Fraud Trends Targeting Seniors

Fraud: Recognize, Reject, Report.

Royal Canadian Mounted Police | Gendarmerie royale du Canada
Competition Bureau Canada | Bureau de la concurrence Canada
Ontario Provincial Police
Canada

What is the Canadian Anti-Fraud Centre (CAFC)?

Competition Bureau Canada

Bureau de la concurrence Canada

Primarily focuses on **fraud and technology-as-instrument fraud and cybercrime**, such as fraud, identity crimes, romance scams, Business Email Compromise, advance fee fraud and spear-phishing / phishing.

Primarily focuses on **technology-as-target cybercrime**, such as ransomware, malware-based cybercrime, data breaches and other cyber intrusions.

CAFC - Primary Goals

PREVENTION through education and awareness
DISRUPTION of criminal activities
INTELLIGENCE dissemination
SUPPORT to law enforcement
PARTNERSHIPS between the private and public sectors

Victim Demographics

- Mass Marketing Frauds (MMF) impacts all regions of Canada, correlates to population densities.
- Victims span all education and socioeconomic levels and are evenly distributed amongst males and females.
- **Seniors tend to lose more money on average (33%).**
- CAFC is seeing an increase of victims under the age of 60.

74% of reports with losses are from cyber facilitated frauds.

(2021 / 2022 / 2023) Reported Fraud Losses

As of December 31, 2021, the CAFC received reports totaling **$386 million CAD** in reported losses.

As of December 31, 2022, the CAFC has received reports totaling **$531 million CAD** in reported losses.

As of December 31, 2023, the CAFC has received reports totaling **$572 million CAD** in reported losses.

It is estimated that less than 5-10% of fraud victims report their occurrences to the CAFC.

Trends: Top 10 Fraud Reports 2022 VS 2023

Fraud Type	2022 Reports	Fraud Type	2023 Reports
Phishing	**10,603**	**Identity Fraud**	**11,228**
Extortion	**8,240**	**Service**	**6,729**
Personal Info	**8,083**	**Personal Info**	**6,150**
Service	**6,255**	**Phishing**	**5,850**
Investments	**4,631**	**Investment**	**4,010**
Bank Investigator	4,189	Bank Investigator	3,608
Counterfeit Merchandise	3,960	Merchandise	3,471
Merchandise	3,935	Extortion	3,150
Vendor Fraud	3,141	Job	2,692
Job	2,520	Counterfeit Merchandise	2,692

Fraud Trends: Top 10 Frauds (by dollar loss) 2022 VS 2023

Fraud Type	2022 Dollar Loss	Fraud Type	2023 Dollar Loss
Investments	**$308 M**	**Investments**	**$309.1 M**
Romance	**$59 M**	**Spear Phishing**	**$58.2 M**
Spear Phishing	**$53.7 M**	**Romance**	**$50.3 M**
Service	**$20 M**	**Job**	**$27.7 M**
Extortion	**$19 M**	**Service**	**$22.2 M**
Emergency - Grandparent	$9.4 M	Extortion	$12.2 M
Merchandise	$8.7 M	Emergency - Grandparent	$11.3 M
Job	$7 M	Merchandise	$10.6 M
Bank Investigator	$6.6 M	Bank Investigator	$10.3 M
Bank Investigator	$4.5 M	Recovery Pitch	$6.7 M

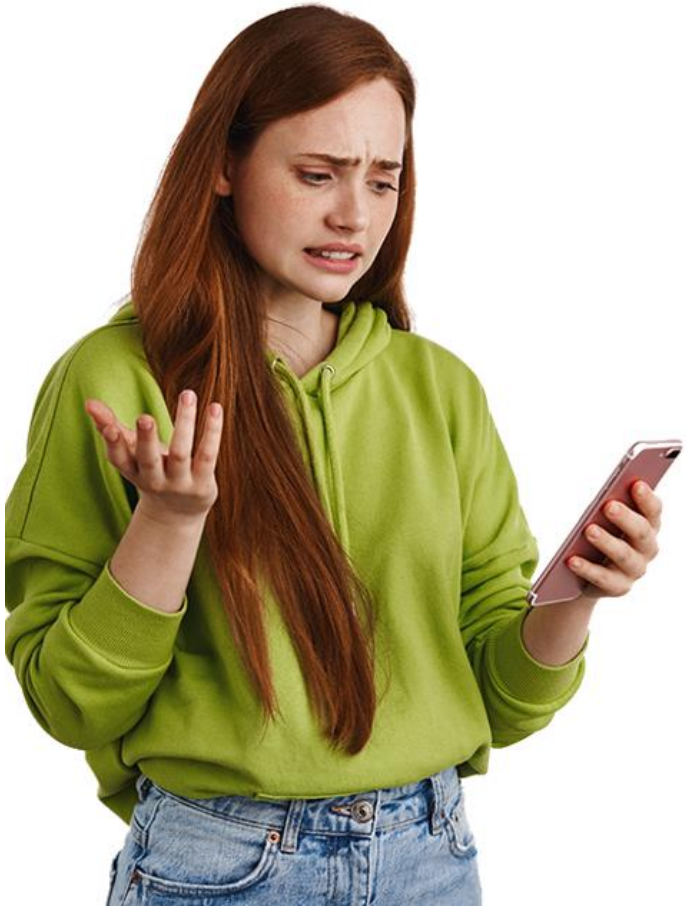
How are victims sending money?

1. Wire Transfer **$169.7** Million (Overseas – Investments / Romance)
2. Other/Unknown **$163** Million (reports with no payments details)
3. Cryptocurrency **$145.6** Million (Investment / Romance)
4. E-transfer **$27.4** Million (Classified / Money Mules / Job / Loan)
5. Direct Deposit **$13.6** Million (Business Email Compromise)
6. Cheque / Money Order / Bank Draft **$12.2** Million
7. Cash **$8.6** Million (Grandparent / Prize/ Lottery)
8. Pre-Paid **$5** Million (Extortion / Grandparent / Romance)
9. Credit Card **$3.5** Million (Card-Not-Present / Crypto)
10. Internet Payment Services (ex. PayPal) **$2.1**

Phishing includes deceptive emails or text messages, claiming to be from a legitimate organization, asking you to click on a link or download an attachment. Don’t do it! These could be malicious attempts at stealing your money or information.

Fraud Initiated By Telephone Call

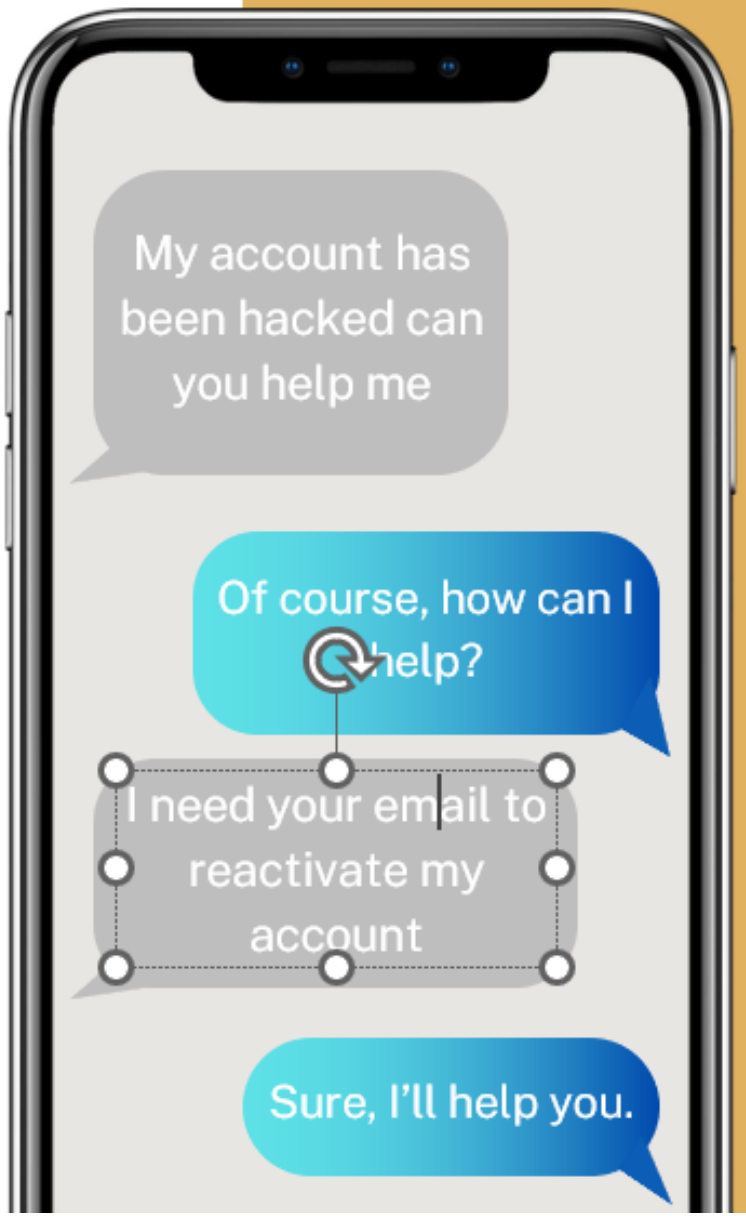
- Automatic Dialing
- Robocalls
- Spoofing
- Delayed Disconnect



Fraud Initiated Email or Text Message

- Spoofing
- Automation
- Email Compromise

Fraud Initiated Email on Social Networks



- Fake Accounts
- Social Media Bots
- Compromised Accounts
- Advertisements

Fraud Initiated Online

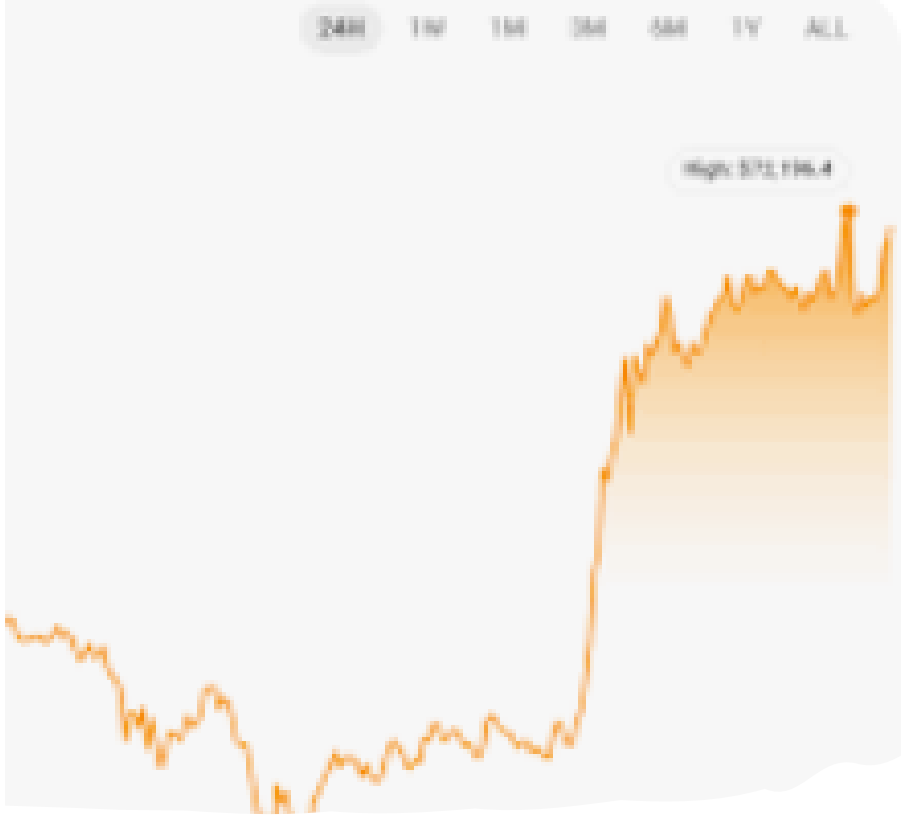
- Fake Information
- Stolen Credit Cards
- Fake Websites
- Search Engine Optimization
- Pop - Ups
- Online Classified (Market Place / Kijiji)

Online shopping scams

- Do your research before making a purchase.
- Know the market value of the item you're buying.
- Independently confirm the buyer's name, address and telephone number.
- Look for reviews, but remember that some can be fake!
- Use a payment mechanism that offers fraud protection (i.e. credit card).

Fraud Initiated By Mail or In Person

- Foreign Money Offers
- Stamps
- Employees
- High Pressure Sales



Investment Frauds (Crypto)

Investment Frauds (Crypto)

Investment frauds represented **$309** million in losses reported to the Canadian Anti-Fraud Centre in 2023, and **$308** million in reported losses as of December 31, 2022.

Investment Frauds (Crypto)

- Most of the investment scam reports the CAFC received in 2023, involve Canadians deciding to invest in cryptocurrency ***after seeing a deceptive advertisement on social media***.
- Victims downloading a trading platform and transferring cryptocurrency into their trading account.
- In most cases, victims are not able to withdraw their funds.
- Many of these of the trading platforms are fraudulent or controlled by fraudsters.
- In addition to crypto trading scams, the CAFC also receives reports on suspected fraudulent Initial Coin Offerings.

Warning Signs – How to protect yourself

- Once the transaction is completed, it is unlikely to be reversed.
- Be wary of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.
- Do research to ensure they are using reputable and compliant services.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project
- Some fraudsters will use the name of legitimate companies to lend credibility to the fraud and convince victims to send money. Verify email addresses, URL's, phone numbers and their physical address.

Warning Signs – How to protect yourself

- Verify if the investment companies are registered with your Provincial Securities Regulator or the National Registration Search Tool (www.aretheyregistered.ca).
- If you receive a suspicious or odd investment related message from a trusted friend, reach out to them through a different means of communication to confirm that it is them.
- Beware of fraudsters asking you to open and fund new crypto accounts, they will direct you to send it to wallets they control - Don’t!

Crypto kiosk company Bitcoin Depot plans to hit “thousands” of locations, with 700 units already installed.

By Danny Nelson · Jul 22, 2021 at 5:56 p.m. EDT · Updated Aug 24, 2021 at 3:08 p.m. EDT ·

Cryptocurrencies – Increased popularity

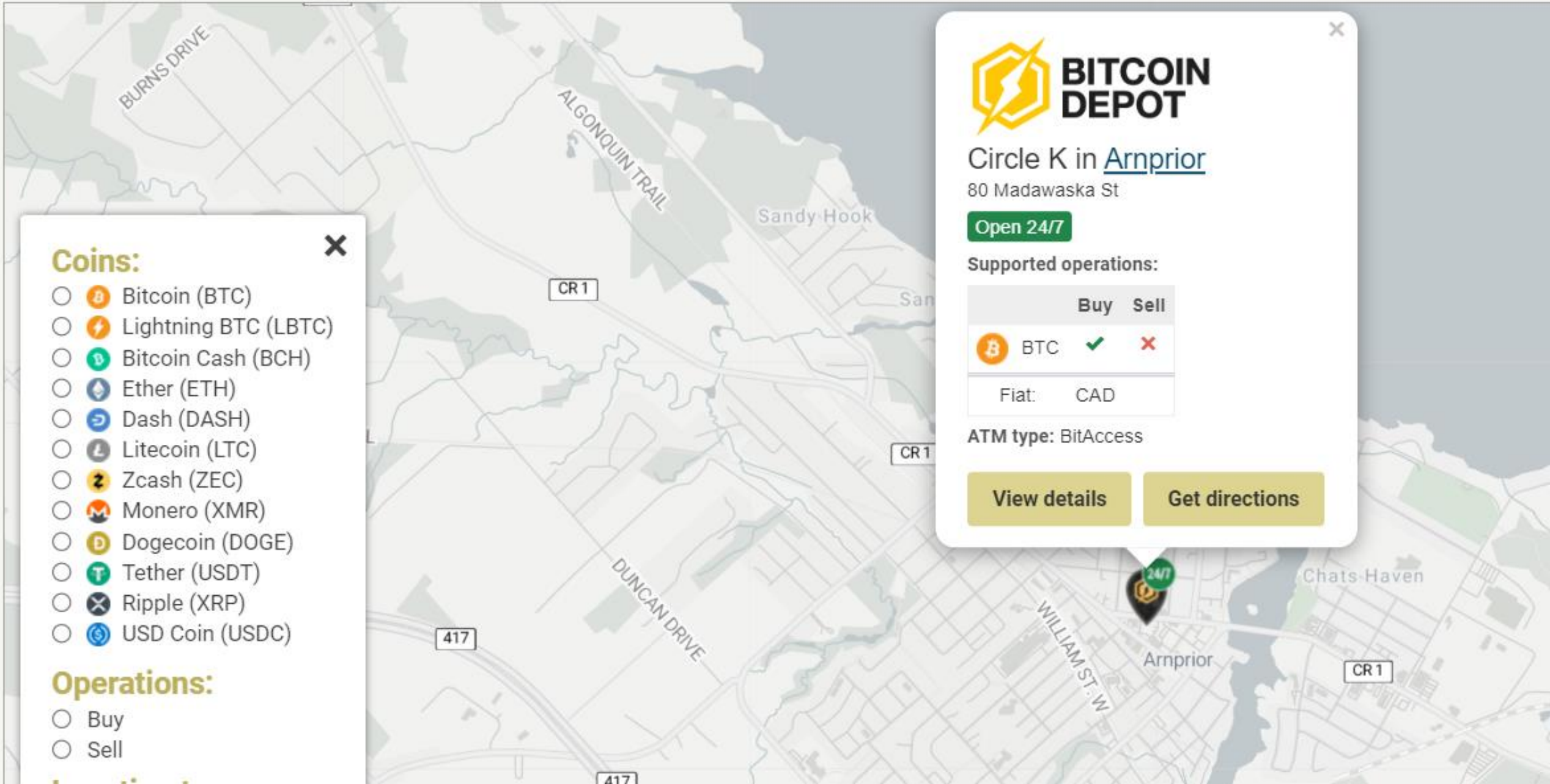
United States – With more than **17,000** machines dispersed around the nation, the United States boasts the most Bitcoin ATMs worldwide.

Canada – Canada is second with over **4,000** Bitcoin ATMs. **The nation has supported cryptocurrencies, and in recent years, the number of ATMs has steadily increased.**

Cryptocurrencies

- Becoming a popular victim remittance amongst fraudsters with funds moving overseas.
- Bitcoin ATM / ABM (https://coinatmradar.com) are increasing in populated areas.
- QR Codes or Letter / Number Combo are easily provided to fraudsters via screen shots sent via text / email.

Total number of Bitcoin ATMs / Tellers in and around Ottawa: 137



The cash-to-crypto industry enables users to buy crypto for cash at physical locations across the globe. the most well-known subset of the cash-to-crypto industry are 'Cryptocurrency ATMs' or 'BTMs'.

https://www.youtube.com/watch?v=MtTQyPUAv3Q

Romance Fraud

Canadian romance fraud victims reported losing over **$50.3** million to fraudsters in 2023.

Fraudster use technology to convince victims to enter into a virtual or online relationship, to gain a victims' trust and affection, through e-mail messages, popular encrypted chat applications, online chat groups, fake profiles on social media, dating sites or even through online platforms.

Romance Fraud

Fraudsters will send random text messages to victims. The messages often read “where are you?”, “where have you been?” or something similar. Once the victim responds, a conversation is started, and the fraudster attempts to build a relationship with the victim.

Scammer asks for money for travel, a medical emergency or assistance with a family emergency or convince the victim to invest into a fraudulent cryptocurrency platform, turning victims into money mules.

Romance Fraud

CBC LISTEN Live Radio On Demand CBC Podcasts CBC Music Playlists Toronto Sign In

Love, Janessa

Play All 6 episodes

How to Subscribe

Share Podcast

Behind every catfish, there's the bait. Who is Janessa Brazil? Stolen images of an adult entertainment star are being used to con victims out of thousands of dollars, breaking hearts in the process. Journalist Hannah Ajala embarks on a quest to find Janessa, in this 7-part true crime series. And who is responsible for catfishing scams? Produced for the BBC World Service and CBC Podcasts by Antica Productions and Telltale Industries.

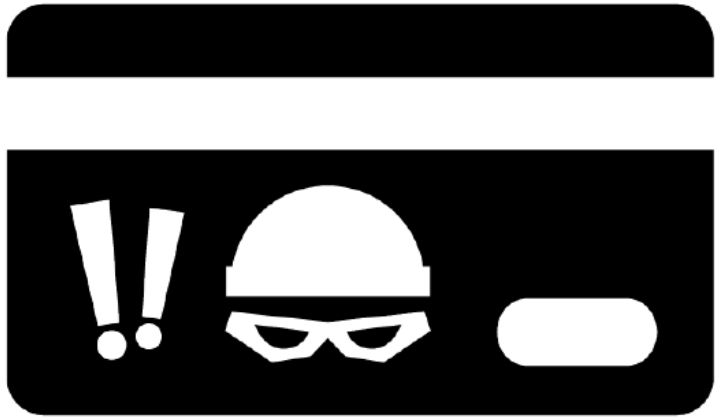
Updated: Feb. 20, 2023

[Love, Janessa | CBC Podcasts | CBC Listen]

Service Frauds

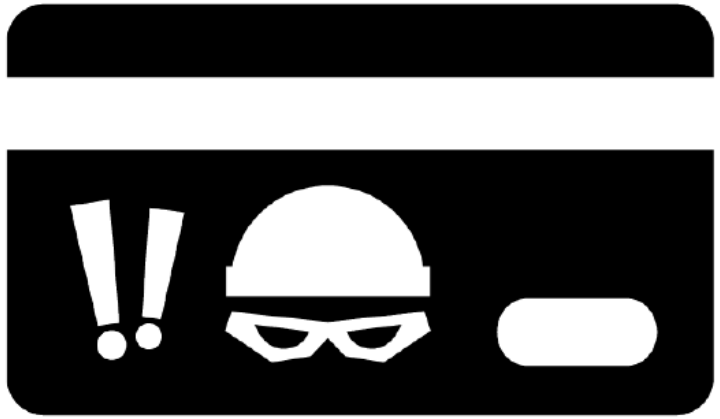
Canadian service fraud victims reported losing over **$10.1** million to fraudsters in 2023.

Tech support: Fraudsters will call victims, appear in pop-ups which seem to freeze your computer, send you an email with a fake invoice or will appear in your online search results for ‘reputable service providers’ providing a phone number for victims to call. Once in contact with victims, fraudsters will request remote access to their computer. If remote access is gained, victims put themselves at risk for identity fraud. Fraudsters may also ask for a payment for their “services”.



Service Frauds

Home Services: Air duct cleaning, furnace repairs, general contractors and more! Victims are approached on social media, telephone or come across a fraudulent ad online. Fraudsters will often ask for a prepayment and won't provide the service. If the company provides the service, they could be low quality, offer invalid warranties or the repairs can cause potential risks.



Service Frauds

Am I responsible for any payment received?

Yes!

Never accept a cheque for more than your selling price.

Never cash a cheque as part of a prize to pay taxes or administration fees.

Never accept payments from someone you have never met in person.

Why?

Because you may be used to launder money or the payment may have been fraudulent and when they ask you to send the overpayment back to them, you lose that money.

Emergency - Grandparent Frauds

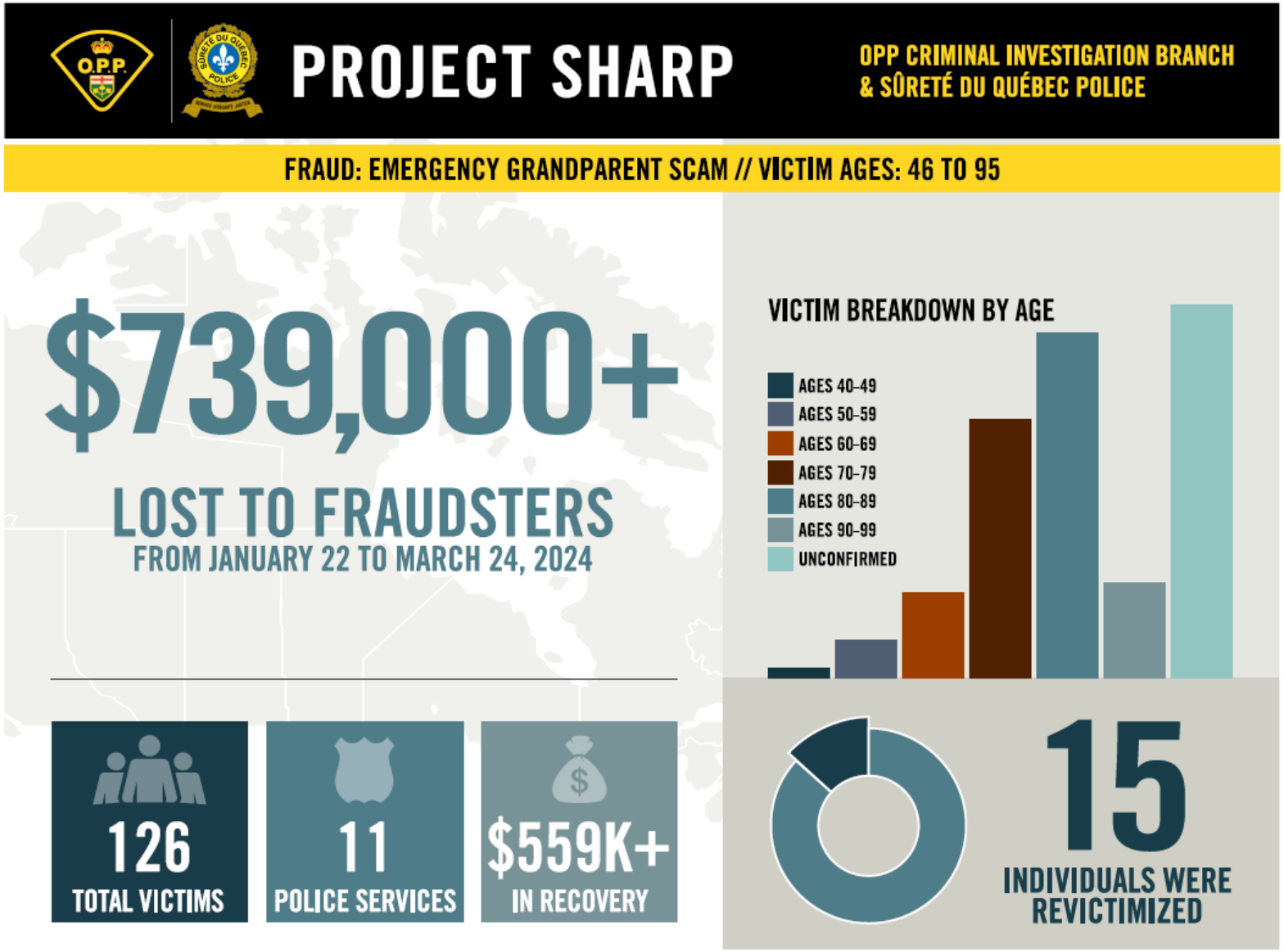
Emergency - Grandparent Frauds

Canadian Emergency – Grandparent fraud victims reported losing over **$11.3** million to fraudsters in 2023, versus **$9.2** million in reported losses in 2022.

Suspects contacts seniors with landlines, to pretending to be family members claiming that their grandchild or family member was involved in an accident, charged with an offence such as an impaired driving, and / or drug offences.

Suspects will claim that they are law enforcement officials, lawyers and even impersonate the grandchild / family member. Fraudsters will proceed to advise the victim that a payment for supposed bail or fine is required immediately in order for the family member to avoid going to jail or face court proceedings. If the victim agrees to pay the requested amount, suspects will arrange to pick up the funds in person or will ask the victim to send cash in the mail.

Emergency - Grandparent Frauds



EMERGENCY-GRANDPARENT SCAM

Fraudsters are targeting seniors by calling and pretending to be a family member in distress, the police or a justice official claiming that a loved one or grandchild is in trouble, and needs money immediately. **Victims are told there's a gag order, and can't speak to anyone.**

PROTECT YOURSELF

Fraudsters...

Call demanding immediate payment for bail, or fines to avoid going to jail

Remember! The courts won't ask for cash to bail out someone in custody, and will require people to be present in court.

Claim to be a lawyer, police or family member in an emergency situation demanding funds

Be suspicious of calls that require immediate action. **Hang up!** Call your local police and contact the family member directly.

Request cash and send couriers for pick up, or demand the victim to send cash by courier services or via cryptocurrency

Never send cash, cryptocurrencies or any other funds to unknown persons, unverified addresses or bank accounts.

If you believe you have been scammed, contact your local police and the **Canadian Anti-Fraud Centre**:

1 (888) 495-8501 / antifraudcentre.ca

Recognize. Reject. Report.

PROJECT SHARP

OPP CRIMINAL INVESTIGATION BRANCH & SÛRETÉ DU QUÉBEC POLICE

FRAUD: EMERGENCY GRANDPARENT SCAM // VICTIM AGES: 46 TO 95

126 NUMBER OF VICTIMS FROM JANUARY 22 TO MARCH 24, 2024

PARTNER AGENCIES

Bank Investigator Frauds

Canadian Emergency – Bank Investigator fraud victims reported losing over **$4.5** million to fraudsters in 2023.

Fraudsters claiming to be from their financial institution, law enforcement or one of their online merchants. Suspects claim that there have been suspicious charges on your credit card or in your online account. They claim the charge is either from an online purchase, in store transaction or overseas transfer. They then state they need your credit card information to cancel the tra

Bank Investigator Frauds

Many reports indicate that scammers will gain access to the victims' computer to continue the "investigation". Victims are then shown a fraudulent transaction on their online banking account. The scammers state they want the victims' help in an ongoing "investigation" against the criminals who stole their money.

The alleged bank investigator and/or law enforcement official indicates they will send victims a deposit of funds, for the victims to send overseas as part of the "investigation". It is not until the transfers are completed that the victims realize funds were never deposited into their account.

We encourage victims / businesses to contact their local police services and to the CAFC: **Online Fraud Reporting System** www.antifraudcentre.ca **or 1-888-495-8501 (Toll Free)**

Prevention and Awareness

To receive CAFC bulletins, statistics and trends, simply email us to be added to our distribution list: partners@antifraudcentre.ca

Prevention and Awareness

X – (Formerly Twitter) - @canantifraud

Meta (Facebook) – Canadian Anti-Fraud Centre

Website - www.antifraudcentre.ca

March is our annual Fraud Prevention Month (FPM)

Browse scams

> **Note**
>
> These lists are intended as navigational aides, and not as comprehensive or official lists of all scams affecting Canadians.

Scams by A-Z index

Alphabetical list of scams

Scams by medium

Browse scams by delivery method

Scams affecting businesses

Find out what scams target businesses

Scams affecting individuals

Find out what scams target individuals

Identity theft and fraud

Learn more about identity theft and fraud


QUESTIONS?