CANADIAN ANTI-FRAUD CENTRE ANNUAL REPORT 2021

- Internet and Cyber Fraud
- Mail Fraud, Identity Fraud and Identity Theft
- Telephone Fraud

FRAUD: RECOGNIZE REJECT REPORT

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, 2022.

ISSN: 2816-8348

PS61-46E-PDF

Executive Foreword

Fraud is often mistakenly framed as a less severe or impersonal crime, and victimization may be downplayed as carelessness on behalf of the victim. Victims may be blamed for being defrauded, or in other words, the fraud would not have occurred if they knew better. This narrative could not be further from the truth.

Canadians are being targeted and victimized by telephone calls, emails, social media posts, advertisements, and fraudulent websites by diverse and coordinated fraudsters and cybercriminals. Technological development has allowed for the monetization and transfer of personal information, creating challenges for individuals seeking to protect themselves from identity theft and fraud.[1] Most Canadians can be vigilant to the majority of fraudulent schemes, but it only takes one moment of distraction or lack of focus to be victimized. Exacerbating this issue is the increasing usage of cryptocurrency in fraud, which allows for the rapid international transfer and exchange of stolen funds.

The 2021 Annual Report provides a sober depiction of current fraud trends observed through the Canadian Anti-Fraud Centre (CAFC). 2021 saw $379 million in total reported fraud losses, which is 130 percent more than observed in 2020 and is the highest total reported annual losses in CAFC's history.

Nonetheless, these trends cannot overshadow the critical importance of the CAFC as an organization. Every day, the CAFC contributes to the deconfliction of fraud investigations with Canadian and international law enforcement, preventing and reducing the impact of fraud victimization. In 2021, the CAFC directly collaborated with partners to successfully recover $3.35 million lost to fraud.

Serving as the central point of fraud, the CAFC relies on the positive and mutually beneficial relationships with hundreds of partners from around the world. This includes collaborating with police services of jurisdiction, working with financial institutions regarding fraudulent activity, engaging cryptocurrency exchanges and assisting in the tracing of illicitly obtained cryptocurrency, and working with a range of partners to improve education and awareness of fraud as a persistent threat.

Canada must continue to embrace the many benefits created by a strong digital environment and economy, but we must also be aware of the current threat environment. As we become a more connected society, awareness of these threats and embracing stronger cybersecurity must be in close alignment. The trends and analysis in this Annual Report chart the importance of the CAFC's efforts to disrupt fraud and identity theft, increase fraud awareness, and educate Canadians on the threat that fraud and identity theft poses.

The 2021 Annual Report underscores the CAFC's dedication to supporting Canadians against fraud and identity theft. After becoming a National Police Service in 2021, the CAFC is in a strong position to continue to assist Canadians victimized by fraud and work with its partners to combat it across Canada. Although fraud is an unwelcome component of the rapid digitization of our society, the CAFC and Government of Canada are taking strong steps to support a safe and positive digital environment for all Canadians.

Chris Lynam
Director General
National Cybercrime Coordination Unit (NC3) and Canadian Anti-Fraud Centre (CAFC)
Royal Canadian Mounted Police

[1] Therrien, Daniel. (April 14, 2022). "The Evolution of Privacy Protection and the Case for Legislative Reform." *Office of the Privacy Commissioner of Canada.*

Executive Summary

The 2021 Canadian Anti-Fraud Centre (CAFC) Annual Report (the Report) provides a statistical review of fraud reporting to the CAFC, observed between January 1 and December 31, 2021. From these observations, the Report highlights significant trends in fraud and identity crimes. Additionally, the Report provides an overview of the CAFC's ongoing efforts and response to the dynamic fraud threat environment.

Highlighted are several important fraud and identity crimes reporting trends. Fraud, identity crimes and associated cybercrime are rapidly growing issues faced by an increasing proportion of Canadians. In 2020, the CAFC observed approximately $165 million in reported victim losses. In 2021, this number drastically increased to $379 million.[2]

Globally, Canadians rank near the top in terms of length of time spent online and are putting more personal information online than ever before. While this trend can be partially attributed to the ongoing COVID-19 Pandemic, the digital environment is expected to continue growing. Canada's digital economy is well positioned, and Canadians will continue to shop, communicate, and work online. Despite the benefits offered by the Internet of Things (IoT), growing Canadian participation in the digital environment will also create opportunities for fraudsters to target potential victims.

With all demographic groups being expected to use technology for many facets of their lives, young and vulnerable Canadians are being increasingly targeted by fraudsters. A second overarching trend observed by the CAFC in 2021 is that seniors (those aged 60 years and older), as well as younger Canadians are increasingly represented in fraud and identity theft reporting. While these groups are widely adopting the benefits of the digital world, they may not necessarily have as strong an understanding of the threat environment. The current trend underscores the need for further education and awareness surrounding cyber literacy and hygiene.

[2] These numbers as well as all other statistics in the Report are based on reports received by the CAFC Fraud Reporting System. Although this report portrays a diverse picture of fraud in Canada, it is important to recognize that only 5-10% of all fraud connected to Canadian victims is reported to the CAFC.

In addition to providing a detailed statistical overview of the CAFC's observed trends, the Report also highlights eight primary forms of fraud:

Type of Fraud	Trend
Investment	$164 million in losses in 2021, compared to $33.5 million in 2020.
COVID-Themed Fraud	$7.8 million in losses from March 6, 2020 to December 31, 2021.
Romance	$64.6 million in losses in 2021, compared to approximately $28 million in 2020.
Merchandise and Counterfeit Merchandise	$12.3 million and $1 million in losses observed in 2021, respectively; compared to $14.4 million and $250,000 in losses observed in 2020.
Extortion	$18 million in losses in 2021, compared to $16.5 million in 2020.
Phishing	7,190 reports observed in 2021, compared to 6,953 reports in 2020.
Spear Phishing	$54 million in losses in 2021, compared to $30.2 million in 2020.
Identity	29,500 reports to the CAFC in 2021 compared to 20,400 in 2020, representing an overall one-year increase of 45%.

The CAFC estimates that these trends will continue in 2022. In addition, the CAFC is observing the rapid growth of cryptocurrency-enabled fraud. Due to its pseudonymous nature and increasing ease of exchange, cryptocurrency will become more prevalent in reported fraud.

Finally, as a result of the declining impact of the COVID-19 Pandemic, the CAFC anticipates a gradual decline in COVID-19-related reporting. This trend may therefore be replaced by new fraud themes in 2022.

About the CAFC

The CAFC is the primary repository for fraud information and intelligence in Canada, and is a partnership jointly operated by the Royal Canadian Mounted Police (RCMP), the Ontario Provincial Police (OPP) and the Competition Bureau of Canada. The CAFC commits to providing timely, accurate, and useful fraud-related information to assist citizens, businesses, law enforcement, and government institutions in Canada and around the world. Through the intake of fraud reports the CAFC enables investigations and disrupts fraud by creating and disseminating information and intelligence for Canadian and international law enforcement and associated partners. Collectively, these efforts lead to a strong and united approach against fraud and identity crimes.

Additionally, the CAFC is the primary organization responsible for fraud awareness products and alerts in Canada. For instance, the CAFC is one of the leading organizations involved in the nationally recognized Fraud Awareness Month each year. In addition, the CAFC's employees and outreach team travel across Canada to provide up-to-date insights through their fraud awareness campaigns.

Located in North Bay, Ontario and originally established in 1993 as PhoneBusters, the CAFC was created in response to the growing threat of deceptive telemarketing practices. In 2022, fraudsters are increasingly enabled by the cyber environment, online communication, decentralized finance and

cryptocurrencies. While the threat continues to develop, the CAFC remains vigilant and responsive to the needs of Canadians. The CAFC is a critical component for reducing the impact of fraud on Canadians, recovering funds stolen through fraudulent activity, and when possible, seeking criminal prosecution of fraudsters. From 1993 to present day, the CAFC remains committed to providing education and assistance relating to fraud and identity theft.

CAFC Core Responsibilities

- Acting as the national fraud reporting centre by receiving online and telephone fraud reports from fraud victims and victimized businesses.
- Maintaining fraud and identity crimes intelligence and information.
- Assisting national and international law enforcement in deconflicting fraud and identity crime investigations, and acting as the liaison between law enforcement and financial institutions.
- Providing investigational capacity through cryptocurrency tracing and money tracking services.
- Engaging in fraud disruption activities with the assistance of partners. In doing so, the CAFC assists in money freezes and recoveries.
- Acting as one of the primary Government of Canada institution for fraud and identity crimes education and awareness efforts. The CAFC additionally provides guidance to seniors and vulnerable populations through its Senior Support Unit, offers advice to reporting victims, and maintains national awareness campaigns.
- Building the new National Cybercrime and Fraud Reporting System (NCFRS) in collaboration with the National Cybercrime Coordination Unit (NC3). This initiative will improve fraud reporting and allow the CAFC to develop a stronger national posture in deconflicting fraud.

$379m
TOTAL FRAUD LOSSES

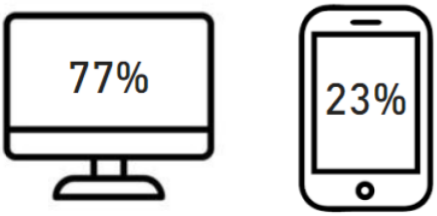
106,000
TOTAL REPORTS FILED

48%
REPORTS OF VICTIMIZATION

+130%
DOLLAR LOSS THAN 2020

+88%
SENIOR REPORTED ID FRAUD

ABOUT **3 IN 4 TOTAL REPORTS** WERE RECEIVED BY THE **CAFC ONLINE REPORTING SYSTEM**



Usage of **CRYPTOCURRENCY** in fraud increased by **238%** from 2020 to 2021.

Investment fraud represents the #1 fraud using Cryptocurrency as payment method with $50M in 2021.

“What our Partners Are Saying”

“Fraud costs Ontario residents and businesses hundreds of millions of dollars each year, and is one of the most under-reported and less understood crimes. Criminals who commit fraud exploit this reluctance and lack of understanding to prey on our communities. The OPP is proud to be a partner in the Canadian Anti-Fraud Centre to jointly combat fraud in Ontario and throughout Canada.”

“The Canadian Anti-Fraud Centre has continually demonstrated its commitment to tackling the fraud problem in Canada by being responsive and agile in its crime prevention, public education, and information sharing efforts. Working together, we increase our effectiveness exponentially. Partnerships such as the Canadian Anti-Fraud Centre are a force multiplier in our fight against fraud.”

Detective Superintendent Dominic Chong
Director, Financial Crime Services
Ontario Provincial Police

“The Canadian Anti Fraud Centre provides Canadian Financial Institutions with critical insight and timely reporting on fraud trending across Canada. They have played a key role in the public private partnership for almost two decades now. Through their transparent reporting on fraud trends, the public is kept informed and on guard to avoid becoming victims of crime.”

BMO Financial Group, Fraud Intake and Investigations

“The Canadian Anti-Fraud Centre provides invaluable intelligence on mass-marketing fraud, and their analysis and trend reporting are critical to our work at the Competition Bureau. Their work disrupts fraudsters and helps Canadians recognize and report suspected fraud. Their Senior Support program is an inspiring example of how government can work with volunteers toward a common goal: protecting Canadians from fraud.”

Matthew Boswell, Commissioner of Competition
Competition Bureau

“Following another successful year, the partnership between the Canadian Anti-Fraud Centre (CAFC) and the United States Secret Service (USSS) continues to flourish. With the on-going transnational criminal organizations targeting Canada and the United States, this partnership between the CAFC and the USSS has facilitated in the return of fraudulent funds for victims both in Canada and the United States. These victims are not only corporations but also individual Canadian citizens that have been defrauded out of their hard-earned money. The United States Secret Service Ottawa District not only values the strong working relationship with the CAFC but is truly honored to be a small part in helping to combat financial crimes alongside Canadian Law Enforcement.”

Resident Agent in Charge Eric Adams
United States Secret Service (USSS), Vancouver Resident Office

2021 Fraud Trends

Fraud in the Digital Era

Fraudsters are increasingly using society's digital reliance to target potential victims. Whether business email compromise in the workplace, investment fraud on your social media feed, remote access of your computer, or fraudsters impersonating your loved ones, fraud is unfortunately a too-common occurrence in Canada.

Over the past several years, many individuals and businesses have increasingly transitioned to providing and receiving services on digital platforms. Banking, investing, working, communicating, and accessing Government services have largely moved online. While it is indisputable that the COVID-19 Pandemic has expedited this shift, this trend will only accelerate going forward.

Fraud has evolved with changes to how Canadians use their digital environment. While the CAFC was initially created in response to the growth of telephone and mail fraud, the widespread adoption of computers and information technology has allowed fraudsters to move to this same domain. In 2015, approximately 50% of CAFC reports were cyber enabled. In 2021, approximately 75% of all reports were cyber enabled, and the CAFC expects this number to increase year-over-year.

Fraud operations are becoming increasingly comprehensive, deceiving, and complex. Increased access to Canadians at a low cost is enabling fraudsters to diversify and expand fraud operations. The cyber environment has eliminated traditional borders, allowing for international fraud operations to increasingly target Canadians.

Within this trend, threat actors are using darkweb marketplaces to exchange personal and financial information. Information that may be collected from a data breach of an organization may be sold or distributed on the darkweb to other cyber criminals, who will use the information commit other forms of cybercrime or fraud. The rapid and decentralized movement of illicit data is creating the potential for repeated victimization, with fraudsters finding more opportunities to access stolen personal information and contact potential victims around the world.

Victimization and Dollar Loss

2021 saw the highest reported fraud dollar loss in Canadian history, with the CAFC observing approximately $380 million in overall reported losses. In 2020, these reported losses totalled approximately $165 million. This statistic demonstrates that Canadians are losing more money per reported victimization.

How is the cyber environment enabling fraudsters?

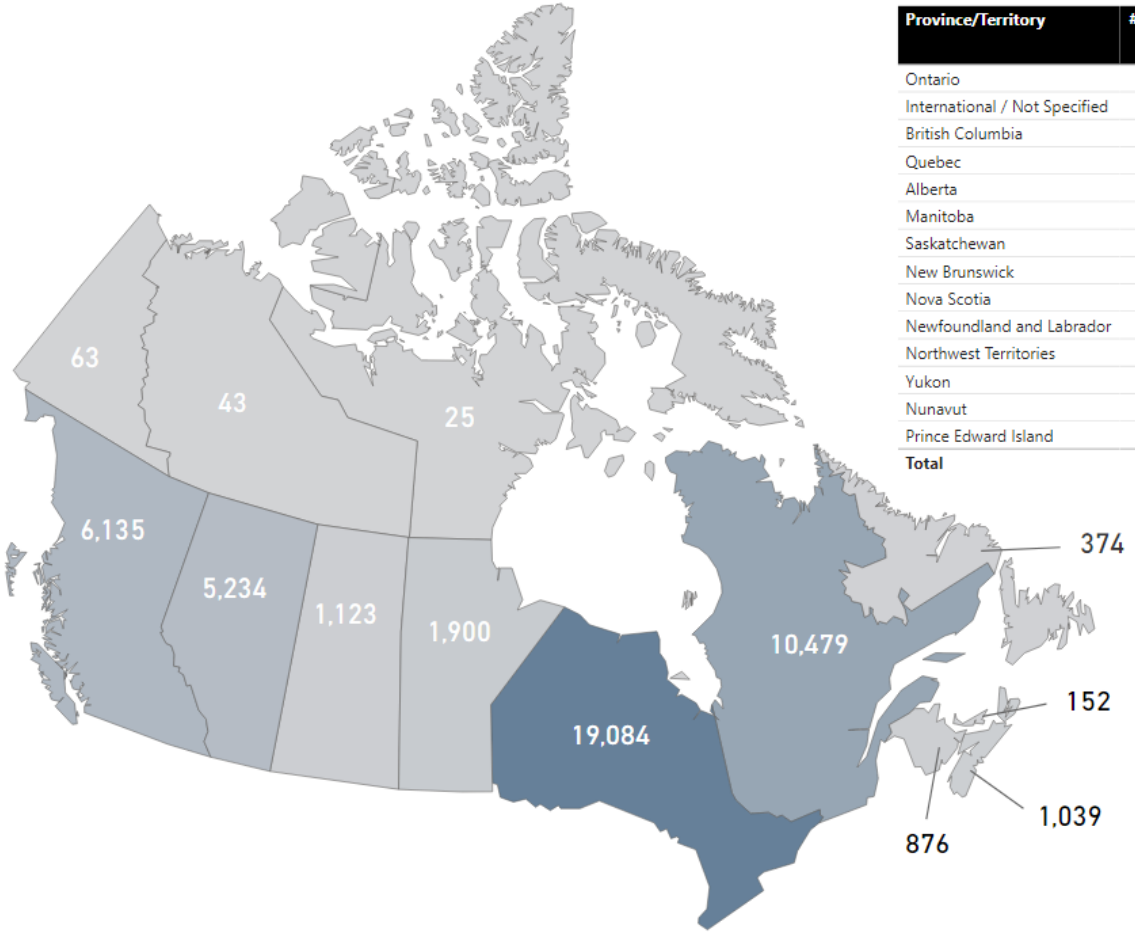
1. Making it easier to contact potential victims.
2. Increased ability to steal, purchase and exchange personal and financial information.
3. Reducing the cost and effort needed to target more Canadians with more diverse forms of fraud.

Top 10 Fraud Types - Number of total fraud reports, victims and dollar loss (2021)[3]

Type	# of Reports	% of Grand Total - Report	# of Victims	% Victimized	Dollar Loss	Average dollar loss per victimization
Extortion	9,230	12.6%	2,410	26.1%	$15,586,265	$6,467
Personal Info	5,941	8.1%	4,119	69.3%	$0	$0
Phishing	4,451	6.1%	1,283	28.8%	$0	$0
Service	3,488	4.7%	2,322	66.6%	$8,539,606	$3,678
Merchandise	3,404	4.6%	2,873	84.4%	$9,068,676	$3,157
Vendor Fraud	3,036	4.1%	1,898	62.5%	$7,122,341	$3,753
Job	2,227	3.0%	1,230	55.2%	$2,759,808	$2,244
Investments	2,205	3.0%	2,016	91.4%	$113,460,519	$56,280
Bank Investigator	1,619	2.2%	619	38.2%	$3,951,298	$6,383
Spear Phishing	1,323	1.8%	670	50.6%	39,529,067	$58,999
Total	**36,924**	**50.3%**	**19,440**	**52.6%**	**$200,017,581**	**$10,289**

[3] This graph represents the top forms of fraud observed by the CAFC in Canada. The CAFC also receives a large number of fraud reports from victims and victimized institutions in countries outside of Canada. Certain forms of fraud, like investment fraud, are represented in a relatively small number of reports, but have a very high average dollar loss. Additionally, the CAFC does not attribute a dollar loss valuation to forms of fraud like personal information theft, identity fraud and phishing, as it is impossible to find and apply an accurate valuation.

Number of Reports by Province/Territory/International (2021)



Province/Territory	# of Reports	# of Reports per Capita (100,000)	# of Victims	% Victimized	Dollar Loss
Ontario	19,084	134	9,713	50.9%	$142,681,717
International / Not Specified	26,919		12,004	44.6%	$110,201,721
British Columbia	6,135	123	3,212	52.4%	$41,482,397
Quebec	10,479	123	4,869	46.5%	$30,006,215
Alberta	5,234	123	2,643	50.5%	$29,980,131
Manitoba	1,900	142	1,008	53.1%	$10,652,189
Saskatchewan	1,123	99	614	54.7%	$4,788,047
New Brunswick	876	113	422	48.2%	$4,297,630
Nova Scotia	1,039	107	449	43.2%	$2,620,944
Newfoundland and Labrador	374	73	200	53.5%	$1,796,259
Northwest Territories	43	105	22	51.2%	$303,885
Yukon	63	157	33	52.4%	$126,561
Nunavut	25	68	15	60.0%	$86,062
Prince Edward Island	152	98	65	42.8%	$84,781
Total	**73,446**	**199**	**35,269**	**48.0%**	**$379,108,540**

Cryptocurrencies and Investment Fraud

Unlike physical and traditional forms of currency, most cryptocurrencies and digital currencies are not issued by a central banking authority like the Bank of Canada. Instead, individuals or groups can create a cryptocurrency with the currency's value validated through the user base and exchange between users, or as a result of the overall support by the user ecosystem. As the name references, cryptocurrencies and digital currencies are entirely digital, and transactions are recorded through a digital ledger system known as a blockchain. All transactions are recorded on the blockchain, and are identified by being given a unique cryptographic hash function, which is a unique string of numbers and letters used to differentiate between each transaction. In many cases, records of transactions are publicly accessible through a blockchain explorer, but the individual users completing the transaction and exchanging the cryptocurrency are not. In this respect, many cryptocurrencies and digital currencies are pseudonymous.

However, because all transactions are recorded, it is possible for law enforcement, organizations, and public users to use cryptocurrency tracing programs to follow the movement of the cryptocurrency. Cryptocurrency tracing is a common measure used to locate cryptocurrency connected to fraud and crime. When cryptocurrency is located to a wallet held on a cryptocurrency exchange, law enforcement can begin the process of freezing the funds in collaboration with the exchange service.

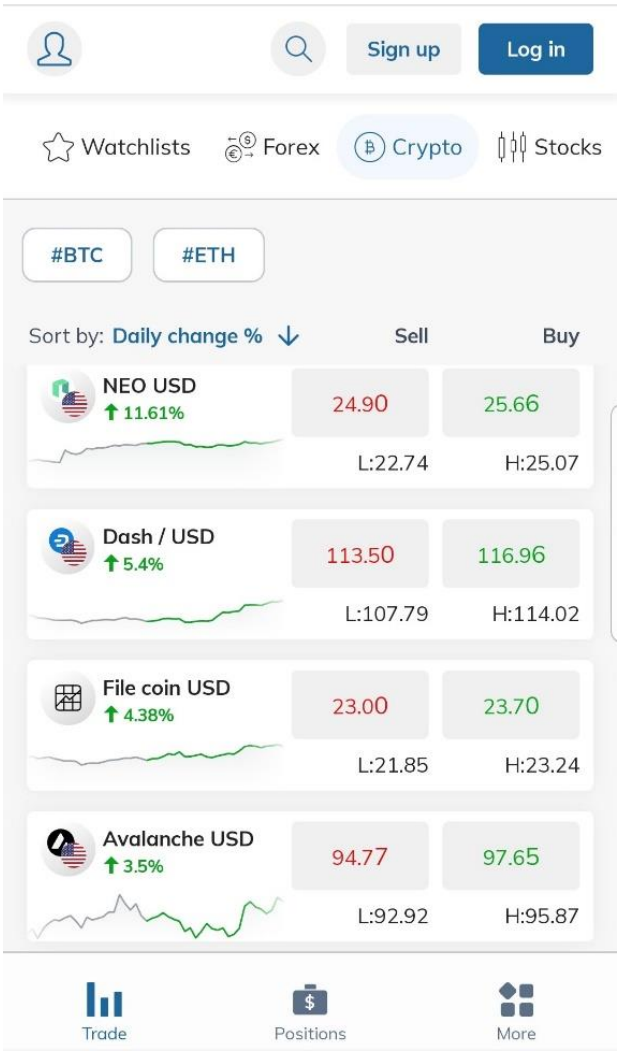
To further challenge law enforcement, fraudsters and criminal organizations use and operate cryptocurrency tumblers, also known as cryptocurrency mixing services. Cryptocurrency tumblers collect large amounts of cryptocurrency from numerous users into a pool, and randomly redistribute the cryptocurrency back to the users for a fee. Cryptocurrency tumbling is used to obfuscate the movement of cryptocurrency and limit law enforcement capacity to trace the movement of funds. Furthermore, fraudsters can move or launder funds through multiple types of cryptocurrency in numerous transactions while using multiple wallets, which can also obfuscate the movement of cryptocurrency and challenge tracing efforts.

Overall, as the identity of the user can be hidden or unknown, and because cryptocurrency can be quickly exchanged between users regardless of country of origin and destination, cryptocurrency and digital currencies are increasingly enabling fraudsters to victimize Canadians with a low risk threshold.

Cryptocurrencies are altering the financial world and are therefore also impacting fraud. The CAFC is observing cryptocurrency-enabled fraud in two general situations: As a theme in defrauding Canadians through cryptocurrency investment fraud; and as discussed above, as a method of facilitating the international movement and laundering of illicitly obtained funds.

Despite its extreme unpredictability, cryptocurrency is quickly becoming a popular investment avenue for Canadians. The rapid growth in cryptocurrency value and narratives of high investor returns is alluring, even when potential investors may not have a strong understanding of cryptocurrency as an investment. Preying on this lack of understanding, fraudsters are creating fraudulent dashboards similar to the image below to give the impression that funds are being legitimately invested. Once the money is invested, fraudsters alter the dashboard and through dialogue convince victims that their "investment" is quickly growing in value, enticing the victim to invest more. When the victim requests to withdraw money, communication ceases and it is only then that the victim recognizes that they have been defrauded.

Investment fraud is by far the costliest form of fraud observed by the CAFC. The CAFC observed 3,442 reports totalling nearly $164 million in losses, leading to an average dollar loss per report of $47,625. This is the most per report and the highest dollar loss compared to all other fraud categories. Investment fraud also produced the highest dollar loss for seniors (reporting victims aged 60 years and older). In 2021, seniors lost a total of $38 million in 487 total reports, creating the average dollar loss per report of $78,000.



An example of a fraudulent cryptocurrency dashboard. Fraudulent cryptocurrency exchanges usually appear very similar to legitimate exchanges.

Narrative:

Defrauded by an investment scam

"At the beginning of February 2021, we read an article about a famous Canadian's interview with a talk show host indicating how he had invested in Bitcoin and had large profits. In this article, there was a company that came up. Believing that this would be a credible company because it was in this article and not realizing that this article was fake, we requested information. The next day, they called us and we initiated the investment. We started out with small amounts and then led to larger ones.

They were trading for us initially with the intent of teaching us how to trade on our own. They were very informative and it was obvious that they knew what they were doing. We were informed that we could start withdrawing funds after 6 months. We sent money through e-transfer initially, then wires, and then bitcoin transfers.

Now that we are requesting for a return on investments, they are being very difficult to deal with and when they finally sent something, it was sent it in a matter where it is worth nothing."

How to protect yourself from investment scams

- Don't click on links or download attachments from unusual or unfamiliar sources, as they may contain malware or viruses.
- Beware of cryptocurrency investment advertisements, **especially those promoted on social media.**
- Always ask for detailed information on the investment, don't trust a platform based on its appearance alone.
- Verify if investment companies are registered with provincial securities agencies through the National Registration Search tool: Aretheyregistered.
- Don't let anyone pressure you into investing, and never share personal information
- Create complex passwords, use multi-factor authentication and practice safe cyber hygiene.
- Visit the CAFC website for more advice on how to protect yourself.

As it is challenging to identify who is exchanging and possessing cryptocurrency, the CAFC is observing cryptocurrency being used to launder funds illicitly gained through fraud. In another fraudulent methodology, by using money mules and illicit cryptocurrency exchanges, fraudsters can minimize detection and successfully convert fiat (government-issued) currency into cryptocurrency, and then back to another format of currency in another country.

Further, the expansion of cash-to-cryptocurrency Automated Teller Machines (ATMs) in Canada has streamlined certain forms of fraud. Canada currently has the second most Bitcoin ATMs in the world, with nearly 2,500 ATM locations.[4] In certain cases, fraudsters convince victims to convert fiat currency into cryptocurrency using ATMs, and then deposit the funds into the fraudster's wallet via the ATM.

Top 5 - Forms of Payment Methods Used in Fraud

Payment Methods	2017	2018	2019	2020	2021	Total
Wire transfer	$49,135,346	$57,874,116	$86,330,471	$84,090,514	$149,310,098	**$426,740,545**
Cryptocurrency	$3,378,428	$8,796,874	$9,641,612	$23,009,414	$77,872,155	**$122,698,484**
Credit card	$7,821,977	$7,575,199	$7,703,243	$5,604,652	$4,755,808	**$33,460,879**
Direct deposit	$3,173,530	$3,183,907	$3,343,850	$11,456,677	$12,266,015	**$33,423,979**
Cheque / Money Order / Bank Draft	$4,589,749	$5,890,769	$6,123,246	$7,201,645	$6,242,378	**$30,047,785**
Total	**$68,099,031**	**$83,320,865**	**$113,142,422**	**$131,362,902**	**$250,446,453**	**$646,371,673**

[4] Find more statistics relating to cryptocurrency ATMS at Coin ATM Radar.

COVID-19-Themed Fraud

Fraudsters often use a theme to engage the victim. Like most Canadians, fraudsters monitor changing political and social events, using specific trends to attract and exploit victims. By using themes within their fraud, fraudsters can take advantage of increased online searches and general interest in specific concepts.

The CAFC has observed COVID-19-themed fraud as a trend over the past two years. From March 2020 to December 31, 2021, the CAFC recorded 30,186 reports of COVID-19 fraud, totalling a dollar loss of $7.8 million. The primary types of fraud exploiting COVID-19 as a theme were merchandise, romance, vendor, and extortion fraud.

What is a money mule?

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.

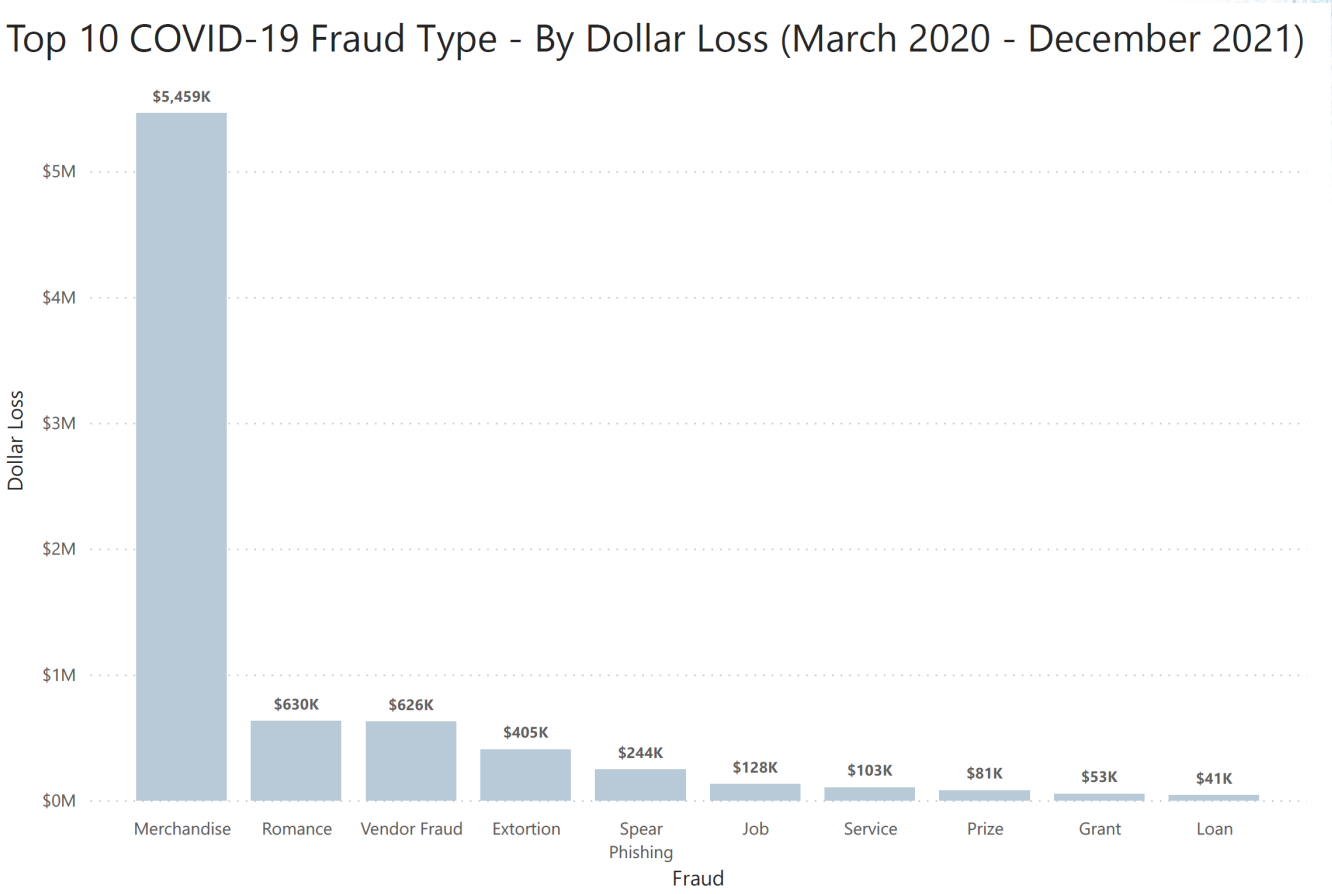
Money mules assist fraudsters by converting illicit funds into different currencies (e.g. to a cryptocurrency or from a cryptocurrency), and assisting in the transfer of the funds outside of Canada.

Within this theme, several notable fraud methods include[5]:

- Canadian Revenue Agency (CRA) Impersonation Fraud and Canadian Emergency Response Benefit (CERB) Fraud. For example, fraudsters impersonating the CRA or attempt to “assist” Canadians in accessing COVID-19 related benefits.
- Engaging in identity theft, stealing Canadian identities to access CERB.
- Fraudulently selling COVID-19-related health products, vaccines and merchandise.
- Generally using COVID-19 as a theme to attract website searches to fraudulent websites.

Although the significant and sustained COVID-19-related fraud activity may decline as the trend becomes less impactful, it is important to remember that fraudsters will always use notable themes to engage with and defraud Canadians. If you are questioning the legitimacy of a website or caller, the CAFC website frequently posts relevant alerts developed from ongoing fraud trend analysis.

[5] For more examples of COVID-19 fraud, please follow this link to the CAFC website



Romance Fraud

Over the past two years, Canadians have spent more time indoors and away from social events. Spending more time online than ever before, Canadians are also spending more time meeting others online.

Over the past year, the CAFC has observed a rapid growth in reported money lost to romance fraud. In 2020, Canadians lost nearly $28 million in 1,546 reports. Losses more than doubled in 2021, with the CAFC recording $64.6 million lost in 1,928 reports.

Merchandise and Counterfeit Merchandise Fraud

Just as Canadians are spending more time socializing online during the COVID-19 Pandemic, they are also spending more time shopping online. In this development, the CAFC has observed the increased occurrence of merchandise and counterfeit merchandise fraud. Whether selling counterfeit products at a heavily discounted price or offering the illusion of a product that will never arrive, fraudsters are using online marketplaces and creating their own marketplaces to defraud Canadians.

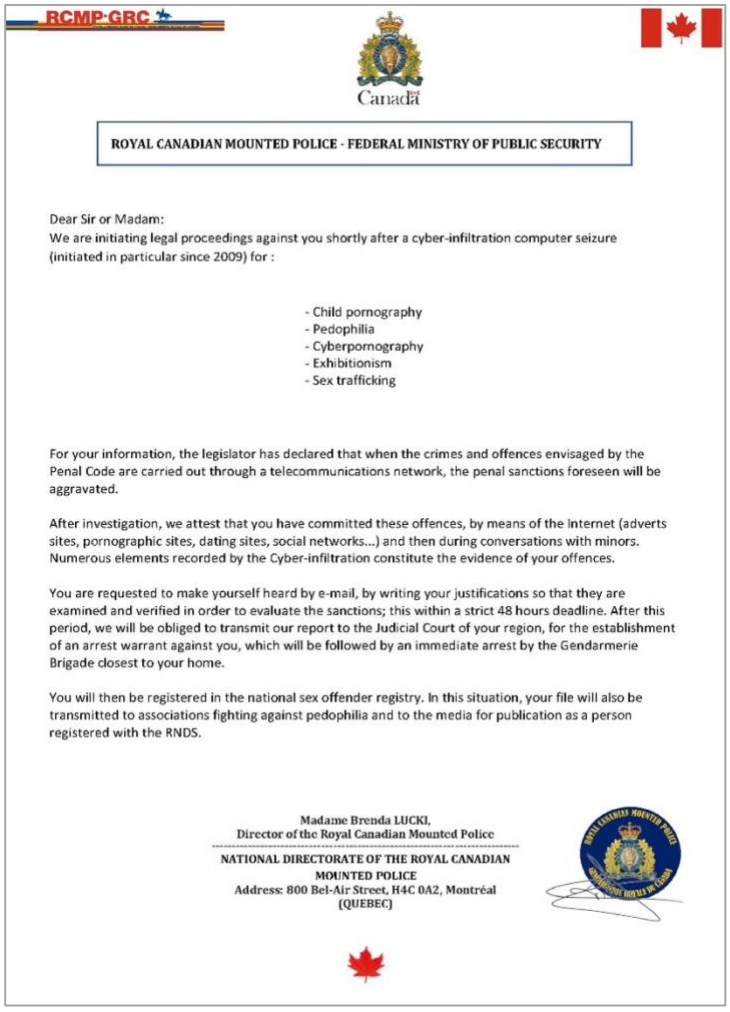
Merchandise fraudsters are also creating fake reviews for counterfeit products to create the perception that their product is of a higher quality, or that people are actually purchasing the products. In 2021, the CAFC observed approximately $12.3 million and $1 million in losses to merchandise and counterfeit merchandise fraud, respectively, in 10,194 total reports.

Extortion Fraud

Extortion, the practice of obtaining money through force or threats, continues to be the most prolific reported method of fraud in 2021. This past year, the CAFC received over 14,000 reports of extortion, totalling nearly $18 million in victim losses. While the CAFC received considerably fewer reports of extortion in 2021 compared to more than 30,000 reports observed in 2020, Canadians lost more per extortion victimization in 2021.

Fraudsters have found success using aggressive and blunt practices in coercing Canadians to be defrauded. Victims are being threatened with criminal charges, jail sentences, fines, death and direct harm to family members.

This is a significant concern for the RCMP and CAFC. Extortion fraud often overlaps with additional criminal offences. For an understanding of extortion fraud, below is an example of a fraudulent letter distributed to Canadians, with the fraudster attempting to impersonate the RCMP:



RCMP·GRC

Canada

ROYAL CANADIAN MOUNTED POLICE - FEDERAL MINISTRY OF PUBLIC SECURITY

Dear Sir or Madam:
We are initiating legal proceedings against you shortly after a cyber-infiltration computer seizure (initiated in particular since 2009) for :

- Child pornography
- Pedophilia
- Cyberpornography
- Exhibitionism
- Sex trafficking

For your information, the legislator has declared that when the crimes and offences envisaged by the Penal Code are carried out through a telecommunications network, the penal sanctions foreseen will be aggravated.

After investigation, we attest that you have committed these offences, by means of the Internet (adverts sites, pornographic sites, dating sites, social networks...) and then during conversations with minors. Numerous elements recorded by the Cyber-infiltration constitute the evidence of your offences.

You are requested to make yourself heard by e-mail, by writing your justifications so that they are examined and verified in order to evaluate the sanctions; this within a strict 48 hours deadline. After this period, we will be obliged to transmit our report to the Judicial Court of your region, for the establishment of an arrest warrant against you, which will be followed by an immediate arrest by the Gendarmerie Brigade closest to your home.

You will then be registered in the national sex offender registry. In this situation, your file will also be transmitted to associations fighting against pedophilia and to the media for publication as a person registered with the RNDS.

Madame Brenda LUCKI,
Director of the Royal Canadian Mounted Police

NATIONAL DIRECTORATE OF THE ROYAL CANADIAN MOUNTED POLICE
Address: 800 Bel-Air Street, H4C 0A2, Montréal (QUEBEC)

Narrative:

Defrauded by extortion fraud

"Initially making contact on WhatsApp, the fraudster acted as an employee of the Public Health Agency of Canada. He told me that my ID was stolen to apply for a phone SIM card, and to call the police using a specific number.

After calling this number, the fraudster acted as the police, and said that I was involved in a crime because my debit card was used to launder money. He asked me to cooperate and not to tell anyone. They said that another student told their parents, and this led to more charges. I was scared, so I followed their direction and sent them money through e-transfer.

After I paid them money, they kept contacting me. They would not stop threatening me and demanding more money."

Further, fraudsters committing extortion are increasingly targeting vulnerable and senior Canadians as they tend to be more susceptible to threats and coercion. In reports by those aged 60 and older, extortion comprised of 26% of all reports, with over 4,000 total reports and nearly $1 million in losses.

Phishing and Spear Phishing

Phishing is of low cost for the fraudster and allows the fraudster to target thousands of potential victims. Because of this simplicity, phishing and spear phishing continued to become more impactful in 2021.

In 2021, the CAFC received a total of over 9,000 spear phishing and phishing reports, with victim losses totalling nearly $54 million. It's important to note that beyond fraud and identity theft, spear phishing is associated to many different forms of cybercrime. Threat actors use carefully crafted spear phishing attacks to compromise company internal email accounts. This situation is known as Business Email Compromise (BEC), and is the most common spear phishing scheme observed by the CAFC. This gives the threat actor a hold within the company's internal infrastructure, which can therefore enable additional fraud or cybercrime.

How do fraudsters get my email address to send me phishing scams?

Sometimes, if you are using an app or accessing a website that asks for information like your email address, the website or app operator may choose to sell your information to other groups or people. As the information moves, it may be accessed by fraudsters.

Second, organizations holding databases of personal information, including email addresses, may be compromised by a cyber attack (known as being "hacked"). Similarly, inadvertently downloaded malware or viruses can lead to personal information theft from your devices.

This information eventually finds its way to online data marketplaces or is simply published online. Fraudsters use these datasets to engage in additional cybercrime not limited to accessing bank accounts, sending spam and scam emails, and stealing more personal information.

One resource to see if your email address has been compromised is haveibeenpwned, a not-for-profit website that aggregates data found in data breaches. If your email address was included in a data breach, make sure to create a new email address or change your password!

What is phishing?

Phishing is when a fraudster contacts you, appearing to be from a recognizable business or organization. The email will contain links or addresses, and may also request you to provide personal or financial information. Once obtaining this information, the fraudster will use it to access your accounts or steal money.

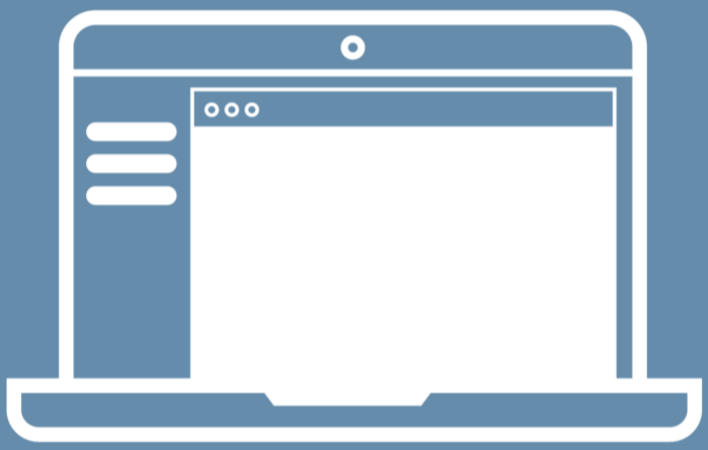
What is spear phishing?

Similar to phishing, **spear phishing** involves fraudsters sending emails to specific targets and pretending to be a business or organization.

Spear phishing differentiates from phishing, based on the fraudster often leveraging existing relationships between the organization and the individual. For instance, pretending to be the financial institution that you personally use. Spear phishing is targeted and specific to the victim, whereas phishing does not target specific organizations or individuals.

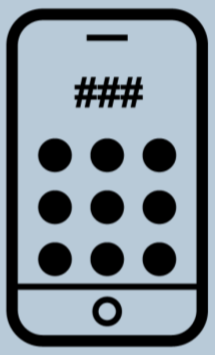
In spear phishing, the fraudster also appears to use a legitimate email or nearly identical address, which is a practice known as **spoofing**.

How Did Fraudsters Contact Canadians in 2021?



The CAFC received **16,126 reports** of suspects first contacting victims by email, and **10,847 reports** where first contact was through the Internet

The CAFC received **10,443 fraud reports** where the fraudster first contacted the victim by social media

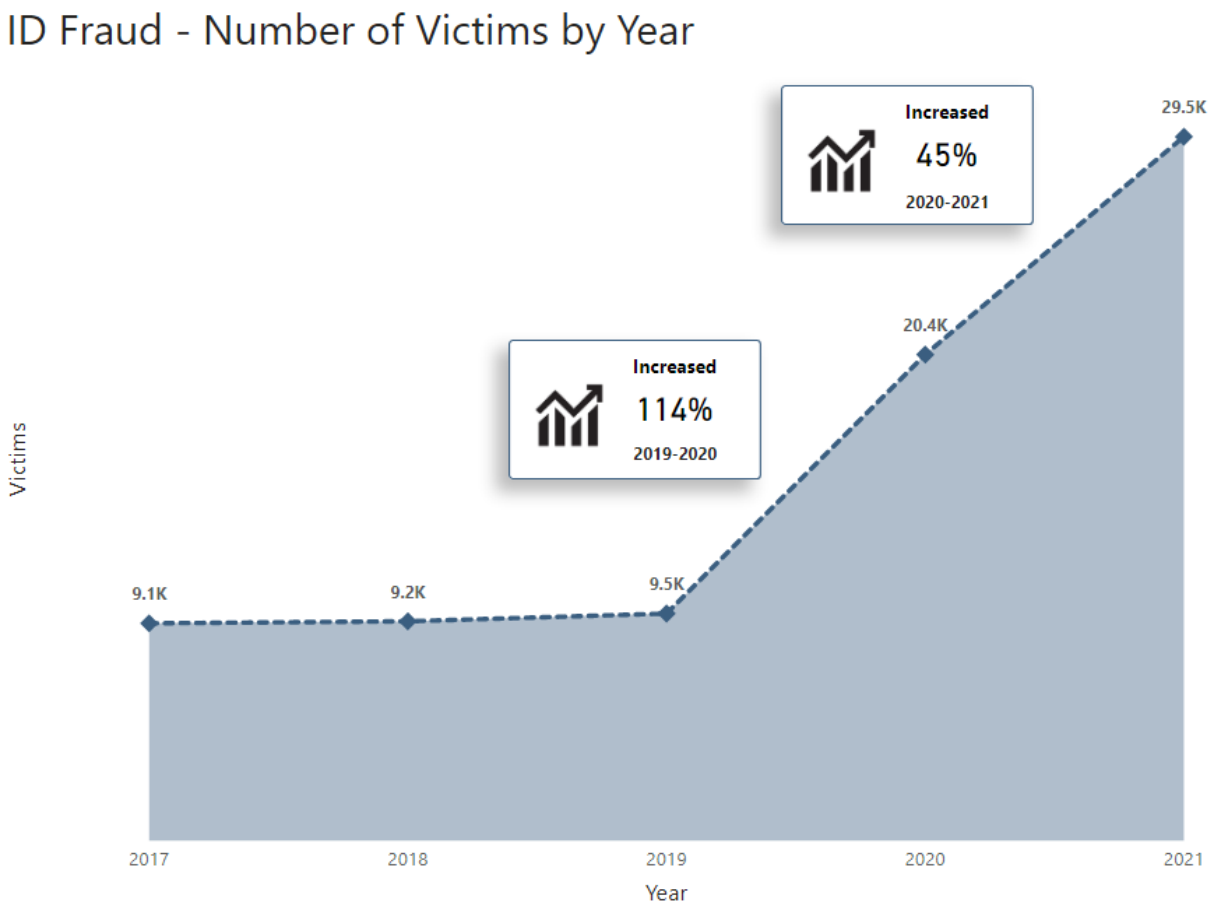


The CAFC received over **32,031 fraud reports** attributed to direct calls.

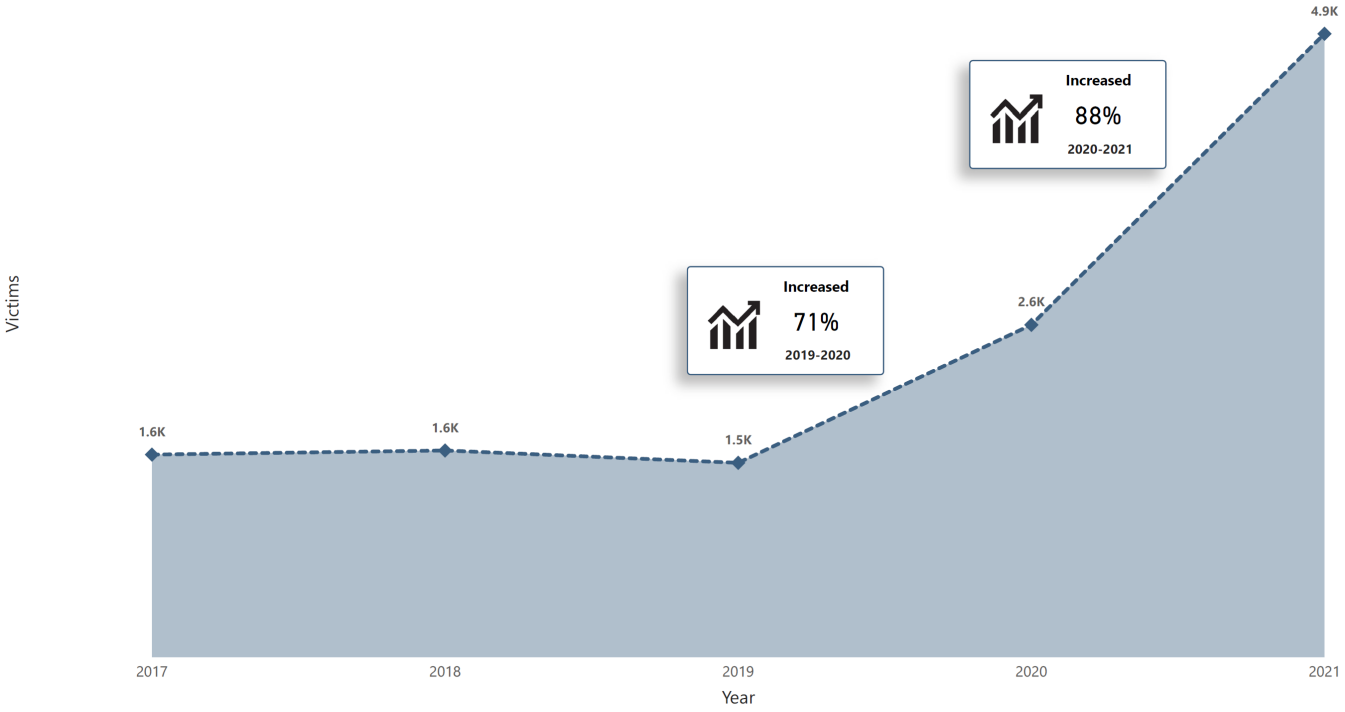
2021 Identity Theft and Identity Fraud Trends

As noted in fraud victimization statistics, the CAFC observed the growth of identity theft and fraud, continuing from previous years. In 2021, the CAFC received 31,782 reports of identity fraud, compared to 20,647 reports in 2020. Beyond identity fraud, the CAFC also observed a significant number of personal information theft reports. In 2021 the CAFC received 7,566 personal information theft reports, which is the second-largest reporting field and continues the trend observed in 2019 and 2020.

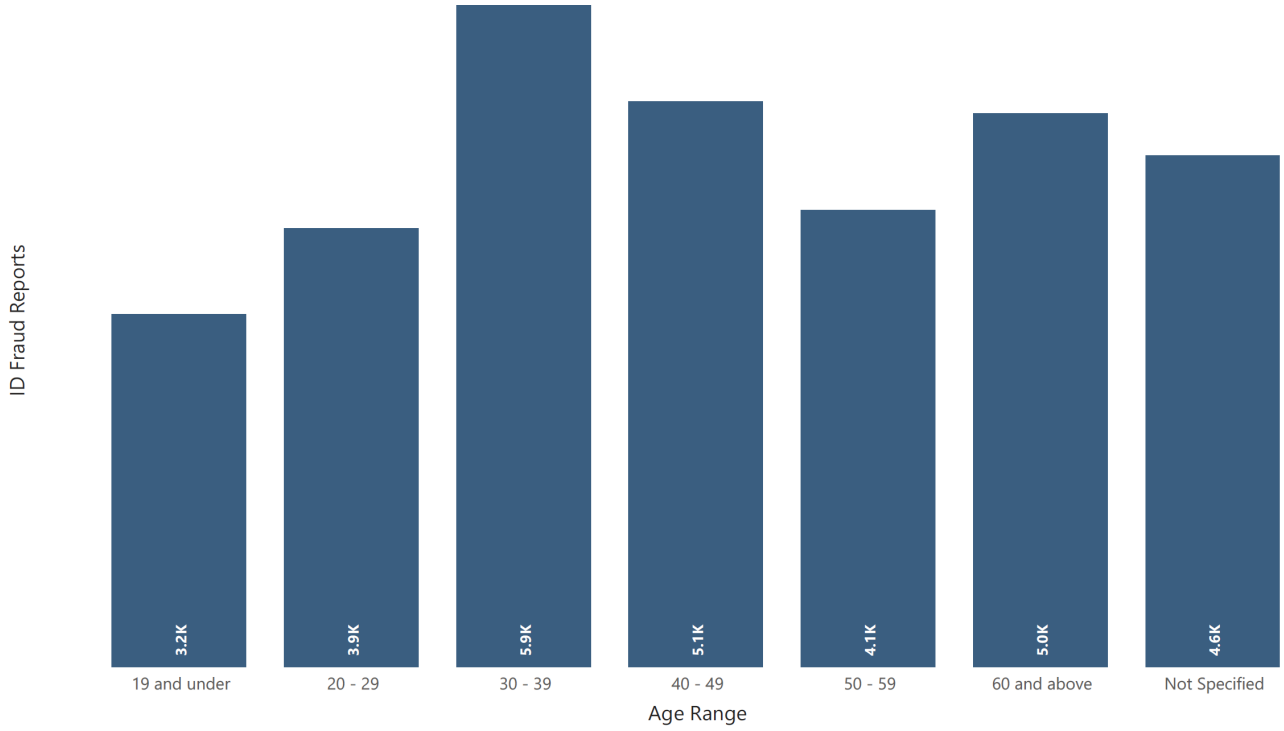
Notably, seniors are being targeted for identity-related crime. Overall, 2021 saw 4,853 identity fraud reports by seniors, compared to 2,587 reports in 2020. Further, in 2021 seniors reported a total of 1,519 instances of personal information theft, compared to 1,407 instances in 2020.



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



Number of ID Fraud Reports by Age Range (2021)



CAFC Activities to Address Fraud

Demonstrated in the statistical trends observed in 2021, fraud and cyber-enabled fraud is becoming increasingly prevalent. Canadians are losing more money and more Canadians are being victimized year-over-year. Although this trend is unlikely to change in the near future, the CAFC is committed to having a positive impact for Canadians. The CAFC assists in freezing or recovering funds by following the movement of funds to accounts, in collaboration with Canadian and international financial institutions. In doing so, the assisting financial institutions can temporarily freeze money to be reclaimed by victims of fraud. In 2021 alone, the CAFC assisted in **36** instances of freezing or recovering funds totalling approximately **$3.35 million**. In one notable instance from 2021, the CAFC assisted in recovering **$1.2 million** for a victim.[6]

The CAFC also has access to cryptocurrency tracing technology, which can assist in the recovery of stolen cryptocurrency through collaboration with cryptocurrency exchanges. This success is in addition to the frequent instances of successful fraud disruption, preventing the loss of funds to fraud.

In collaboration with partners across Canada and internationally, a total of **$3.35M** was **RECOVERED** for Canadians after reporting a fraud in 2021.

But We Can't Do It Alone

Since the CAFC functions as a fraud report intake mechanism to collect information and intelligence as it relates to fraud and identity crimes, the CAFC relies on the assistance of its wider community and the Canadian public to stop fraud.

The CAFC works with hundreds of partners in several key roles:

1. Exchanging information and intelligence as it relates to individual reports, after receiving expressed consent in the reporting process.
2. Working with financial institutions, government organizations, currency and cryptocurrency exchanges, law enforcement, shipping companies and courier services to disrupt fraud and identity theft.
3. Sharing up-to-date fraud trends with partners, creating awareness of the fraud landscape.
4. Sharing fraud prevention material and statistics.
5. Responding to media requests with accurate and relevant material.
6. Providing education and fraud awareness, stopping crime before it happens.

In 2021 alone, the CAFC responded to 382 media requests.

[6] The CAFC provides actionable intelligence for law enforcement and financial partners, who then complete fraud recoveries when possible. Although this statistic is valuable for reference, recoveries assisted by the CAFC requires partners to report back on the final outcome of files. Partners may not report back to the CAFC, and as such this statistic is likely undervalued.

The CAFC and NC3:
Partners in Addressing Fraud and Cybercrime

On April 1, 2021, the RCMP National Cybercrime Coordination Unit (NC3) and CAFC became partner organizations under the same operational branch of the RCMP. As fraud and identity theft is inextricably linked to the cyber environment, the NC3 and CAFC's mandates closely align.

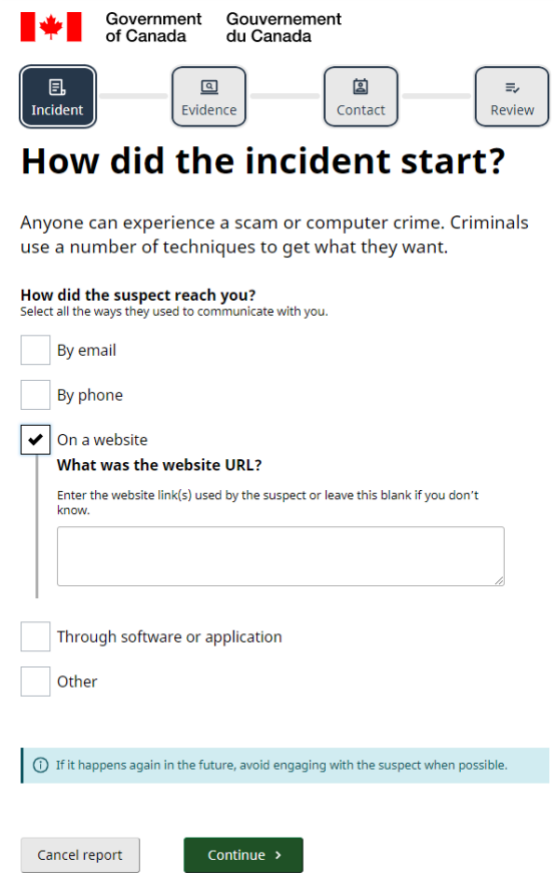
The NC3, created following the 2018 National Cyber Security Strategy, coordinates cybercrime investigations involving multiple policing jurisdictions in Canada and abroad. The NC3 primarily focuses on technology-as-a-target cybercrime, which includes ransomware, malware-based cybercrime, data breaches and related cybercrime. Additionally, the NC3 provides technical capabilities, cyber intelligence and analysis for Canadian law enforcement and international partners, having an impact on cybercrime around the world.

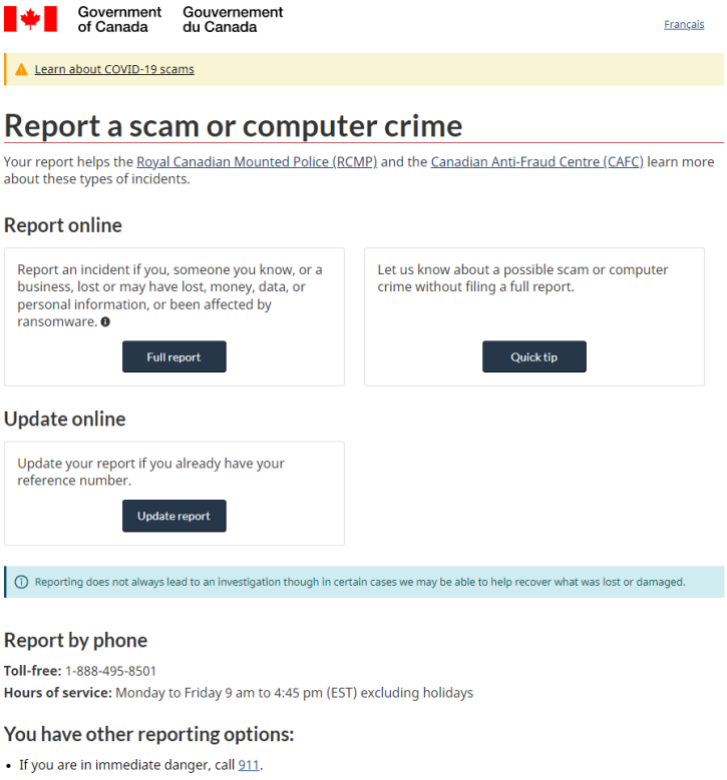
Currently, the CAFC and NC3 are building a **new national cybercrime and fraud reporting system (NCFRS)** for Canadians and businesses, creating the single source for cybercrime reporting. The CAFC and NC3 appreciate your input to help design the NCFRS. Take part in our research and become a volunteer: https://report.antifraudcentre.ca/recruitment.

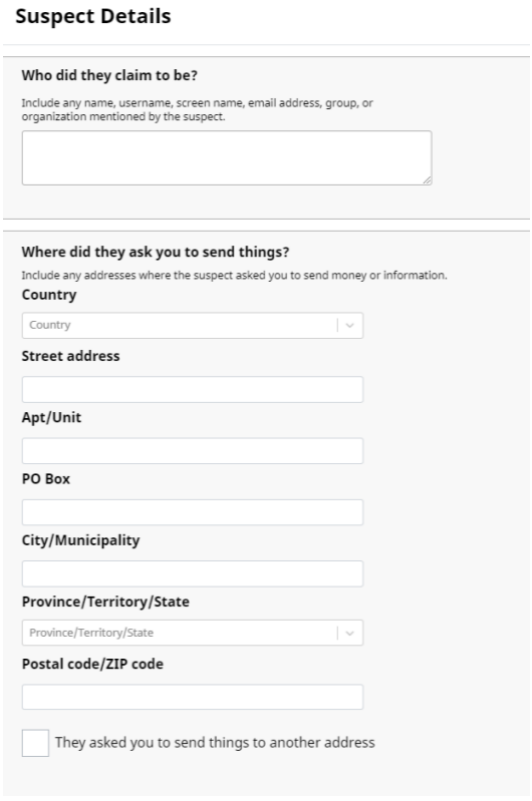
From 2021 onwards the NC3 and CAFC are united partners in addressing fraud and cybercrime, and will continue to be valuable resources for Canadian and international law enforcement.

New National Cybercrime and Fraud Reporting System (NCFRS) Fast Facts

- Currently in Beta Version, the New National Cybercrime and Fraud Reporting System (NCFRS) is scheduled to be fully operational in 2023.
- In 2021, the NCFRS had:
  - 13,317 total visitors.
  - 2,880 total reports received (3% of daily anticipated reports.
  - Conducted user research with volunteers.
  - 51% total full-report completion rate.
  - 41% of total users who submitted a report.







How the CAFC Makes a Difference

STOPPING FRAUD BEFORE IT HAPPENS

- Providing dedicated fraud awareness campaigns for Canadian communities, and leading the March Fraud Awareness Month
- Acting as the Canadian source for fraud and identity theft material and education

AFTER A FRAUD VICTIMIZATION

- Operating the national fraud reporting system
- Creating fraud reports, collecting reported information and intelligence

AFTER A FRAUD REPORT IS CREATED

- Working with Canadian and International law enforcement and financial institutions
- Acting as the liaison between partners and victims

LOCATING LOST FUNDS

- Provide direction to temporarily freeze, and assist in the recovery of stolen funds
- Performing cryptocurrency tracing
- Assisting law enforcement with file information and intelligence

PREVENTING RE-VICTIMIZATION

- Referring victims to the Senior Support Unit
- Providing post-victimization educational material to prevent re-victimization
- Refer victims to non-profit organizations

WORKING WITH PARTNERS

- Partnered with the National Cybercrime Coordination Unit to deconflict ransomware and mandate-related cybercrime
- Exchanging fraud information and material with financial institutions, banking association and police partners

Success Stories at the CAFC

Cryptocurrency Success

Reclaiming stolen cryptocurrency is exceptionally challenging. The pseudonymous and decentralized format of cryptocurrency, as well as the many potential avenues to launder and convert cryptocurrencies create a considerable challenge for law enforcement. As such, success in cryptocurrency-related fraud continues to be limited. Nonetheless, the CAFC remains responsive to this new technology.

From one example in 2021, an Ontario victim was deceived into sending $40,000 in Bitcoin to a bank investigator cryptocurrency fraud. Reacting quickly, the CAFC was able to trace the stolen cryptocurrency to an account held by an individual located in India, relaying the intelligence and account information to the investigating body. The investigating officer contacted the cryptocurrency exchange holding the funds, which then froze the stolen assets toward the eventual return of the stolen funds to the victim.

Cryptocurrencies and decentralized currencies will likely become adopted by more Canadians as investments and exchangeable currency. However, these forms of currency will also continue to be used by fraudsters to obfuscate the movement of illicit funds. In response, the CAFC regularly provides assistance to law enforcement in this form of fraud.

Senior Support Unit Success

The CAFC Senior Support Unit (SSU) is comprised of community volunteers dedicated to reducing the impact of fraud across Canada. The SSU is a critical component of the CAFC, providing advice, education and assurance to vulnerable Canadians targeted by fraudsters.

In an instance of SSU success, on August 2021, the SSU contacted a victim who had sent $25,000 to a mailing address in Ukiah, California. Using this address and in working with Ukiah police, the CAFC was able to locate the package addressed to another elderly victim. It was later discovered that this elderly individual was previously victimized by the same fraud, and was acting as a money mule in the hopes of reclaiming her own money lost to the same fraud. As a result of the investigation, police were able to reclaim the lost $25,000 for the Canadian victim.

Partnerships Success

Reducing the impact of fraud requires a complex team of law enforcement, financial institutions, monetary exchanges and other additional partners. Most fraud investigations require collaboration by numerous organizations in law enforcement and the financial sector. The CAFC is committed to developing strong partnerships to have a positive impact on disrupting and reducing fraud.

For example, Canadian and American businesses enjoy a strong economic relationship and require the fast transfer of currency through streamlined payment methods. Small and medium-sized businesses frequently use money transfers as an easy and accessible method to exchange currency for goods and services. This is often facilitated by email communication between businesses. In many cases, businesses exchange banking information via email prior to exchanging funds.

In one instance, a Canadian company was victimized by a spear phishing attack by a group or individual impersonating a business with a strong relationship to this company. After being defrauded for approximately $1.1 million, the business acted quickly and in less than 24 hours filed a report with the CAFC. The CAFC immediately worked with the United States Secret Service (USSS), which was then able to assist in freezing the lost funds by working with an American financial institution. From the fast reaction by all organizations involved, nearly all of the lost money was recovered for the victim organization.

Future Efforts and Moving Forward

As the fraud landscape continues to develop, the CAFC will act as a responsive resource for Canadians and organizations. In this respect, the CAFC is in the process of outlining several priority areas of focus.

The CAFC will continue to develop a stronger partnership regime with the NC3. Cybercrime and fraud increasingly overlap and require a united law enforcement response. Working closely with the NC3 will increase information sharing, improve reporting through the forthcoming fraud and cybercrime reporting system, and strengthen communication channels between both organizations. Additionally, this partnership will leverage previously founded partnerships with government, law enforcement, financial institutions and other organizations.

The CAFC will also build stronger partnerships with partners focused on fraud and identity crimes. Serving as an intelligence-driven organization between investigating bodies, victims and victimized organizations requires a concerted effort. Specifically, CAFC will continue to evaluate the impact of cryptocurrencies in enabling fraud and potential responses.

Reporting by Canadians is fundamental to the work of the CAFC and underpins its ability to deliver on its mandate. Online reporting is a valuable tool in the reporting process, but also engaging vulnerable or less technologically savvy victims by phone to provide guidance, support and prevention will continue to be important going forward.

As per this report, fraud and identity crimes victimizes more Canadians year-over-year, producing more losses per victimization across nearly all forms of fraud. This has demonstrated the necessary value of many CAFC services. The evolving threat environment and exponential growth of fraud require the CAFC continually adapt to be effective.

Capabilities such as cryptocurrency tracing, intelligence analysis, prevention activities and public outreach continue to play key roles in reducing the threat of fraud. Overall, the CAFC will continue to monitor reporting trends and the impact of fraud on Canadians, and will look for ways that the organization can evolve to respond to this demand.

What you can do to prevent fraud and identity crimes

1. Report any instance of fraud or attempted fraud to your local police and the CAFC
   - Doing so can lead to potential fraud resolutions, including the recovery of lost funds and the attribution and arrest of fraudsters. Reporting provides critical insight and information into fraud trends. This assists the CAFC and law enforcement on approaches to reducing the impact of fraud.
   - If Canadians didn't report successful and attempted fraud and identity crimes, the CAFC would be unable to develop a strong understanding of the threat environment. Accurate victim reporting is the best way to create an understanding of the true impact of fraud.
2. Follow fraud awareness campaigns led by the CAFC and its partners
   March is the Fraud Awareness Month, the national effort in providing education and informative material on what fraud is and how to avoid it.

   Follow the CAFC's Twitter and Facebook pages and review the CAFC's website for up-to-date information on fraud and identity theft.

3. Act as a community leader against fraud and identity crimes
   Know how to spot fraud and help protect your community, friends and loved ones. Everyone can have an impact in reducing fraud in Canada.

Conclusion

The 2021 Annual Report outlines a record year for fraud losses by Canadian victims. Based on the current trend, there are indications that fraud and identity theft will continue to increase. To address this development, it is important for all Canadians become more aware of the current fraud threat environment. The CAFC recommends Canadians report all observed fraud to local police and the CAFC, by telephone or through the online reporting system.

The CAFC is actively working to give a stronger understanding of fraud to Canadians. With the growing trend of fraud victimization and the increased cost of fraud, the CAFC will continue to position itself as the national advocate for fraud reporting, deconfliction, intelligence, education and awareness.

About the Numbers

The statistics within the 2021 Annual Report are sourced from all reports received and verified by the CAFC between January 1 and December 31, 2021. 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. The statistics in the Annual report contain reports from both attempted victimizations and actual victimizations.

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 specific forms of fraud.

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

Additional Statistics

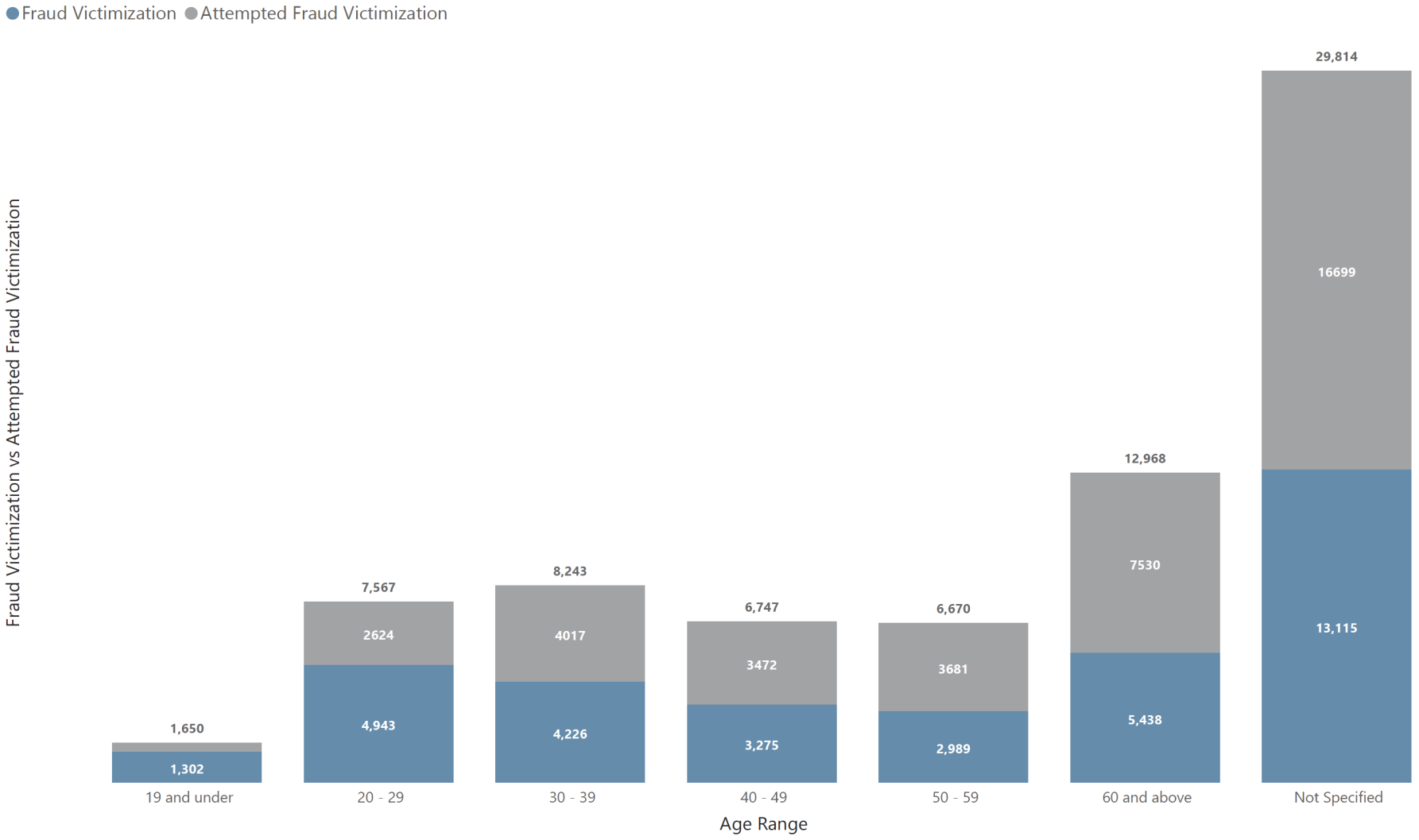
Number of ID Fraud Victims per Capita (100,000) by Province/Territory/International

Province/Territory	# of Victims	# of victims per Capita (100,000)
Quebec	9,986	117
Prince Edward Island	133	86
Ontario	8,372	59
British Columbia	2,779	56
Alberta	2,223	52
Manitoba	650	48
New Brunswick	351	45
Saskatchewan	493	44
Nunavut	14	38
Nova Scotia	363	37
Newfoundland and Labrador	153	30
Northwest Territories	11	27
Yukon	10	25
International	3,929	
Not Specified	27	
Total	**29,494**	**80**

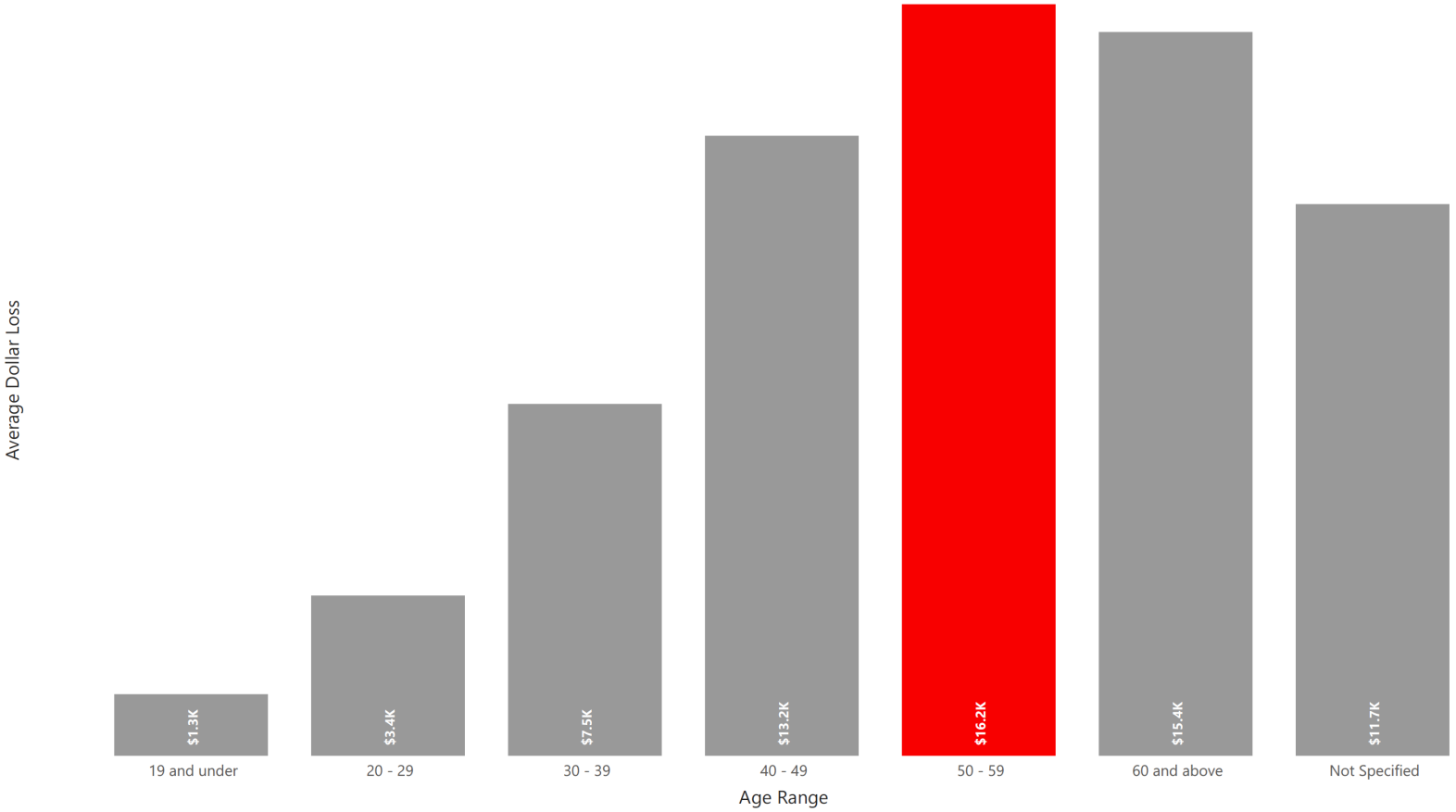
Number of ID Fraud Victims by Province/Territory/International (2017-2021)

Province/Territory	Victims (59 -)	Senior Victims (60 +)	Total Victims
Ontario	20,335	5,528	25,863
Quebec	18,939	2,870	21,809
British Columbia	7,446	1,654	9,100
International	8,063	68	8,131
Alberta	5,916	991	6,907
Manitoba	1,544	332	1,876
Saskatchewan	1,111	260	1,371
Nova Scotia	758	171	929
New Brunswick	700	131	831
Newfoundland and Labrador	327	68	395
Prince Edward Island	210	34	244
Not Specified	101	18	119
Northwest Territories	35	5	40
Yukon	30	6	36
Nunavut	24	3	27
Total	**65,539**	**12,139**	**77,678**

Number of Attempted Fraud Victimizations vs Fraud Victimizations by Age Range

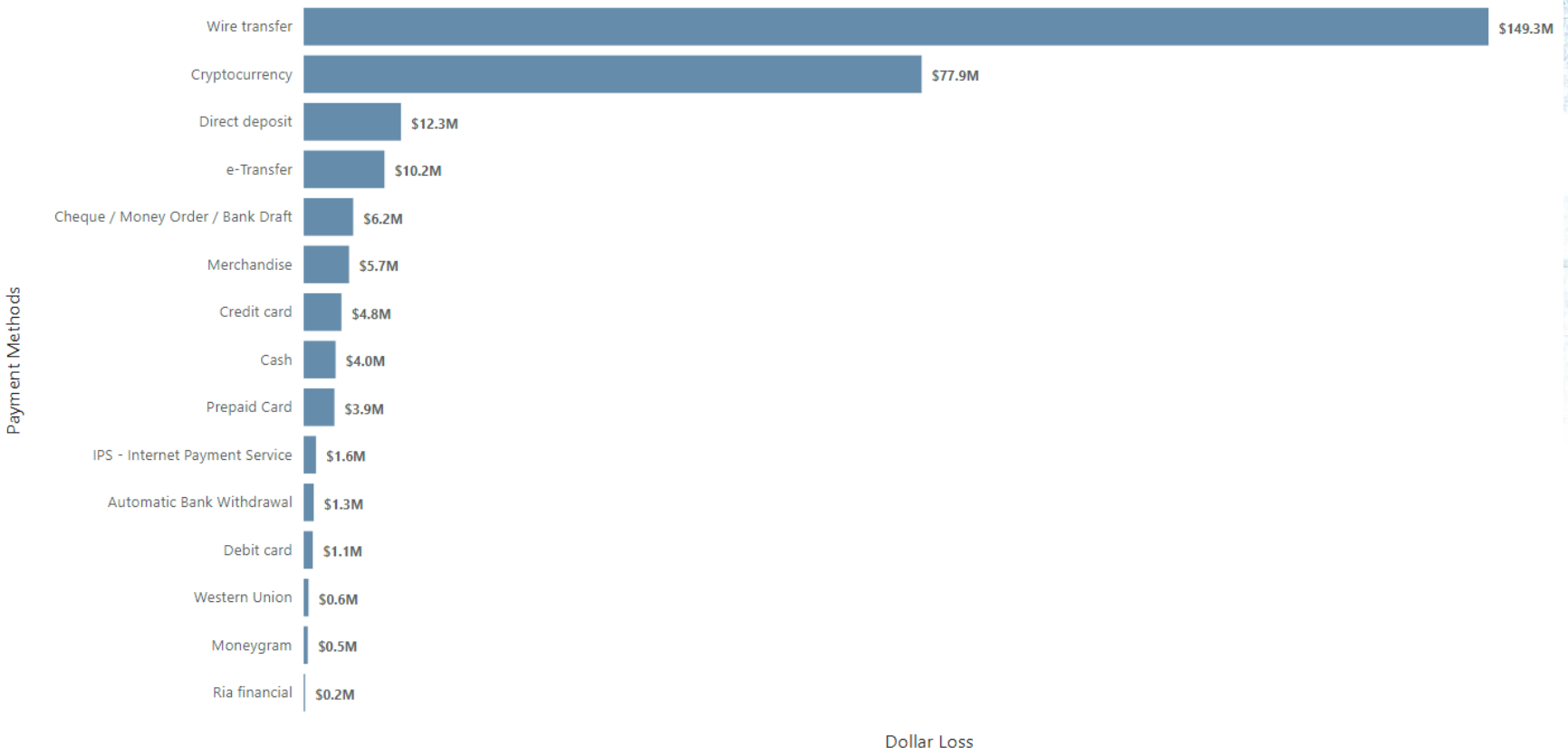


Average Dollar Loss by Age Range

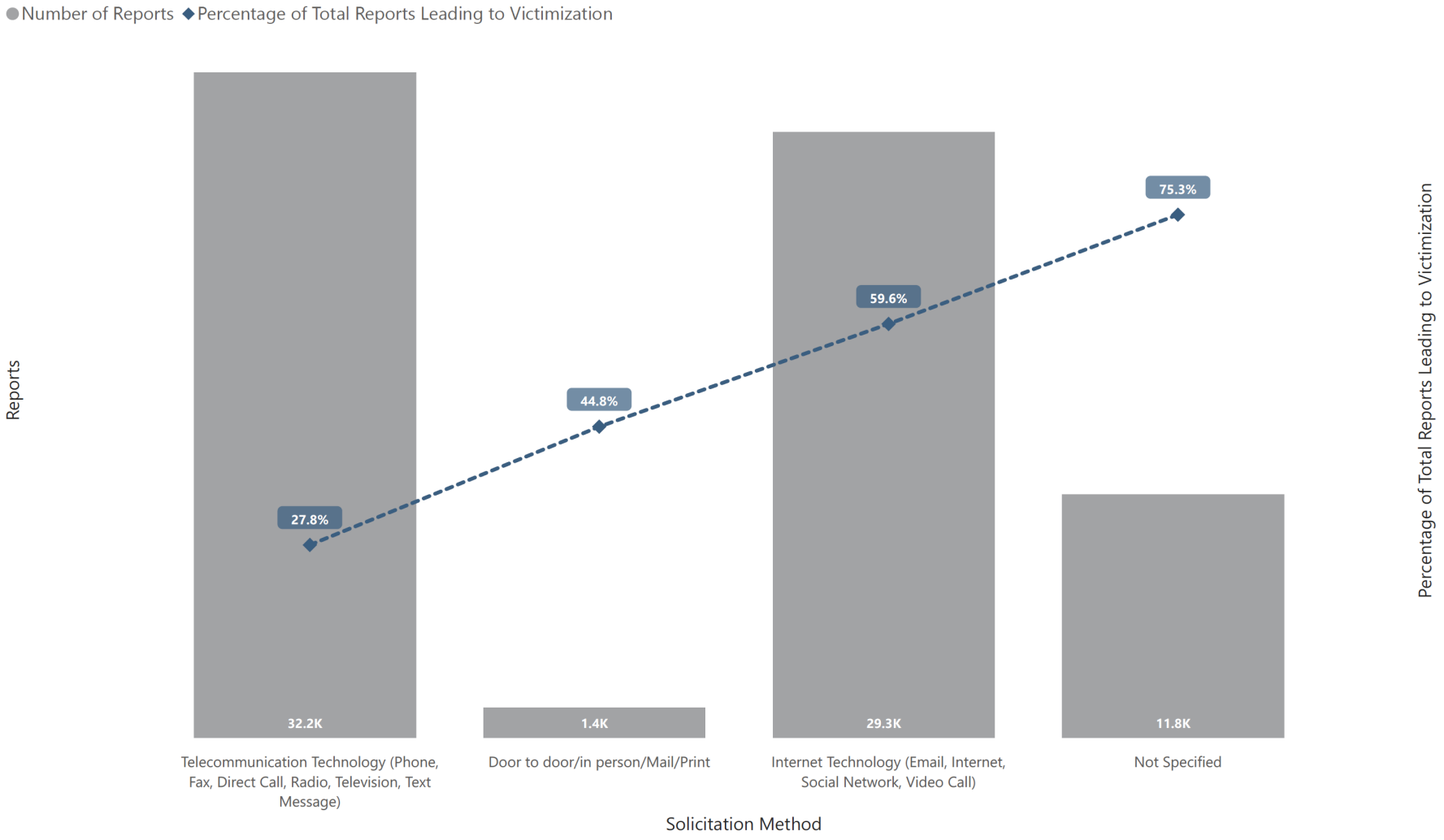


Age Range	# of Reports	# of Victims	% Victimized	Dollar Loss	Average dollar loss per victimization
19 and under	1,650	1,302	78.9%	$1,696,112	$1,303
20 - 29	7,567	4,943	65.3%	$16,813,067	$3,401
30 - 39	8,243	4,226	51.3%	$31,646,550	$7,489
40 - 49	6,747	3,275	48.5%	$43,223,792	$13,198
50 - 59	6,670	2,989	44.8%	$48,311,236	$16,163
60 and above	12,968	5,438	41.9%	$83,798,264	$15,410
Not Specified	29,814	13,115	44.0%	$154,089,617	$11,749
Total	**73,659**	**35,288**	**47.9%**	**$379,578,639**	**$10,757**

Dollar Loss by Payment Methods



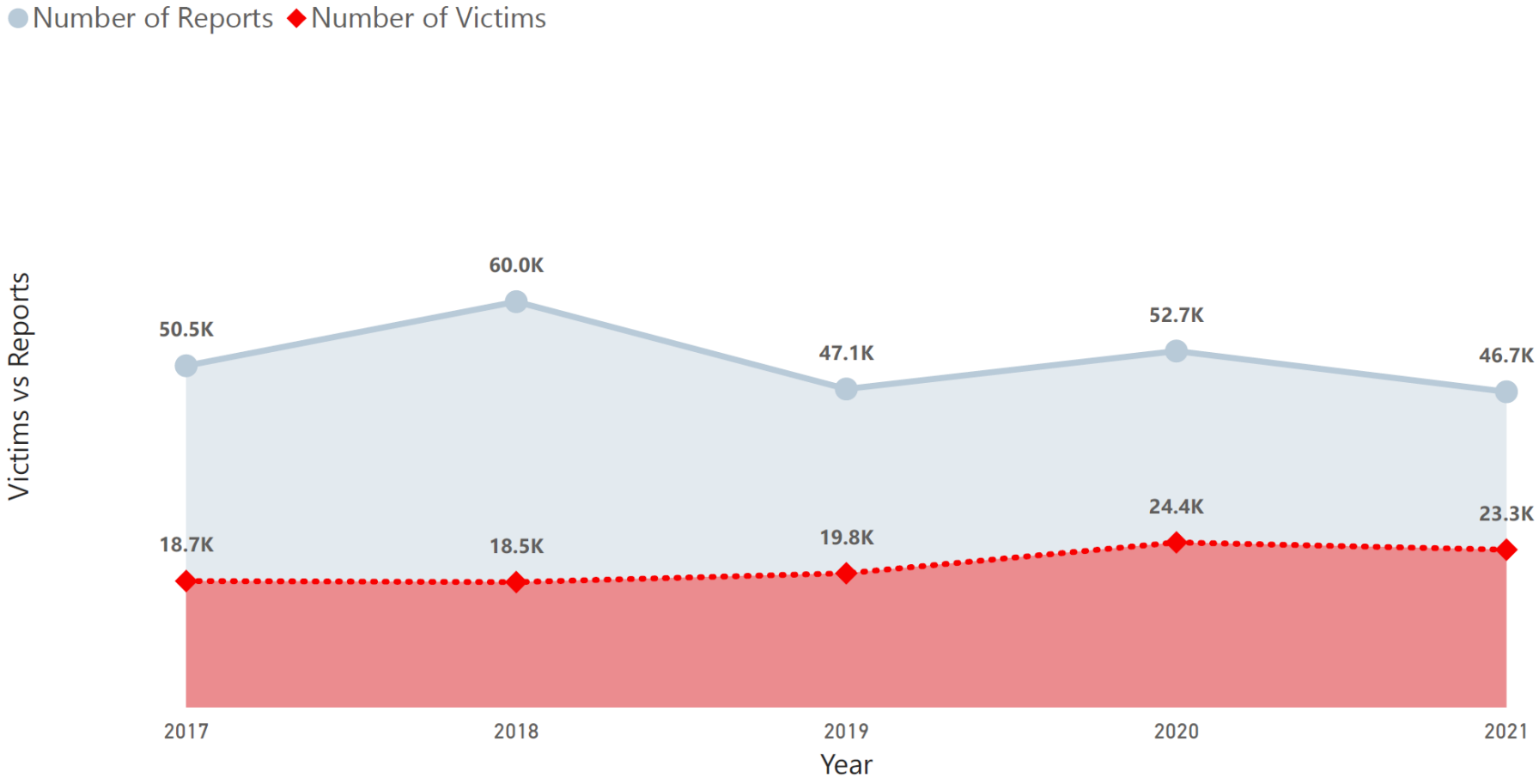
Number of Reports and Percentage of Total Reports Leading to Victimization by Solicitation Method



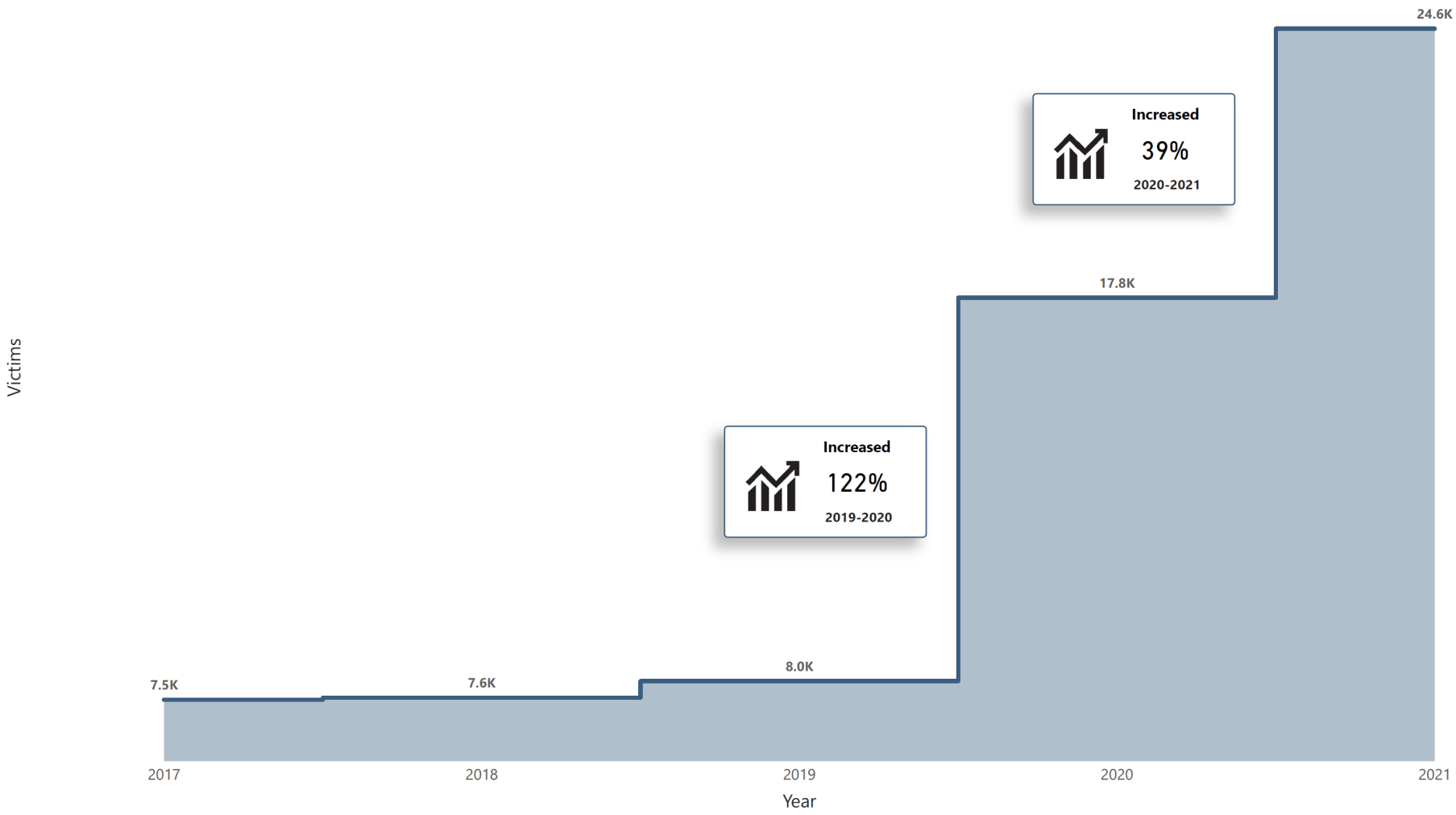
Senior (60+) - Top 10 Fraud Categories

Fraud Type	# of Reports	% of Grand Total - Report	# of Victims	% Victimized	Dollar Loss	Average dollar lost per victimization
Extortion	2,483	19.2%	391	15.7%	$4,483,419	$11,467
Service	1,525	11.8%	1,051	68.9%	$4,854,146	$4,619
Personal Info	1,519	11.7%	878	57.8%	$0	$0
Phishing	1,389	10.7%	356	25.6%	$0	$0
Bank Investigator	858	6.6%	339	39.5%	$2,486,670	$7,335
Prize	580	4.5%	165	28.4%	$2,459,919	$14,909
Emergency (Jail, Accident, Hospital, Help)	573	4.4%	181	31.6%	$1,884,010	$10,409
Merchandise	492	3.8%	401	81.5%	$940,708	$2,346
Investments	487	3.8%	449	92.2%	$38,040,646	$84,723
Vendor Fraud	431	3.3%	180	41.8%	$1,017,044	$5,650
Total	**10,337**	**79.9%**	**4,391**	**42.5%**	**$56,166,561**	**$12,791**

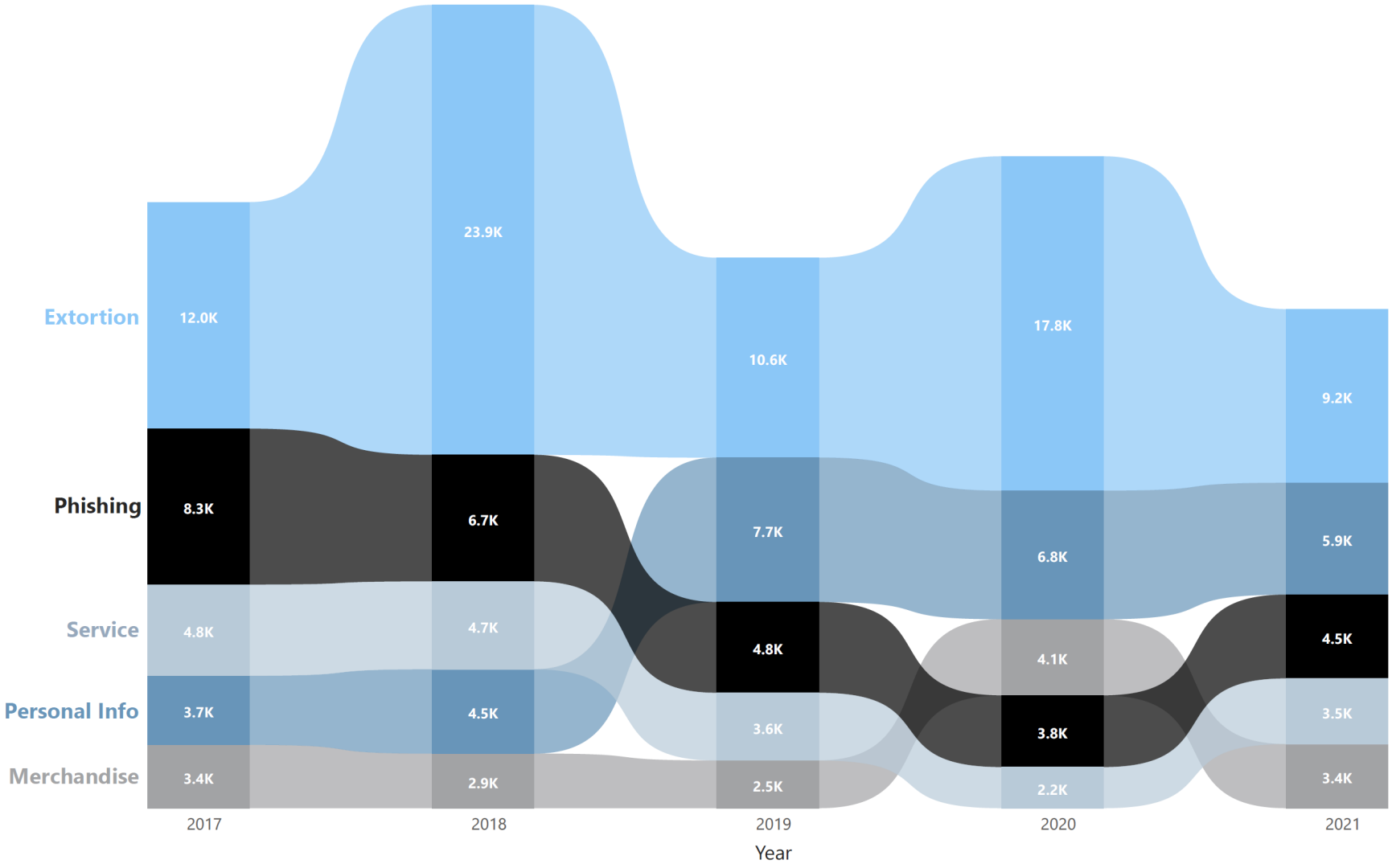
Number of Reports and Victims by Year



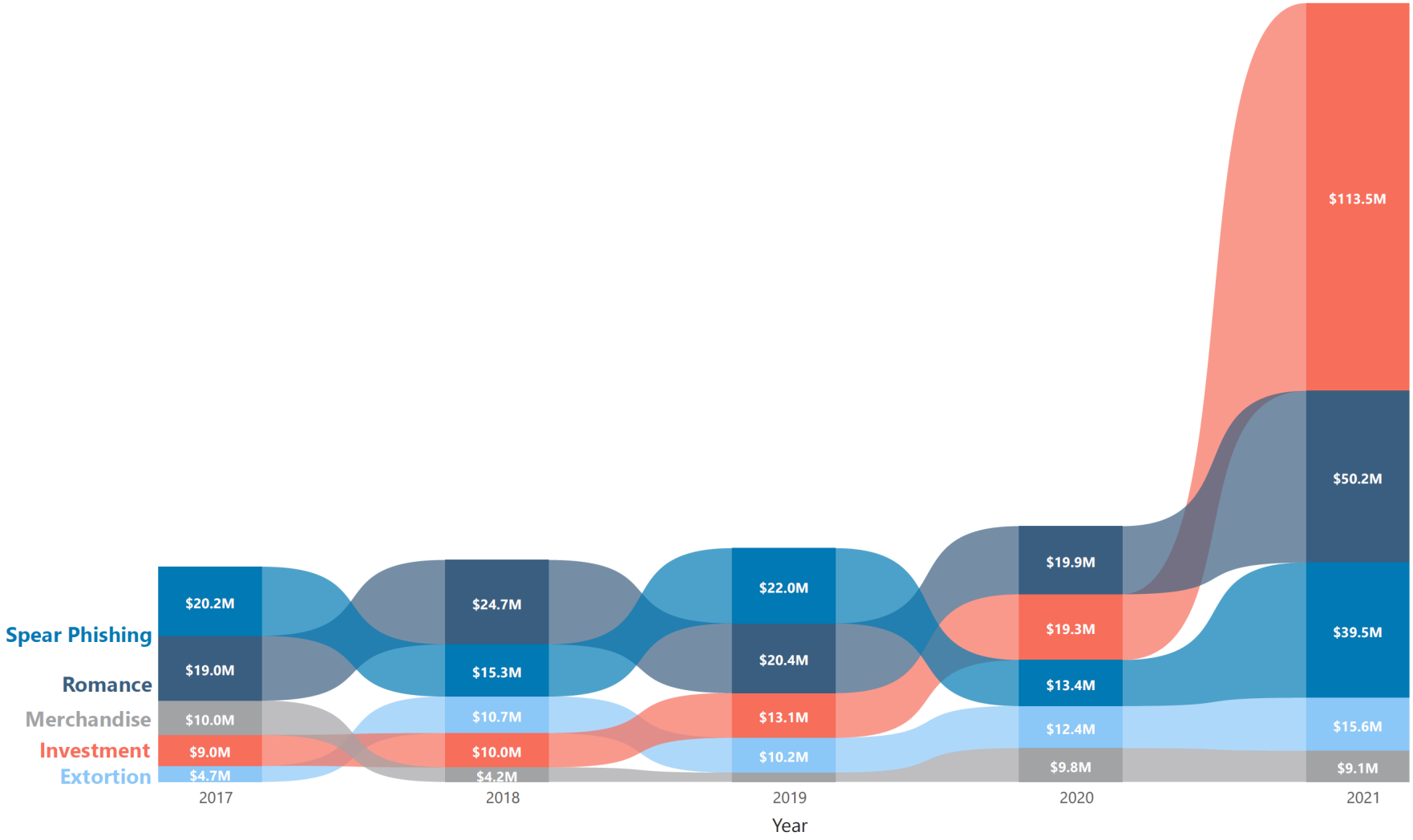
Number of Non-Senior ID Fraud Victims by Year (Less than 60 Years Old)



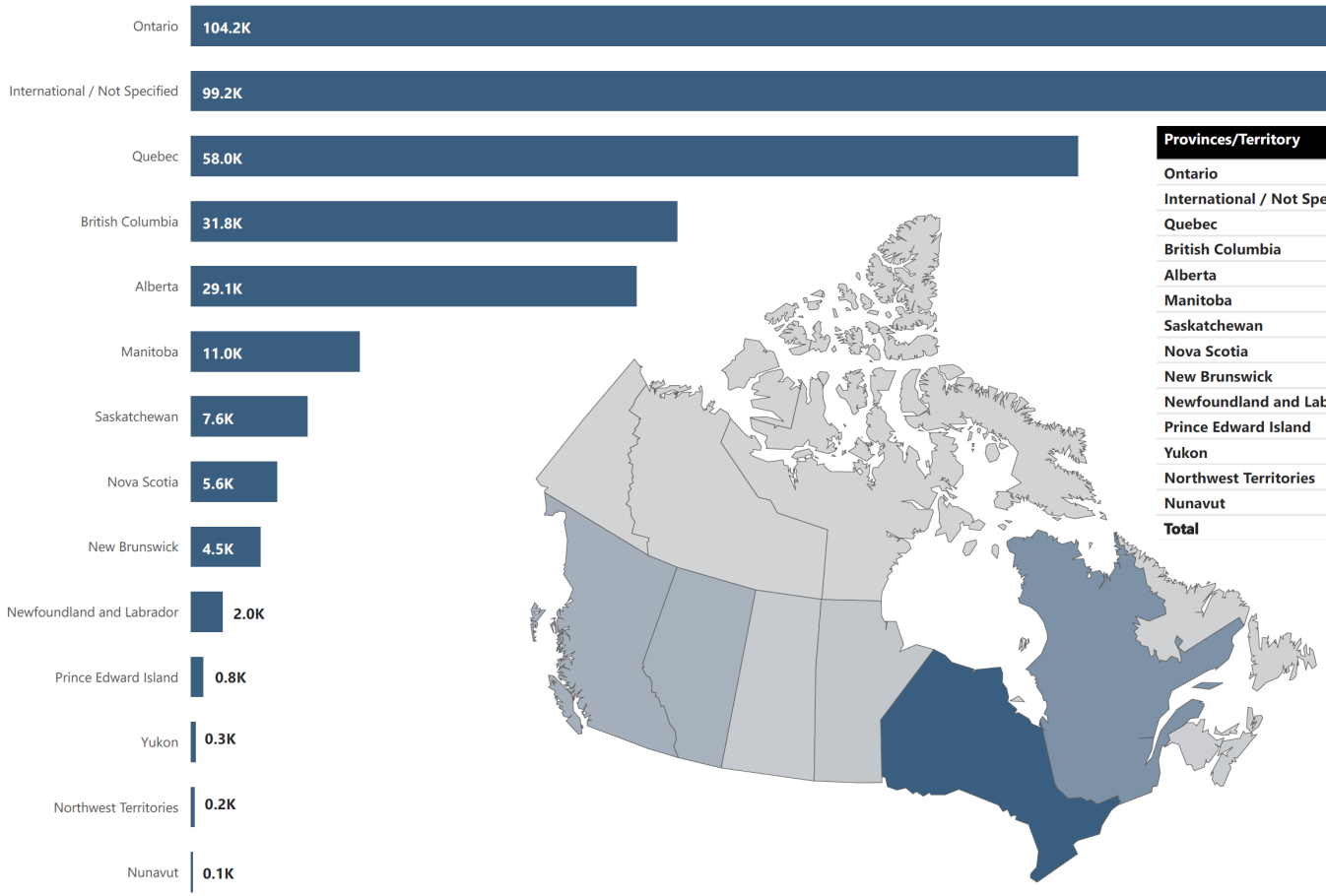
Top 5 - Number of Reports by Year and Fraud Type



Top 5 - Dollar Loss by Year and Fraud Type

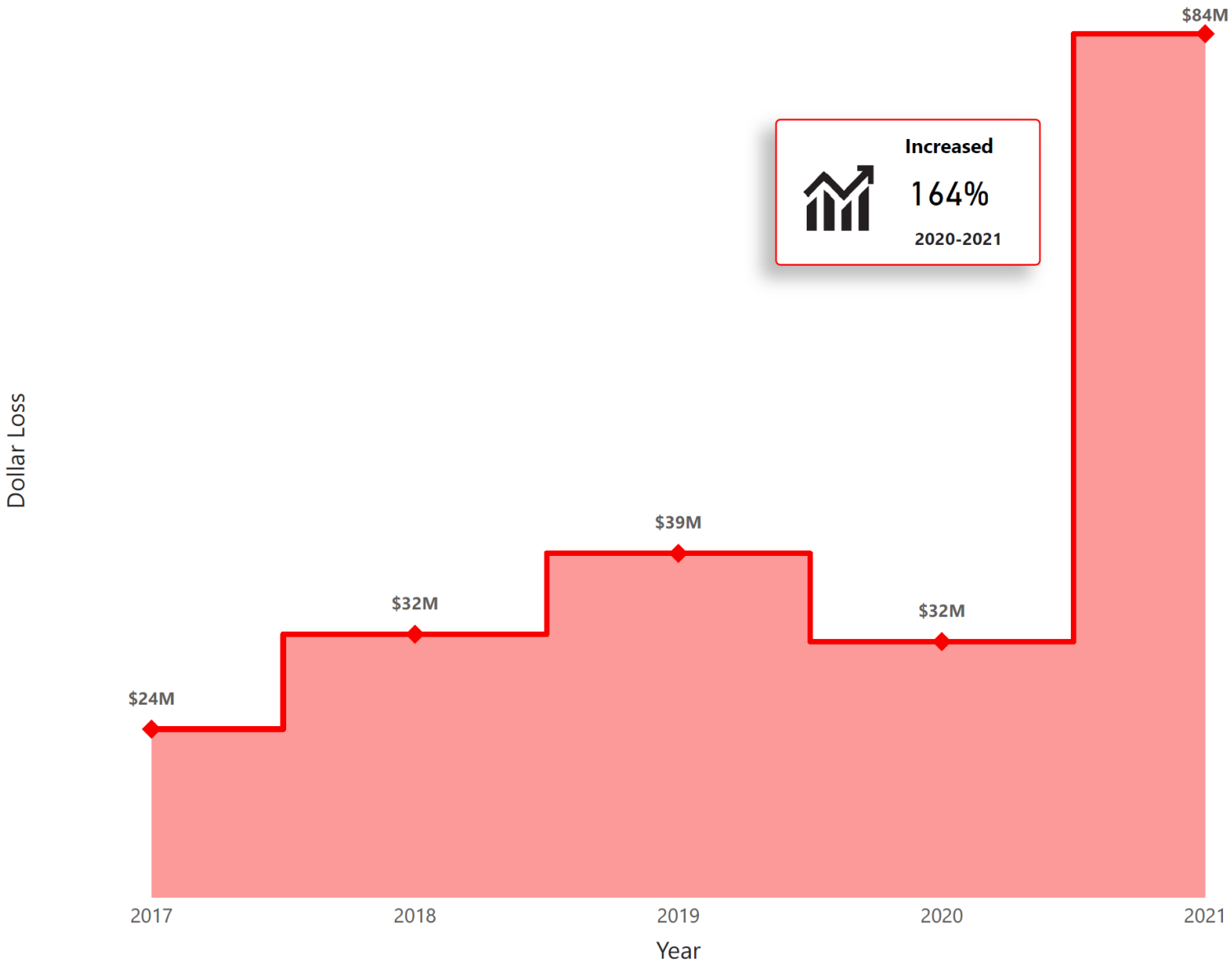


Number of Reports by Province/Territory/International

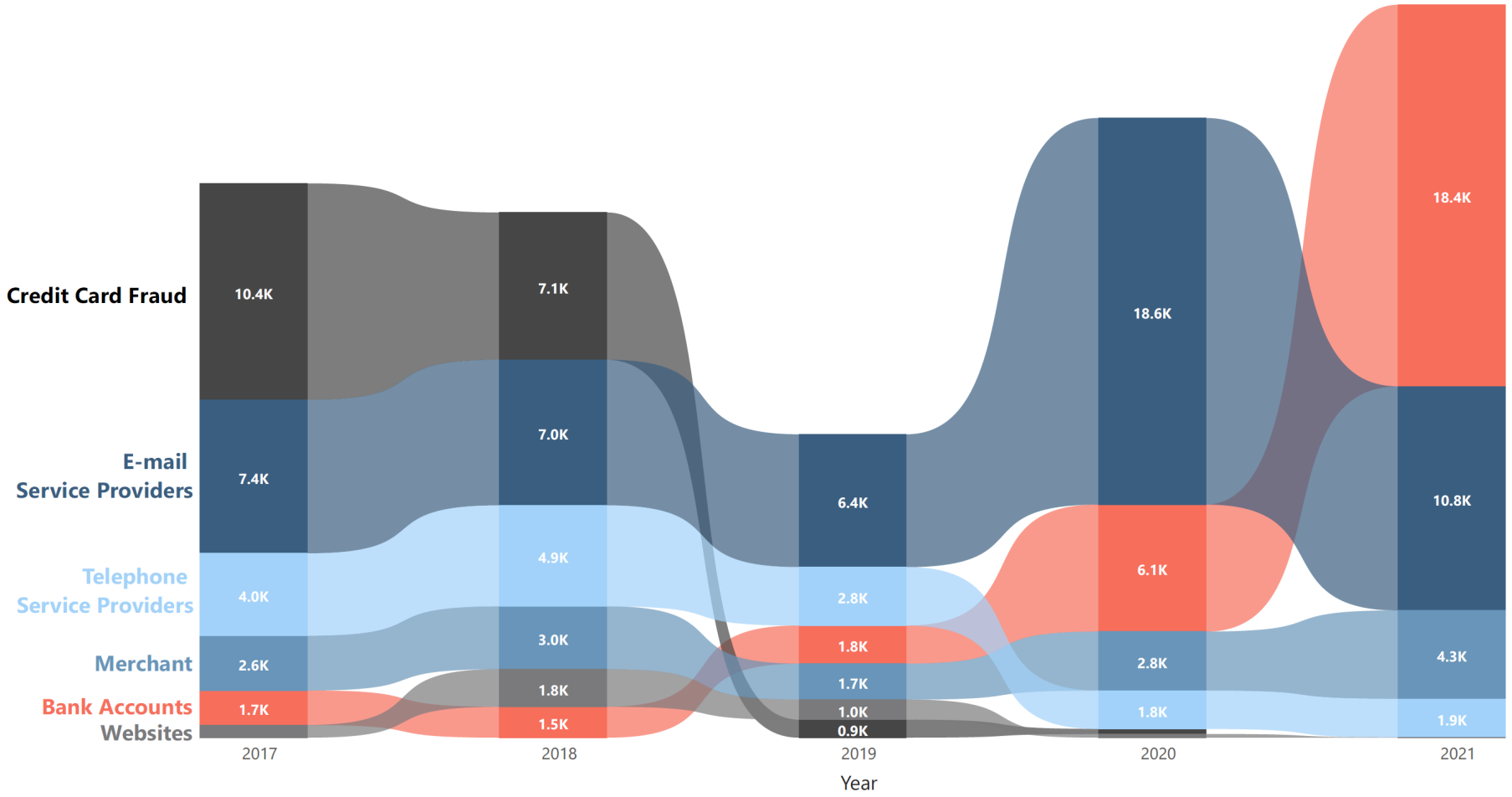


Provinces/Territory	2017	2018	2019	2020	2021	Total
Ontario	21,400	24,233	19,114	20,362	19,084	**104,193**
International / Not Specified	11,750	14,445	11,681	34,405	26,919	**99,200**
Quebec	9,967	13,229	11,659	12,687	10,479	**58,021**
British Columbia	6,188	7,490	5,294	6,705	6,135	**31,812**
Alberta	5,871	7,074	5,277	5,675	5,234	**29,131**
Manitoba	2,179	2,714	1,937	2,279	1,900	**11,009**
Saskatchewan	1,462	1,730	1,370	1,941	1,123	**7,626**
Nova Scotia	1,175	1,204	969	1,251	1,039	**5,638**
New Brunswick	999	992	775	886	876	**4,528**
Newfoundland and Labrador	491	494	318	380	374	**2,057**
Prince Edward Island	161	197	119	165	152	**794**
Yukon	63	63	59	57	63	**305**
Northwest Territories	33	36	43	49	43	**204**
Nunavut	20	23	15	25	25	**108**
Total	**61,759**	**73,924**	**58,630**	**86,867**	**73,446**	**354,626**

Senior (60+) - Dollar Loss by Year



Disruption Initiatives - Number of Reports by Year and Fraud Type



Within mandate and when possible, the CAFC prevents fraud by disrupting fraud attempts. The CAFC works with industry partners and law enforcement to prevent and disrupt fraud.


Username
xxxxxxxx
Password