without the victim's knowledge. The fraudster threatens to send the recorded material to friends, family members, or work colleagues if money or additional images are not sent.

Social media can allow fraudsters to develop an understanding of someone's social circles and enable communication between threat actors and potential victims. Social media platforms are commonly used in sextortion.

In 2022, the CAFC observed more reports of sextortion targeting teenagers and younger victims, particularly through online video games, chat groups and social media. Threat actors may impersonate a younger individual to slowly develop trust or begin a virtual relationship.

Like extortion and other forms of fraud, sextortion can be isolating and traumatic. This uncomfortable experience can force the victim to pay the fraudster and be afraid of reporting or telling a parent or guardian. Unfortunately, payment is never a solution. Once someone pays, they will be further targeted with continued threats.

As this form of fraud is targeting young Canadians and teenagers, it is important that parents and children develop an understanding of this online threat. To find more information on sextortion and to report instances of child victimization on the Internet, please visit the [Canadian Centre for Child Protection \(C3P\)](#).

NARRATIVE OF A SEXTORTION REPORT

“Communication was initiated through Facebook Messenger after I received a Facebook friend request. We both had friends in common, so I accepted the request.

The chat quickly became explicit and led to a video call in which they recorded a nude video of myself. They immediately demanded \$15,000.00 or they would destroy my life. They demanded that I text them at another phone number and continued to harass and threaten me.

I sent \$250 hoping that would get them to leave me alone. It did not, and they started threatening to send images and video to my family and friends if I did not continue to send more money. This continued to the next day and included them sending images on Facebook Messenger to many of my contacts as well as my wife and place of work. This situation has created animosity with my wife, and embarrassed me publicly to many people who respected me.”

Most Common Types of Fraud by Age and Dollar Loss

Age Range	# of Reports	# of Victims	% Victimized
19 and under			
Extortion	247	183	74.1%
Identity Fraud	723	720	99.6%
Personal Info	290	281	96.9%
20 - 29			
Extortion	947	535	56.5%
Identity Fraud	2,733	2,718	99.5%
Personal Info	1,074	952	88.6%
30 - 39			
Identity Fraud	4,946	4,929	99.7%
Personal Info	1,572	1,410	89.7%
Phishing	1,074	390	36.3%
40 - 49			
Identity Fraud	3,762	3,752	99.7%
Personal Info	1,251	1,060	84.7%
Phishing	996	328	32.9%
50 - 59			
Identity Fraud	2,220	2,208	99.5%
Personal Info	1,026	789	76.9%
Phishing	1,120	308	27.5%
60 and above			
Extortion	2,194	475	21.6%
Identity Fraud	2,510	2,497	99.5%
Phishing	2,415	601	24.9%

Age Range	# of Reports	Dollar Loss	Average Dollar Loss per Victimization
19 and under			
Extortion	247	\$1,573,480	\$8,598
Investment	43	\$346,463	\$9,624
Merchandise	112	\$114,775	\$1,148
20 - 29			
Extortion	947	\$3,784,729	\$7,074
Investment	411	\$6,324,110	\$16,730
Job	649	\$801,666	\$1,681
30 - 39			
Investment	589	\$22,392,456	\$41,163
Merchandise	601	\$1,007,616	\$2,052
Romance	133	\$3,274,550	\$34,110
40 - 49			
Investment	630	\$43,238,558	\$74,293
Job	237	\$1,800,264	\$11,615
Romance	168	\$10,836,571	\$84,004
50 - 59			
Investment	582	\$72,710,657	\$133,170
Romance	203	\$11,451,380	\$73,880
Service	648	\$1,441,000	\$2,888
60 and above			
Investment	858	\$78,760,257	\$95,583
Romance	351	\$19,524,955	\$67,327
Service	2130	\$8,566,972	\$5,148

Extortion and sextortion targeting individuals younger than 30 is an ongoing trend, producing the most reports and largest losses for this age group in 2022.

Extortion Targeting Specific Ethnic Groups

The CAFC has been observing reports targeting other specific ethnic groups within Canada. As this form of extortion is often perpetrated in the victim's native language, it is possible that these forms of fraud originate within the targeted individual's region of origin. For instance, the CAFC has been observing extortion targeting international students with threats of deportation or denial of study or work permits.

Like other forms of fraud, extortionists will target victims with fraud scenarios that are likely to elicit a response or immediate reaction. As Canadians who have recently moved to Canada are likely concerned with citizenship, immigration or permits, fraudsters will exploit this concern in an attempt to defraud them.

Emergency-Grandparent Fraud

Emergency fraud takes place when a fraudster contacts a potential victim, often by telephone or land line, and states that a family member is arrested, injured, in the hospital or otherwise in danger. The fraudster may impersonate the individual's relative to play into the target's emotions and then put pressure on the individual by saying urgent fees must be paid to either avoid prosecution, assist in a defence, or pay medical bills, among other narratives. The person on the phone will likely advise that there's a "gag order" and recommend against talking to others anyone about the situation, to ensure isolation and increase the potential for successfully defrauding victims.

A variation of emergency scam that has become very common in 2022, is the "grandparent scam/fraud". These are emergency frauds which target seniors and have callers claim to be their grandchildren or calling on behalf of them. Seniors may be uncomfortable with quickly ending conversations or hanging up on the fraudster, giving fraudsters more time to apply pressure and convince them.

Seniors and vulnerable populations are particularly susceptible to intense pressure or threats applied by fraudsters. Fraudsters may harass seniors with emergency calls at various times of day and night using different phone numbers, further disorienting and scaring them. In 2022, the CAFC received many reports of senior victims initially ignoring these forms of scams but then eventually losing money after the calls, threats and harassment by the fraudster continued.

In 2022, the CAFC received 2,494 total reports of emergency fraud and \$9.4 million in losses. In comparison, the CAFC received 1,106 reports totaling \$2.4 million in losses in 2021. Seniors were strongly impacted by emergency fraud, with \$7.7 million in losses through 1,672 reports.

In emergency and grandparent fraud, the CAFC is observing increased direct contact between fraud associates and victims. This includes showing up at victims' houses to retrieve cash and helping them with transportation to the bank.¹⁰ Fraudsters are also encouraging victims to send cash as a package in the mail.

Despite the challenges faced in this type of fraud, police partners are successfully finding and arresting perpetrators located in Canada associated to fraud operations. For example:

- The Service de police de la Ville de Montréal (SPVM) arrested four individuals responsible for over 100 senior fraud reports in various Montréal neighbourhoods.¹¹
- York Regional Police arrested two people linked with four grandparent fraud victimizations in the region.¹² As stated previously in this report, comprehensive fraud operations increasingly require associates located in Canada to complete part of the fraud.

When fraud is reported quickly and a pattern of fraud is developed, the CAFC and police partners can have a positive impact for victims of fraud.



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”](#)

NARRATIVE OF AN EMERGENCY-GRANDPARENT FRAUD REPORT

“My father received a call that my son had been in a car accident and that they had found drugs on him. They then put what sounded like a child on the phone to say ‘Get me out of here, it’s horrible.’ In order for him to get out my father had to pay \$12,000. A cash collector picked the money up from my father’s house.

The same group called again, asking for another \$12,000 for court proceedings and lawyer fees. Several days later, another courier picked it up from my father’s.

About a week later, they asked for another \$5,000. My father sent the money in a box by courier service.

A week after previous contact, they asked for another \$7,000. When my father said ‘no,’ the man became extremely verbally abusive and threatened him and his family. My father was very scared so he sent it again by courier to another address. Although my father saw my son and I everyday while this was going on he never told us in fear of what they could do. They threatened him and he was in fear for his and our lives.

Later that month, my brother called my father to warn him about grandparent scams, and this is when he told the family.

After the previous times, they continued to call and my father refused. They told him that he had a short period of time to send more money, or they would pick up my son from school and arrest him. My father kept refusing and told them that someone was going to take care of this for him. They continued to harass and threaten him, and even called while we were at the police station filing the report. My father is still living in fear of what they could do.”

Romance Fraud

With the growth of online dating websites and applications, Canadians may enter into romantic online relationships with individuals they have never met in person or who may not be located in Canada. Whether finding love through a dating site or app, social media or other means, Canadians are consequently being victimized by romance fraud.

Offering companionship and affection to people looking for a relationship is an effective method for developing a connection with potential fraud victims. Once a connection is created, the fraudster can leverage these feelings to convince victims into sending money to them. The initial relationship can shift towards promises to pay the money back, pressure or guilt, anger and even extortion or threats.

In a variant of the romance scam that is contributing to the substantial losses, fraudsters initiate a romance scam, which later transitions to an investment scam. Known as “pig butchering,” the targeted individual enters a virtual relationship with the fraudster. After a period of time in this relationship, the fraudster encourages the individual to initiate some form of investment. Common investment schemes include cryptocurrency, but may also include real estate, gold and other investment directions.

Once the fraudster develops a connection with an individual, they often convince them to give personal information, details about their lives and work, or sexual and explicit material. This information and material can be used to extort or threaten a victim if they do not comply with the fraud. As the fraud progresses, the fraudster may even request that the victim travel to another country, which can become exceptionally dangerous and lead to further forms of exploitation or victimization.



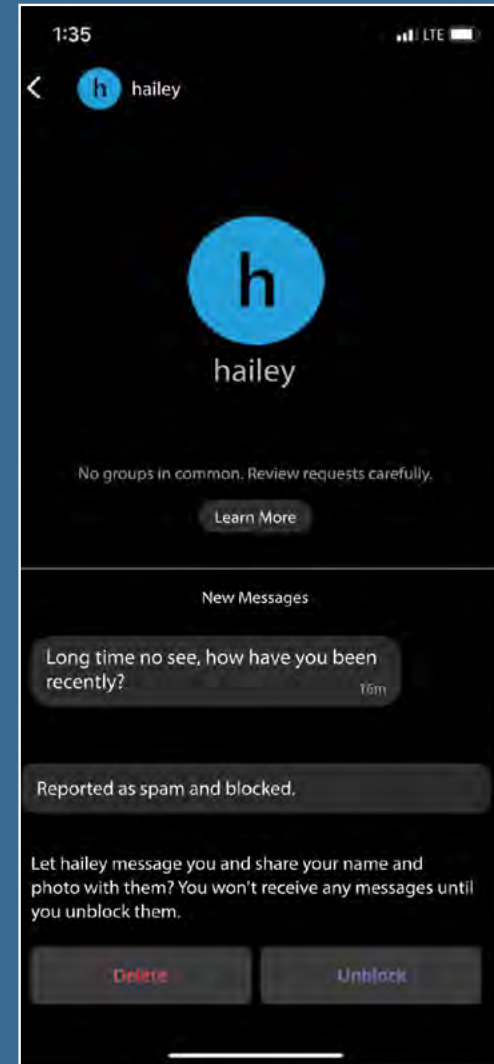
Romance fraud often takes place over prolonged periods of time. Attentive family members may be able to notice changes in the personality or habits of a family member. Changes may include:

- **Online or Internet usage:** The victim may spend significantly more time online and more time in video calls or chatting with a specific person (the fraudster).
- **Reluctance to share information about an online relationship:** Despite spending a considerable amount of time talking to their companion, the victim may be secretive or elusive about the relationship with family members. In many cases, the fraudster strongly discourages the victim from sharing information or details about the relationship, because family members are likely to discover the fraud and encourage ending the relationship.
- **Financial difficulty:** As romance fraud often takes place over an extended period of time, the victim may have ongoing, noticeable, and uncommon financial difficulties.
- **Personality changes:** The fraudster may convince the victim to become more closed off to friends and family members, in an attempt to increase the bond between them and reduce the chances for a family member to intervene with the fraud.

In 2022, the CAFC received 1,420 reports totalling \$59 million in losses. Romance fraud continues to be one of the most prolific forms of fraud observed by the CAFC. Romance fraud can be especially traumatic, with the victim dealing with both financial and emotional loss at the conclusion of the relationship.

Romance scams do not have to begin on dating sites or apps.

Many begin with a direct message on a messaging app or social media. Be cautious when someone you do not know contacts you, and report any questionable profiles as spam.



NARRATIVE OF A ROMANCE FRAUD REPORT

“I recently went online to try the dating sites, and met this man on Sep 24, 2022. We had an instant connection and I was wary of being scammed. Through our relationship and because I was worried about scams, he provided me with a lot of evidence to prove his identity. He called me two or three times per day, ending always with a nightly phone call regardless of where I was. Sometimes calls lasting for 2 hours. He was very detailed, stories were always correct and past information was correct.

He told me that he was awarded a contract that brought him to Turkey. He sent me itinerary docs, videos of being there and other pieces of information.

Following his request, I loaned him money because he said that his bank account was frozen. He needed that to open a Turkish bank account to deposit a bank. I transferred the money to a specific account.

Two weeks later, he needed further assistance as Turkey was placing a tax on his income. I transferred him \$10,000, and then purchased a bank draft for \$12,000 and deposited it into another account. Today, he asked for another \$30,000, and I realized that this was a scam.”

Looking for love online? Signs that a relationship may be romance fraud:

- ▶ An individual says that they are living in another country or never want to meet in person.
- ▶ A person you meet online seems overly eager to begin a committed or serious relationship.
- ▶ After talking for a period of time, a person begins to pressure you to send money for serious events or issues they are facing.
- ▶ A person begins to exhibit toxic relationship qualities if you do not send them money (e.g. become angry, distant, or make you feel guilty).
- ▶ A person tries to convince you to invest money into a venture or cryptocurrency.

Impersonation of Government Organizations

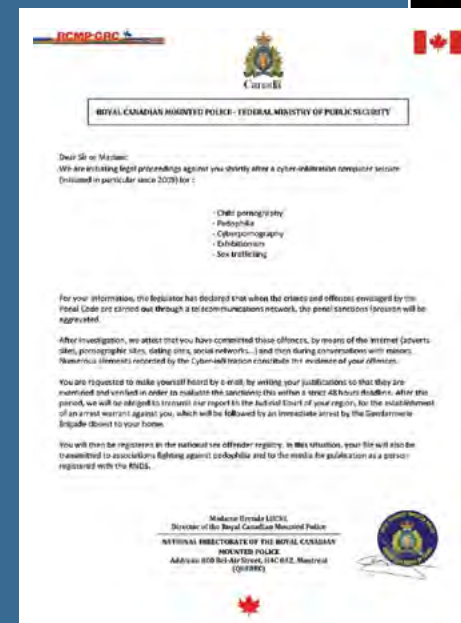
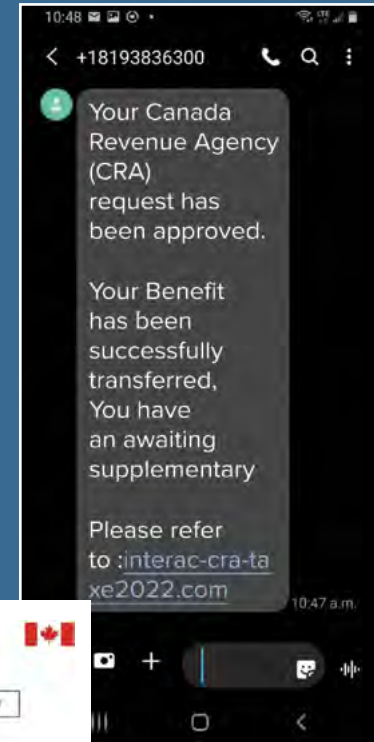
In 2022, the CAFC observed reports of fraudsters impersonating financial institutions, the Canada Revenue Agency (CRA), Canadian Border Services Agency (CBSA), courier and delivery companies, the RCMP, other domestic and international police agencies, as well as other Government of Canada organizations.¹³ The CAFC even received reports of fraudsters impersonating the CAFC.

Depending on the impersonated organization, these fraud schemes are linked to several notable forms of fraud, including:

- Telephone and text-message phishing;
- Canceled charges or in the payment for merchandise (merchandise fraud);
- Extortion attempts and threats of arrest, punishment, harm or fines;
- Personal information theft, identity theft and identity fraud, by impersonating financial institutions.

More specifically, the CAFC has also been observing more reports of bank investigator fraud. This fraud takes place when a fraudster impersonates a bank investigator or authority, and calls to resolve suspicious transactions. The CAFC received 4,255 reports totaling \$6.7 million in losses connected to bank investigator fraud in 2022.

Fraudsters are impersonating many different Canadian organizations to give the appearance of legitimacy in their messaging. Text messages and emails containing attachments and links continue to be popular methods to defrauding victims.



¹³ "Mounties warning of scam using name of RCMP commissioner"

Merchandise and Counterfeit Merchandise Fraud

Transitioning beyond the COVID-19 pandemic, Canadians are returning to shopping in-person. Although the CAFC received a considerable number of merchandise and counterfeit merchandise fraud reports in 2022, the CAFC observed fewer reports and a lower dollar loss than in 2021.

In 2022, the CAFC observed approximately \$8.8 million and \$900,000 in losses to merchandise and counterfeit merchandise fraud, with 7,994 total reports. This is compared to approximately \$12.3 million and \$1 million in losses to merchandise and counterfeit merchandise fraud in 2021, with 10,194 total reports.

NARRATIVE OF A MERCHANDISE FRAUD REPORT

“I was looking to buy an item through Facebook Marketplace, and found an ad for the same product. I was able to get the individual’s email address. After agreeing to the sale, I transferred money to their account. We arranged for a date and time to pick up the item. When the day came to pick up the item, they stopped answering their phone and was not present at the address.

I contacted my bank and they told me once the money was deposited they can not cancel the transaction and I have to file a police report.”

Identity Fraud, Identity Theft, and Personal Information Theft Trends

The theft of personal information is closely linked to most forms of fraud. If the fraudster is not attempting to steal money, they will try to steal personal information. This will translate to other forms of financial crime and fraud.

Identity fraud is initiated after identity or personal information is stolen. Often, victims may not realize when personal information has been stolen or when their identity is at risk. There are countless ways in which personal information or identities can be stolen, including:

- Purchasing something online from an unsecure website;
- Submitting personal information to a fraudulent online questionnaire;
- Forgetting to shred financial or personal information and leaving it in a recycling bin;
- Submitting login information to a spoofed website;
- Submitting personal information over the phone, when asked by a fraudster acting as a bank or government employee.

Fraud scenarios can be unsophisticated or elaborate, and the loss of personal information can be especially harmful to the victim. Identity theft and personal information theft can lead to long-standing financial and personal challenges, especially if identities are used to commit additional forms of fraud.

After the theft, fraudsters may use identities to hide criminal activities, open fraudulent bank accounts to hold and transfer fraud proceeds, take out loans and purchase items, and even access other personal bank accounts to directly steal money.

The CAFC continues to see increases in personal information theft and identity crimes. In 2022, the CAFC received 8,086 reports of personal information theft and 19,543 reports of identity fraud, compared to 7,808 reports of personal information theft and 31,797 reports of identity fraud in 2021.

Note: Identity fraud is used for financial gain. However, the CAFC is unable to accurately track how much money is lost to identity crimes through reports, as identifying information and individual identities can be used in many illicit ways that are not known by the victim at the time of reporting.

NARRATIVE OF AN IDENTITY THEFT/ FRAUD REPORT

“I received an email from Equifax notifying me that an account had been opened under my name. Upon verification of the details on Equifax, I saw a suspicious new credit card with a bank I didn’t use, with a line of credit created. I also noticed a new phone number against my legitimate Equifax account. I called the bank to flag this and they advised I should go to the branch. When I went to the branch, I realized someone had opened the credit card account with the stolen information. The bank contacted their fraud unit and was able to shut down the account.

I subsequently filed a police report with my local police. When I attempted to file a fraud alert with TransUnion, I tried to create an account. I wasn’t able to as I was told an account was already created under my name. I contacted TransUnion by phone and with them was able to determine that an account was created using a fake email address and the street address against my Social Insurance Number. TransUnion was able to place the fraud alert and also deleted the fake account.”

Fraud and Organized Crime

There is a strong association between fraud and international organized crime. Although this is not necessarily a new trend, criminal enterprise is finding greater success at engaging in fraud operations to extort or steal money from Canadians. The vast majority of fraud is perpetrated by organized and international crime groups targeting a significant number of Canadians. Furthermore, coordinated spear phishing frauds targeting private-sector organizations are often perpetrated by similar groups.

As fraud losses continue to steeply rise and losses per victimization continue to grow, organized fraud groups are becoming more creative in moving large sums of money from Canada to other countries. Unusual movement of money or large transactions are often stopped or flagged by Canadian financial institutions. Because of this diligence by financial institutions, fraud groups use **money mules** within Canada to assist in the movement of fraudulently-stolen money.

Money Mules

A **money mule** is an individual who knowingly or unknowingly transfers or transports illicit funds on behalf of a criminal or fraudulent organization, for the purpose of deceiving criminal and regulatory authorities. There are two general subgroups:

- Money mules who **actively** participate in fraud.
- Money mules who **passively** participate in fraud.

Money mules who **actively** participate in fraud willingly act as intermediaries for fraud groups. Professional money mules may pick up packages containing money from a victim's house or postal office, open and operate bank accounts using stolen identities, or simply use their own identity and bank accounts to move money through their account for a portion of the profit.

Another form of active participation by money mules in fraud is following the victimization by job fraud. Victims become an active money mule while not knowing that they are assisting a fraud operation. Often given the title of "financial agent" or "client/portfolio manager," these individuals are hired as "payment processors" for the fraud operation. In this occupation, the victim is sent money to their personal account, and are given instructions to move the money outwards to listed accounts held by either the fraud operators or other money mules.

Additionally, victims who have lost considerable amounts of money may be extorted to act as money mules, with a promise that they will get some or all of their money back if they complete the work.

Fraud victims can also be **passive** money mules in fraud operations. These examples are usually linked to identity theft and fraud, and personal information theft. The fraud operation will use the stolen identity to open new bank accounts or gain access to personal accounts without the victim's knowledge, and then funnel money through the account to hide the movement of money.

Money mules are key enablers of fraud operations in Canada. The CAFC has been observing the close connection of money mules to emergency and grandparent fraud, cryptocurrency fraud, investment fraud, and other groups of fraud that are leading to significant losses per victimization. As fraud becomes increasingly lucrative, the impact of organized crime in this sphere will continue to challenge law enforcement efforts.

Fraud Targeting Seniors

Seniors (individuals aged sixty years and older) and vulnerable populations continue to make up a growing portion of total fraud reporting to the CAFC in 2022. In 2021, the CAFC received nearly 13,000 reports by seniors totalling \$83.6 million in losses. Looking back to 2022, the CAFC received approximately 17,000 reports totalling \$137.8 million in losses, demonstrating that this group of Canadians continued to be targeted by fraudsters and cyber threat actors.

Generally, older individuals are particularly susceptible to conventional forms of fraud where first contact is by telephone or land lines and contains pressure, threats and harassment.

As seen in 2021, seniors continue to be victimized by extortion, with 2,194 reports totaling \$7.7 million in losses in 2022. Seniors also reported phishing as a dominant fraud theme, with 2,415 total reports to the CAFC. Senior losses to investment fraud rapidly increased in 2022, with approximately \$78.8 million in total losses compared to \$38 million in total losses in 2021. Additional fraud trends increasing from 2021 include service, emergency, and bank investigator fraud, among others.

Other dominant fraud types like romance fraud, personal information theft, prize fraud, and merchandise fraud remained fairly stable in 2022. Despite travel picking up again in 2022, timeshare fraud continued to decline, with 19 reports totaling \$783,000 in losses in 2022, compared to 30 reports totaling \$2.1 million in losses in 2021.



Senior (60+) – Top 10 Fraud Categories

Fraud Type	# of Reports	%GT Report	# of Victims	% Victimized
Identity Fraud	2,510	12.9%	2,497	99.5%
Phishing	2,415	12.4%	601	24.9%
Extortion	2,194	11.3%	475	21.6%
Service	2,130	11.0%	1,664	78.1%
Personal Info	1,808	9.3%	1,175	65.0%
Bank Investigator	1,687	8.7%	512	30.3%
Emergency (Jail, Accident, Hospital, Help)	1,672	8.6%	750	44.9%
Investment	858	4.4%	824	96.0%
Prize	743	3.8%	230	31.0%
Merchandise	510	2.6%	395	77.5%
Total	16,527	85.1%	9,123	55.2%

Senior (60+) – Top 10 Fraud Categories by Dollar Loss

Fraud Type	Dollar Loss	Average Dollar Loss per Victimization
Investment	\$78,760,257	\$95,583
Romance	\$19,524,955	\$67,327
Service	\$8,566,972	\$5,148
Extortion	\$7,718,495	\$16,249
Emergency (Jail, Accident, Hospital, Help)	\$7,134,791	\$9,513
Bank Investigator	\$4,197,111	\$8,197
Prize	\$3,174,427	\$13,802
Foreign Money Offer	\$2,429,560	\$115,693
Grant	\$1,653,370	\$10,599
Recovery Pitch	\$974,419	\$15,716
Total	\$134,134,357	\$26,913

Personal information theft and phishing continue to impact seniors and vulnerable Canadians. The CAFC observed significantly more identity fraud reports from this age group in 2022. Emergency fraud reports tripled in 2022 from 2021. Investment scams continue to produce the largest losses by seniors, and this number has more than doubled from \$38 million in 2021 to nearly \$79 million in 2022.

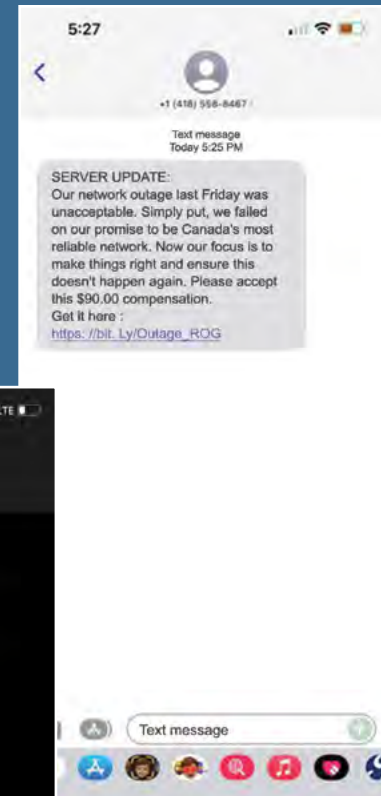
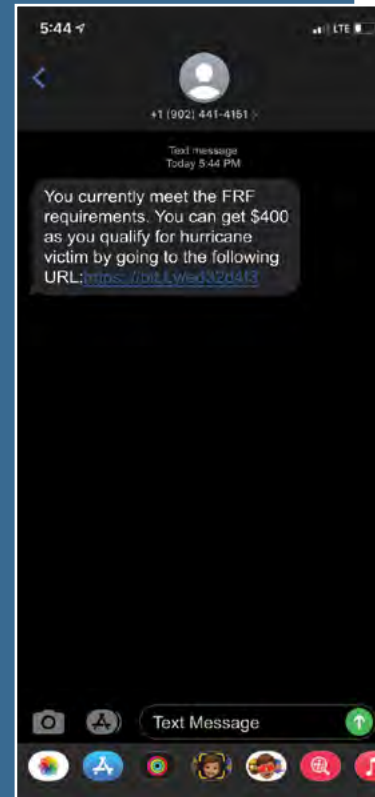
New Fraud Themes

The fraud environment is highly dynamic. Fraud operations nuance their approaches depending on success of their attempts, socio-cultural trends, and law enforcement efforts to challenge their ecosystem.

For example, in 2022, the CAFC observed a decrease in the once-popular COVID-19 fraud and saw an increase in fraud trends relating to current events such as the ongoing conflict between Russia and the Ukraine, Hurricane Fiona relief efforts, Rogers national outage refunds and others. Certain fraud types, like charity scams and phishing were leveraging Canadian's attention on current events to defraud them.

Internet-enabled fraud continues to grow, but telephone-first contact is the most reported fraud subset received by the CAFC. Fraudsters are also using new methods of contact, including first texting the potential victim with a phishing attempt, and waiting for the victim to engage by responding to the text or clicking a link within the text.

The Rogers service outage and Hurricane Fiona relief efforts were two trending fraud pitches observed in 2022.



Remote Access Software

Remote access software is increasingly cited in fraud reports to the CAFC, particularly in connection to bank investigator fraud and tech support fraud. The fraudster offers “support” for ongoing computer or financial issues, requesting access to devices to provide assistance. Fraudsters will often request for victims to turn on computers or click on links texted to cell phones. Fraud using remote access tools is particularly effective if victims are distracted or confused, especially when the fraudster creates a sense of pressure or urgency.

Remote access tools are legitimate and proprietary software that allow for the remote access of computers and the virtual transfer of files. In using this form of technology in an illegal manner, fraudsters request the victim to download the remote access application. They will then convince the victim to provide the tool-generated access code to be able to remotely access their computer, and permit other permissions like file transfer and screen blackout. This allows the fraudster to look into the bank accounts, access personal information, make new banking and cryptocurrency accounts, among other possibilities.



New Technologies Enabling Fraud

The Internet is enabling fraudsters in contacting and targeting potential fraud victims on a large scale. Advertisements, social media platforms, email, and chat groups and forums offer unprecedented and fast access to people around the world.

Within the cyber environment, fraudsters can obfuscate their identities, impersonate friends, authority figures, or other personalities, and even create countless accounts managed by automated accounts or programs (bots). The cyber environment is allowing for more complex forms of fraud that are becoming increasingly challenging for users to recognize as fraud.

There are several technological developments that the CAFC is forecasting to have stronger impacts on the fraud environment: Generative Artificial Intelligence I large language models, voice cloning software, deepfakes, and bots.

Predictive and Conversational Language Models, Voice Cloning Software, and Deepfakes

Artificial Intelligence (AI), including dialogue-based Generative AI, like Chat GPT, and Google's Bard AI, were introduced in 2022 and 2023 and are gaining considerable international attention. Both easily accessible to the public, they can assist in drafting complex emails and documents, provide helpful suggestions when asked questions or posed with a challenge, give users an alternative perspective to questions, and offer other forms of assistance, such as fast, high-quality translation and robust, detailed writing. While this technology can be helpful, it also creates new dynamics in the fraud environment.

Related to AI chat tools, an emerging form of technology that will increasingly enable fraud is voice cloning/mimicking software. In this type of program, users can input sound bytes or dialogue from a user or use stock sound bytes of famous and recognizable people. For minimal or zero cost, anyone can program a voice model to say whatever they would like it to say.¹⁴ Fraudsters are able to use famous voices to offer increasingly elaborate fraud schemes, and the CAFC is observing this in advertisements on video streaming services.

¹⁴ An example of this technology is [Uberduck](#)

High-quality fake profiles of non-existent people, combined with the ongoing improvements of fake audio-visual material will continue to challenge users in detecting potentially fake or malicious profiles.

When someone posts online content containing their voice, voice cloning software will be able to use these sound samples to impersonate them when committing fraud. Although we are in the earlier stages of this technology's application, the CAFC is receiving more emergency fraud reporting of victims hearing an individual on the phone that sounds similar to their own relatives or grandchildren in pain or crying for help.

Beyond voice cloning/impersonation, the CAFC has been observing the use of AI-generated profiles, video and images of people to engage in fraud. AI developments introduced new methods of creating increasingly complex fake profiles and identities (Deepfakes).¹⁵ For example, AI programs can be used to create fake faces on social media profiles.¹⁶

By combining all discussed forms of voice, imagery, and video content through available open-source software, there is the potential for fraud operations to completely impersonate someone, and create a new virtual identity that is indistinguishable from the real person.

Bots

Internet robots, or “bots”, are software applications that manage automated tasks over the Internet. Bots can be programmed to contact users of social media sites through direct messages, post articles on websites, engage in conversation with each other and with users (chatbots), send text messages, and more. Most commonly, bots perform automated and straightforward tasks faster and more cheaply than a human being. Relating to malicious computer activity, bots can spread viruses, malware, and initiate cyber incidents.

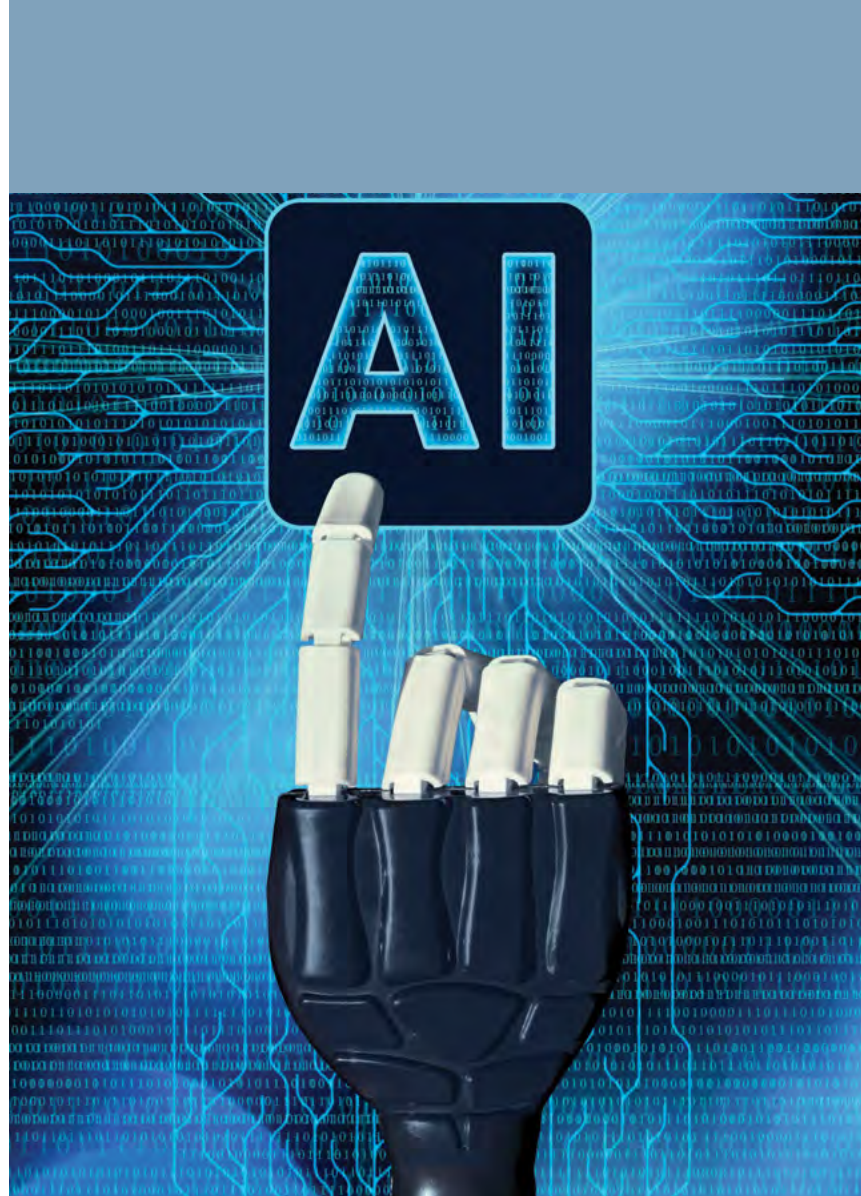
Most directly related to fraud, individuals may be contacted by other users of a site, and not realize that the user they are interacting with is indeed a bot. Bots can deceive users into being defrauded, with the user losing money or personal information in the process. They may be sent a message with a link, and accidentally click the link, making them susceptible to personal information theft, viruses or malware. A bot may redirect a user to other sites, which can further engage the user in a fraud pitch. Finally, engagement with a bot may signal to a cyber threat actor or fraudster to reach out and contact the user directly.

¹⁵ Nightingale, Sophie J., and Hany Farid. (February 14, 2022). [“AI-Synthesized Faces and Indistinguishable from Real Faces and More Trustworthy.”](#) *Psychological and Cognitive Sciences* 119(8).

¹⁶ Bond, Shannon. (March 27, 2022). [“That Smiling LinkedIn Profile Might be a Computer-Generated Fake.”](#) *NPR*.

Ongoing research of social media activity is beginning to find very high levels of website activity attributed to malicious bots.¹⁷ While bots are a longstanding and ubiquitous threat, easily observed by Internet users, active attempts to detect and eliminate bots through antivirus software, online tests like CAPTCHA and reCAPTCHA, and Internet activity monitoring, has only led to more sophisticated and widespread botnets. Bots are one of the most widespread tools used by cybercriminals, and can vary in quality which can make them difficult to detect by individual users. Cybercriminals are finding success with bots despite Canadian businesses and government creating stronger strategies to combat this threat. The CAFC observes bots as a developing threat, and one that will continue to impact Canadian Internet users in the years to come.

Bots are one of the most widespread tools used by cybercriminals to target a significant number of potential victims. The ongoing success of botnets in connection to fraud and cybercrime, combined with the ongoing efforts by businesses and governments in creating stronger strategies against this threat, creates the perspective that bots will both become stronger, more widespread, and more comparable to actual human users. The CAFC observes bots as a developing threat trend that will continue to have an impact on Canadian Internet users.



17 Pfeffer, Jurgan, et al. (January 26, 2023). "Just Another Day on Twitter: A Complete 24 Hours of Twitter Data." arXiv preprint arXiv:2301.11429.

Update on Current Efforts

Whether actively learning about fraud and of the methods to avoid it, needing to file a report with the CAFC and local police departments, need guidance and support after a fraud victimization, or want to let the CAFC know of a fraud attempt, the CAFC works diligently to be a positive presence for Canadians. From the committed efforts by the reporting and intake analysts, Senior Support Unit staff and volunteers, communications and media personnel, and intelligence and investigative teams, the CAFC will continue support victims of fraud.

The CAFC would like to thank all Canadians and those located outside of Canada who have contacted or filed a report with the CAFC. Without ongoing engagement, the CAFC would not be able to provide our services and effectively coordinate fraud efforts with police of jurisdiction.

An Update on the National Cybercrime Solution and National Cybercrime and Fraud Reporting System

From last year's update, the CAFC continues to be engaged with the National Cybercrime Coordination Centre (NC3) to create the RCMP National Cybercrime Solution (NCS). The NCS will be a centralized data repository containing fraud and cybercrime investigative data, incidents and intelligence jointly managed by the NC3 and CAFC.

2022 saw important progress on the NCS project. The NCS has transitioned to full development phase with its first production release in April 2023, with an anticipated full delivery date in the second half of 2024.

As introduced in the Annual Report 2022, the National Cybercrime and Fraud Reporting System is in Beta version and is forecasted to be fully operational in 2023-24.

In 2022, the NCFRS had:

- 21,238 visitors;
- 5,256 total reports received; and,
- Continued ongoing user research resulting in a 30 per cent decrease in NCFRS load time.

As the NCFRS progresses, the CAFC and NC3 welcome feedback that may assist in the development of the NCFRS. You can still take part in our research and become a volunteer at report.antifraudcentre.ca/recruitment

Conclusion

By all indicators, 2022 was the most impactful recorded year for fraud targeting Canadians. Reported losses surpassed the \$500 million threshold for the first time in the CAFC's existence. These losses produced profound financial and emotional trauma for thousands of Canadians, and it's still estimated that only 5-10% of people report fraud and cybercrime. **Fraud is not a victimless crime.** From our reporting analysis, the Canadians that continue to be most impacted by fraud and identity theft are seniors, vulnerable populations and those who may already be under financial pressure. Due to increasing losses per victimization, more Canadians are becoming completely financially devastated by fraud.

Challenging the threat of fraud requires a whole-of-society approach. The CAFC is a leader in fraud awareness and education, and we thank all Canadians for carrying these messages forward. The CAFC would also like to thank all partners, including law enforcement and financial institutions, on their efforts to have a positive impact on fraud victimization and harm reduction.

The CAFC is the national police service for fraud reporting, deconfliction, intelligence sharing, education and awareness, and relies on these strong partnerships to continue in this role.

About the Numbers

The statistics within Annual Report 2022 are sourced from all reports received and verified by the CAFC between January 1 and December 31, 2022. Some reports received by the CAFC may be incomplete, may not contain a description of money lost, and may omit other details in the reporting process. When filing a report, individuals have the option of offering as many or as few details as they choose. However, detailed and complete information provided in reporting can better assist the CAFC in finding resolution to individuals impacted by fraud, and lead to stronger fraud intelligence and statistics.

The statistics in the Annual Report contain reports from both attempted and actual victimizations, and can therefore include reports with no dollar loss. The CAFC greatly values all reports, including those of attempted victimizations or potential fraud occurrences. These reports are valuable and provide more robust information for further trends analysis.

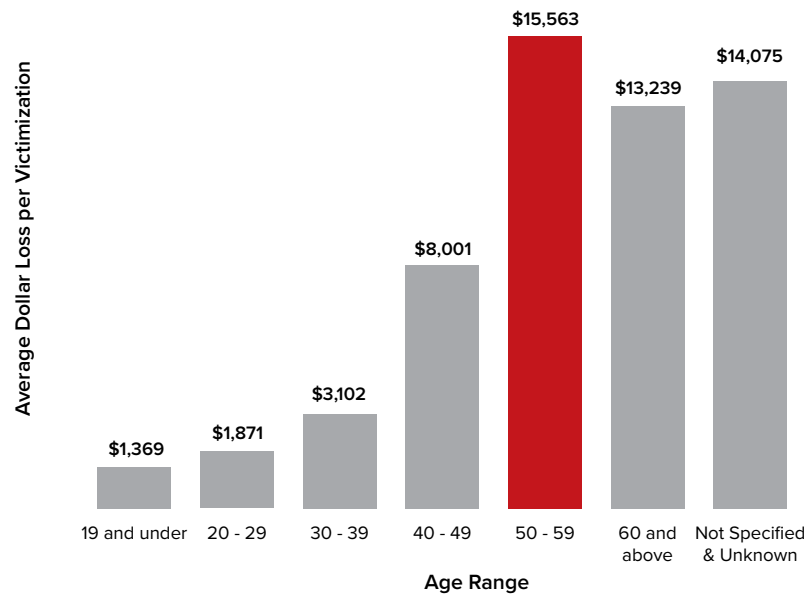
In certain forms of fraud, such as identity theft or personal information theft, a true dollar figure may not be obtained. For instance, a threat actor who steals an individual's identity may do so to sell identity-related credentials to other threat actors, or attempt to obtain credit cards using the individual's identity, among other potential options. The fluid nature of fraud creates challenges in determining exact dollar losses for these forms of fraud.

Due to the large dataset and significant number of reports received by the CAFC, the numbers may vary over time. The CAFC continues to validate reports from the previous year, and individuals may file reports at a later date while noting the occurrence took place in the previous year. Because of this, the total reports and dollar loss may vary into 2023.

Unless explicitly noted, all references to currency are in Canadian dollars (CAD).

Additional Statistics

Average Dollar Loss by Age Range

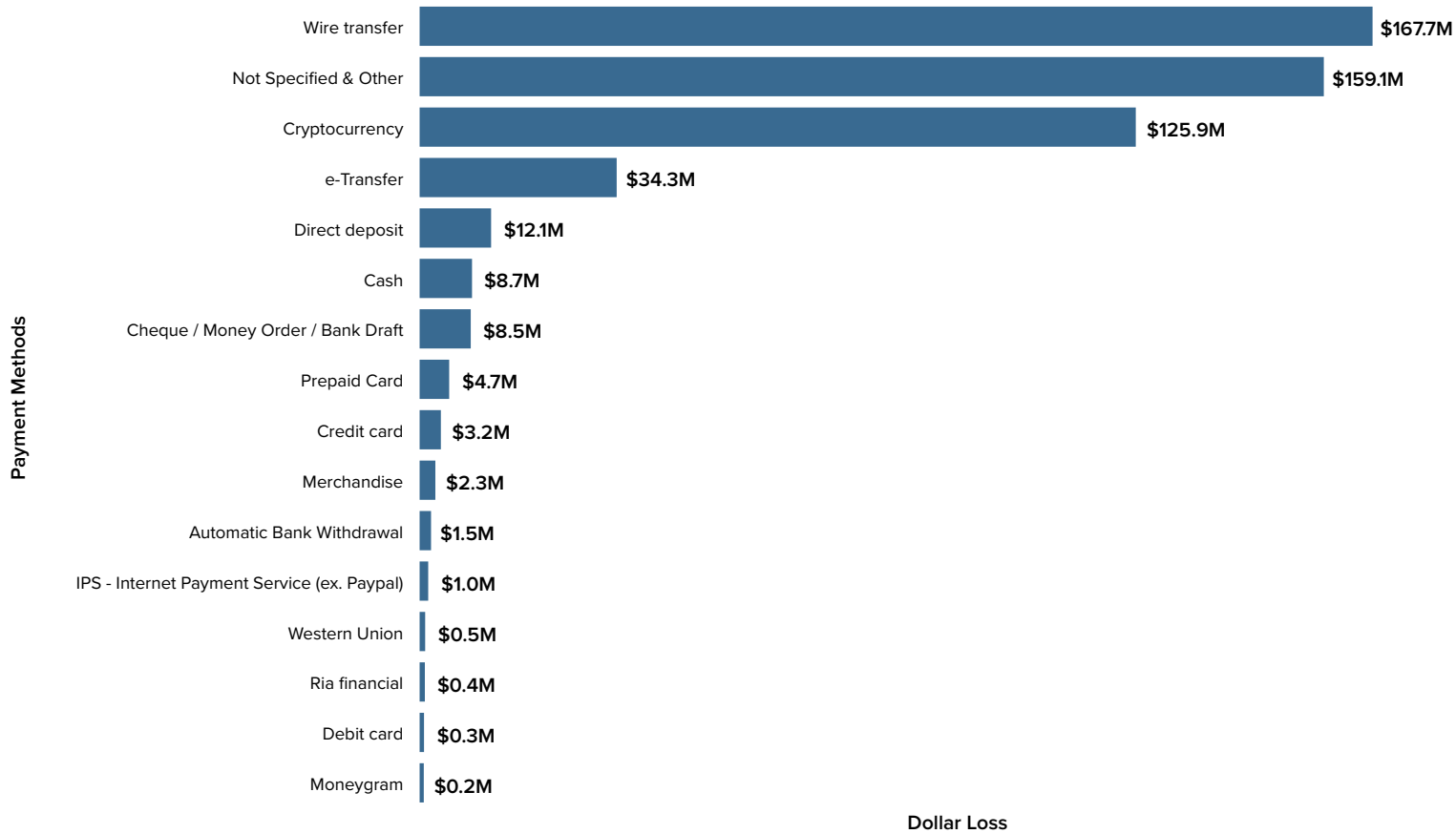


Age Range	# of Reports	# of Victims	% Victimized	Dollar Loss	Average Dollar Loss per Victimization
19 and under	1,978	1,730	87.5%	\$2,368,433	\$1,369
20 - 29	9,569	7,510	78.5%	\$14,052,225	\$1,871
30 - 39	12,578	9,832	78.2%	\$30,500,840	\$3,102
40 - 49	10,679	7,759	72.7%	\$62,080,599	\$8,001
50 - 59	9,291	5,860	63.1%	\$91,196,944	\$15,563
60 and above	19,424	10,419	53.6%	\$137,935,844	\$13,239
Business & Deceased	43	35	81.4%	\$641,092	\$18,317
Not Specified & Unknown	27,359	13,617	49.8%	\$191,661,990	\$14,075
Total	90,921	56,762	62.4%	\$530,437,966	\$9,345

Individuals aged 50-59 and older continue to report higher losses than other age groups, carrying over from 2021.

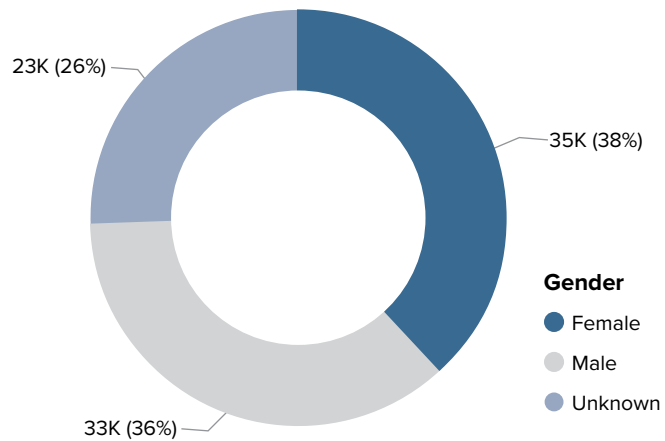
Businesses also reported extensive losses per victimization, which can be connected to forms of fraud like spear phishing and targeted fraud for larger losses.

Dollar Loss by Payment Methods

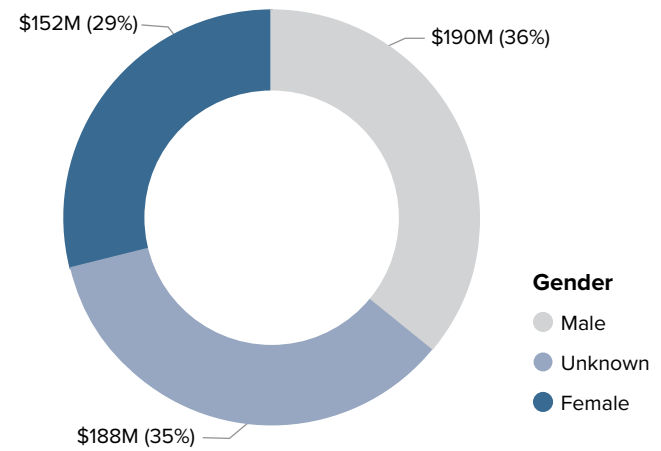


Wire transfers continue to produce the highest losses in 2022. Cryptocurrency losses grew from approximately \$78 million in 2021 to nearly \$126 million in 2022. Of note, Interac e-transfer is largely a Canadian-only service, which demonstrates that in CAFC reporting, \$34.3 million was sent to fraudsters potentially located in Canada through this transfer method.

Number of Reports by Gender



Dollar Loss by Gender



After accounting for reports by individuals who do not specify their gender, male individuals reported slightly more than female individuals, and also had slightly higher losses.

Senior (60+) – Solicitation Method by Gender for Identity Fraud

Gender	# of Reports	# of Victims	% Victimized
<input type="checkbox"/> Female	1,196	1,190	99.5%
Conventional Fraud	1,182	1,176	99.5%
Cyber-Enabled Fraud	14	14	100.0%
<input type="checkbox"/> Male	1,288	1,281	99.5%
Conventional Fraud	1,274	1,269	99.6%
Cyber-Enabled Fraud	14	12	85.7%
<input type="checkbox"/> Prefer not to say / Unknown	26	26	100.0%
Conventional Fraud	26	26	100.0%
Total	2,510	2,497	99.5%

Senior (60+) – Solicitation Method by Gender

Solicitation Method Group	# of Reports	# of Victims	% Victimized
<input type="checkbox"/> Female	10,132	5,403	53.3%
Conventional Fraud	7,089	3,634	51.3%
Cyber-Enabled Fraud	3,043	1,769	58.1%
<input type="checkbox"/> Male	8,893	4,761	53.5%
Conventional Fraud	5,873	3,045	51.8%
Cyber-Enabled Fraud	3,020	1,716	56.8%
<input type="checkbox"/> Prefer not to say / Unknown	399	255	63.9%
Conventional Fraud	332	214	64.5%
Cyber-Enabled Fraud	67	41	61.2%
Total	19,424	10,419	53.6%

Seniors were largely impacted by conventional solicitation methods, including direct telephone calls. Both genders demonstrated comparable levels of victimization through reporting. Particularly in male reporting, cyber-enabled fraud continues to increasingly impact seniors. Conventional pitches were the overwhelmingly dominant method with respect to identity crimes against seniors.

Senior (60+) – Solicitation Method by Gender for Investment Fraud

Gender	# of Reports	# of Victims	% Victimized	Dollar Loss	Average Dollar Loss per Victimization
<input type="checkbox"/> Female	248	236	95.2%	\$17,805,296	\$75,446
Conventional Fraud	47	43	91.5%	\$3,092,116	\$71,910
Cyber-Enabled Fraud	201	193	96.0%	\$14,713,181	\$76,234
<input type="checkbox"/> Male	597	575	96.3%	\$57,775,076	\$100,478
Conventional Fraud	122	113	92.6%	\$22,625,785	\$200,228
Cyber-Enabled Fraud	475	462	97.3%	\$35,149,291	\$76,081
<input type="checkbox"/> Prefer not to say / Unknown	13	13	100.0%	\$3,179,885	\$244,607
Conventional Fraud	6	6	100.0%	\$436,585	\$72,764
Cyber-Enabled Fraud	7	7	100.0%	\$2,743,300	\$391,900
Total	858	824	96.0%	\$78,760,257	\$95,583

Investment fraud often begins with a social media advertisement or direct message. From 2022 statistics, investment fraud produced extensive losses, and most losses began with a cyber-enabled fraud pitch.

Senior (60+) – Payment Methods for Investment Fraud

Fraud Type Payment Methods	Investment	
	# of Payment Methods *	Dollar Loss
Cryptocurrency	458	\$23,456,840
Not Specified & Other	355	\$29,976,874
e-Transfer	305	\$3,351,867
Wire transfer	154	\$19,011,904
Credit card	127	\$273,543
Automatic Bank Withdrawal	20	\$74,943
Cheque / Money Order / Bank Draft	18	\$2,396,688
Debit card	17	\$2,625
Cash	11	\$50,000
IPS - Internet Payment Service (ex. Paypal)	11	\$53,465
Direct deposit	9	\$59,823
Prepaid Card	5	\$500
Moneygram	2	\$17,350
Ria financial	2	\$33,834
Vigo money transfer	1	\$0
Western Union	1	\$0
Total	1,496	\$78,760,257

*Note that each report received can have more than one payment method.

Cryptocurrency continues to be a dominant form of currency in investment fraud, due to the ease of international transfer and the challenges in recovering stolen funds.

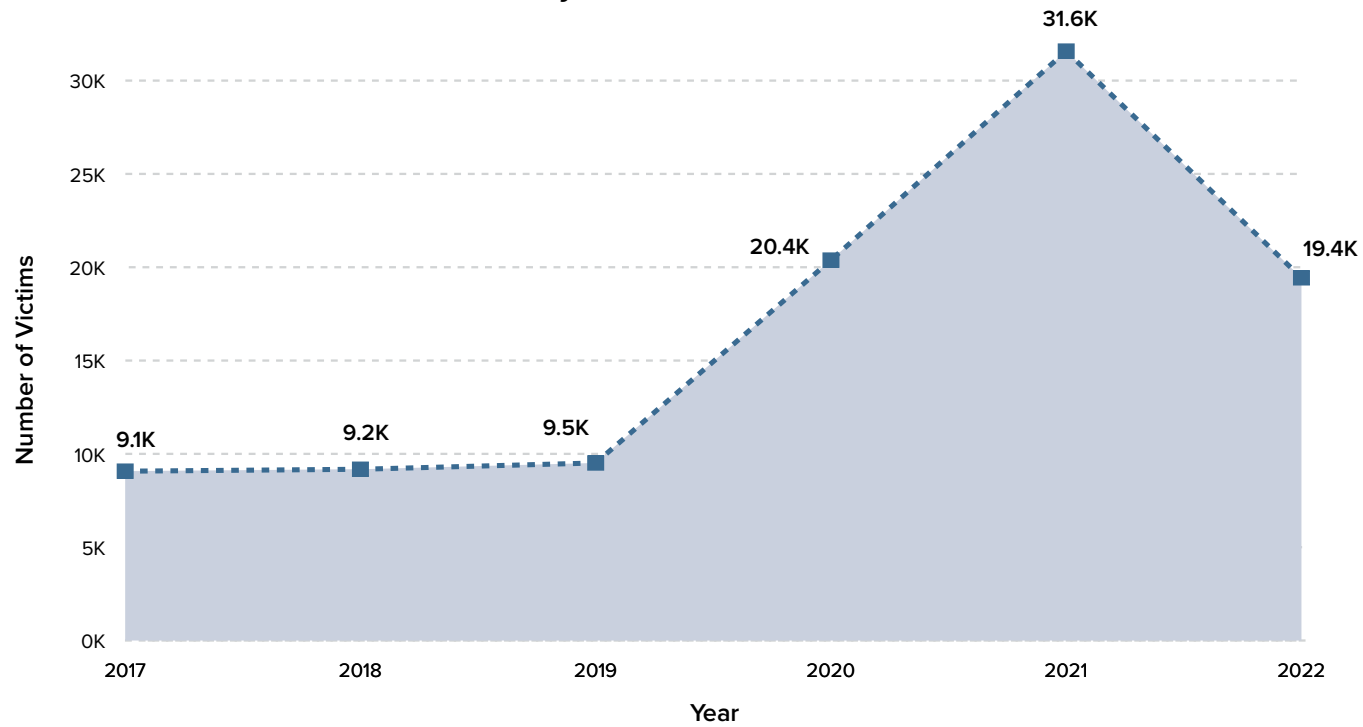
Additionally, a portion of wire transfer losses related to investment fraud can be attributed to the victim using a wire transfer to send cash to the fraud operation, with the expectation that the fraudster will invest the money for them.

Number of Reports and Victims by Year



Total reports and reported victimizations remained relatively steady in 2022. However, the CAFC is limited by overall capacity to intake reports. Fraud reporting continues to become increasingly complex, which leads to an increased amount of time receiving and reviewing reports. The NCFRS will help improve overall report processing.

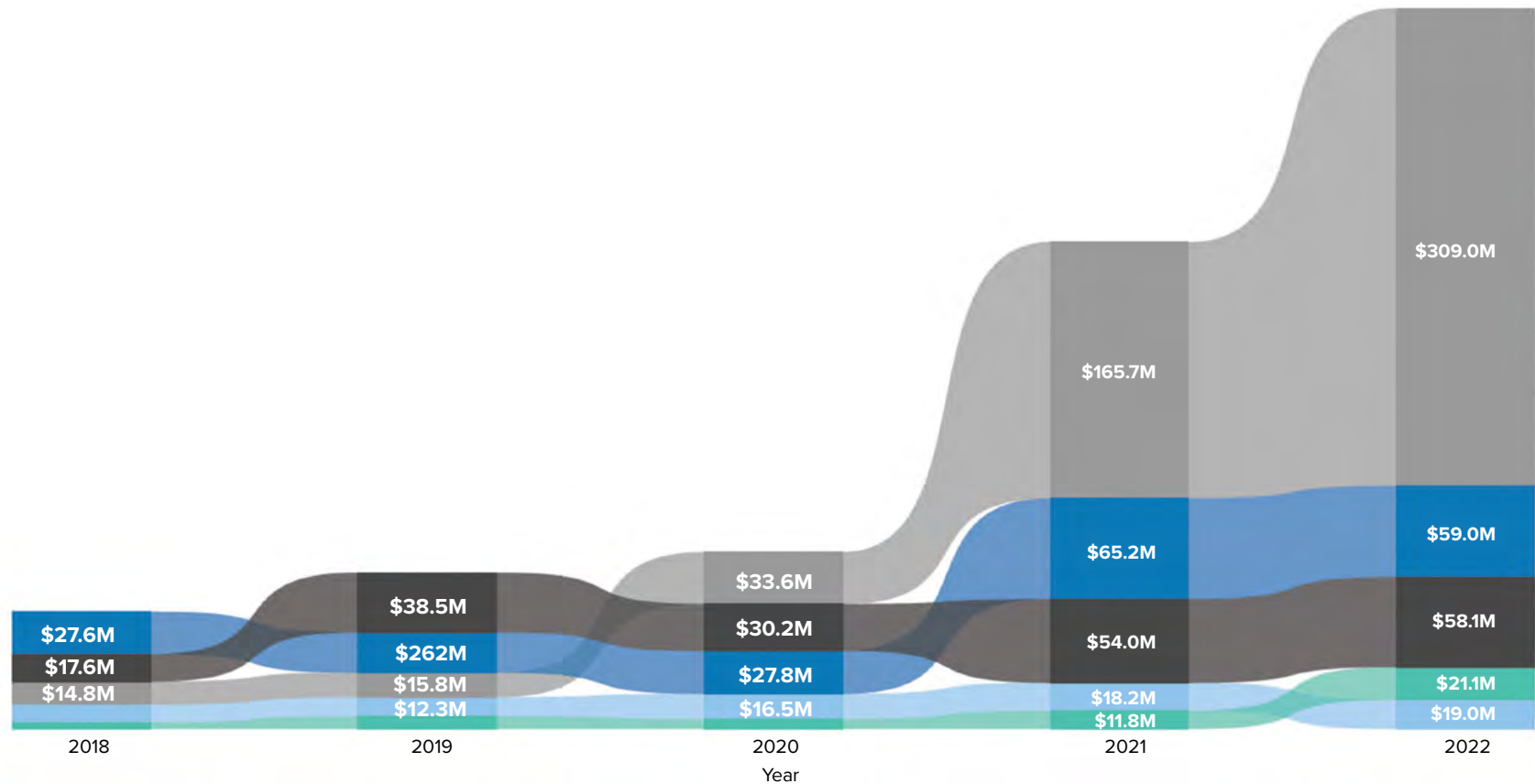
ID Fraud – Number of Victims by Year



The CAFC continued to receive a high number of identity fraud reports in 2022.

Top 5 – Dollar Loss by Year and Pitch

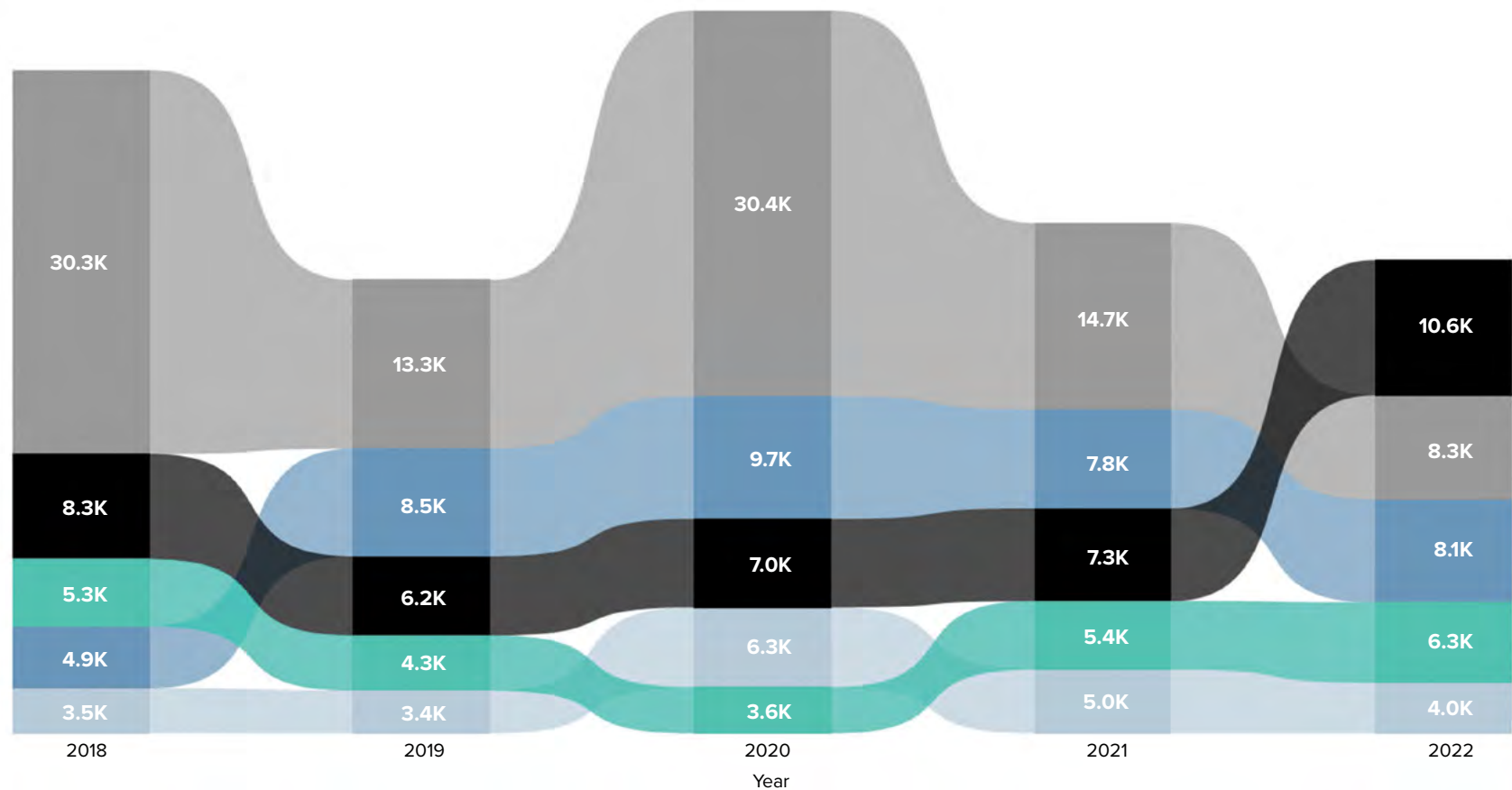
● Extortion ● Investment ● Romance ● Service ● Spear Phishing



One of the dominant trends observed by the CAFC is the rapid growth of high-losses in fraud, and high-losses in several key types of fraud. Investment fraud was responsible for a significant portion of fraud losses over the past two years, as well as romance fraud and spear phishing.

Top 5 – Reports by Year and Pitch

● Extortion ● Merchandise ● Personal Info ● Phishing ● Service



While extortion is leading to more overall losses, the CAFC is receiving fewer reports of extortion. This may mean that fraud operations are focusing on high-impact targets. Phishing continues to be more pronounced, being directly connected with identity crimes and personal information theft. Merchandise and service fraud reporting remained relatively steady in 2022.

Top 5 – Forms of Payment Methods Used in Fraud

Payment Methods	2018	2019	2020	2021	2022	Total
Wire transfer	\$56,924,372	\$84,599,095	\$83,190,511	\$150,480,009	\$167,709,188	\$542,903,175
Not Specified & Other	\$27,386,413	\$17,019,999	\$25,480,764	\$107,038,806	\$159,104,694	\$336,030,677
Cryptocurrency	\$8,643,554	\$8,248,482	\$22,540,247	\$77,564,511	\$125,911,221	\$242,908,014
e-Transfer	\$1,787,178	\$2,959,583	\$4,952,030	\$9,956,857	\$34,270,576	\$53,926,225
Direct deposit	\$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

Top 5 – Reports by Province/Territory

Province/Territory	2018	2019	2020	2021	2022	Total
Ontario	28,257	23,166	27,345	29,962	25,595	134,325
Quebec	15,488	14,398	18,350	21,120	20,078	89,434
British Columbia	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
Nova Scotia	1,312	1,075	1,503	1,451	1,480	6,821
New Brunswick	1,105	858	1,086	1,265	1,239	5,553
Newfoundland and Labrador	543	355	481	545	516	2,440
Prince Edward Island	209	128	227	295	243	1,102
Yukon	66	68	68	76	105	383
Northwest Territories	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

Above, five-year trends demonstrate that although wire transfer losses spiked in 2021 and lesser so in 2022, cryptocurrency losses continue to grow at a much faster pace; from \$8.2 million in 2019, to \$22.5 million in 2020, to nearly \$126 million in 2022. E-Transfer is also quickly growing as a popular type of fraud payment method.

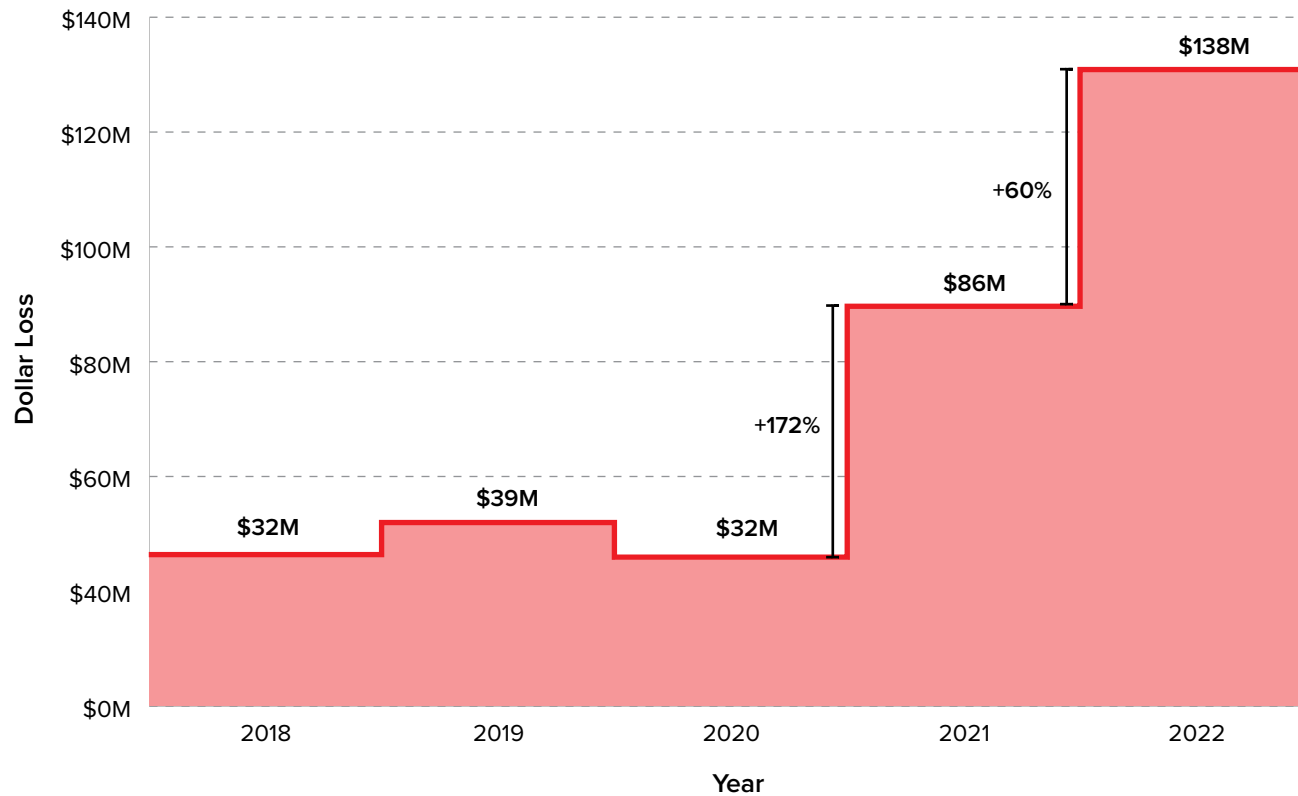
The CAFC consistently receives a majority of reports from Ontario and Quebec, followed by British Columbia and Alberta.

Year-Over-Year Dollar Loss Difference by Payment Method

Payment Method	# of Payment Method	YoY % - # of Payment Method	Dollar Loss	YoY % – Dollar Loss
Wire transfer	2,132	21.83% ▲	\$167,709,188	11.45% ▲
Other / unknown	3,349	10.35% ▲	\$159,104,694	48.64% ▲
Cryptocurrency	5,281	-0.13% ▼	\$125,911,221	62.33% ▲
e-Transfer	5,108	27.38% ▲	\$34,270,576	244.19% ▲
Direct deposit	4,954	-69.55% ▼	\$12,102,988	32.03% ▲
Cash	1,189	106.42% ▲	\$8,734,765	116.79% ▲
Cheque / Money Order / Bank Draft	424	1.92% ▲	\$8,510,772	41.85% ▲
Prepaid Card	2,377	-13.60% ▼	\$4,702,159	20.99% ▲
Credit card	6,324	-18.05% ▼	\$3,236,031	-26.63% ▼
Merchandise	1,337	-25.72% ▼	\$2,261,937	-60.21% ▼
Automatic Bank Withdrawal	354	25.09% ▲	\$1,500,186	41.55% ▲
IPS - Internet Payment Service (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% ▲
Debit card	494	6.01% ▲	\$258,468	-74.68% ▼
Moneygram	137	-33.50% ▼	\$217,909	-57.54% ▼
Transfast	11	-15.38% ▼	\$46,141	384.93% ▲
Not Available	62,127	-4.30% ▼	\$0	NaN
Vigo money transfer	4	0.00% ■	\$0	NaN

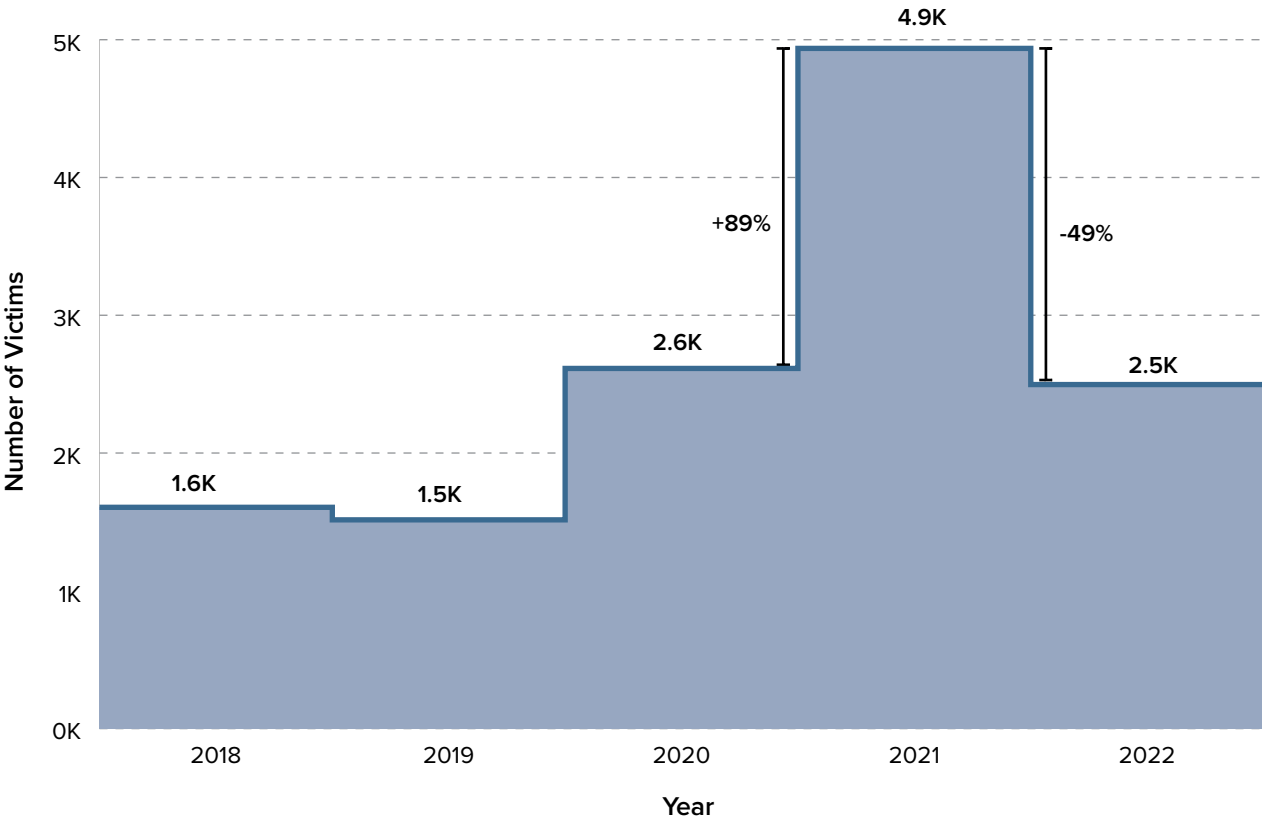
Comparing 2021 to 2022, losses by e-Transfer and cash increased significantly, followed by notable increases in cryptocurrency, among others. Cash losses are often connected to seniors and vulnerable victims sending packages of cash through courier services or money mules/cash collectors picking up money from their places of residence.

Senior (60+) – Dollar Loss by Year



Within a five-year time-span, seniors are targeted by both conventional and cyber-enabled fraud. The CAFC continued to see elevated losses in 2022 by this age group.

Senior (60+) – Number of ID Fraud by Year



The CAFC received fewer identity fraud reports in 2022 by seniors, receiving a number comparable to 2020.

www.antifraudcentre-centreantifraude.ca

