

A Guide to Protect Yourself Against Investment Fraud

FAIR Canada is the only national, non-profit, independent investor advocate in Canada. We are a trusted voice that provides informed, objective comment on significant issues that have an impact on investor fairness and protection.

Inside This Guide

Introduction	2
What is Fraud?	3
How is Fraud Changing?	5
Why Do Investors Continue to Fall for Fraud?	7
Tips on How to Spot a Scam	9
What Can You Do to Protect Yourself?	10
It's Important to Report Fraud	12
Investor Resources	12

Introduction

Today's investment landscape offers such a range of products, investing tools, and information that the average investor may feel overwhelmed. As advancements in technology continue to accelerate, new online investing platforms and opportunities are showing no signs of slowing down any time soon.

And as the world of investing continues to innovate, so do the tactics of fraudsters when designing and carrying out scams against unsuspecting victims.

In this guide, we discuss investment fraud and some key things you should know before investing, including helpful tips to protect yourself from investment scams.

Learning Outcome

After reading the guide, you'll be able to:

- Identify some common types of fraud.
- Gain insights on how fraud is evolving.
- Understand some reasons why investors fall for fraud.
- Identify signs to spot a scam.
- Find out how to protect yourself.
- Know how to report fraud.

What is Fraud?

While fraud takes many forms and shapes, it often involves victims losing their hard-earned savings with little chance of ever getting it back.

A fraud basically occurs when someone tries to take your money away from you through deceit or an unlawful act. Most fraudsters can be extremely convincing. Some frauds focus on getting small amounts from as many different victims as possible before moving on. Other frauds work by building trust and asking victims to contribute increasingly larger amounts of money over time.

While fraud takes many forms and shapes, it often involves victims losing their hard-earned savings with little chance of ever getting it back. As such, it is important to be cautious and look out for potential fraudsters. In particular, you should be alert when a stranger approaches you with a “great, new investment opportunity.”

Have no doubt, fraud is an increasing concern for Canadian investors and regulators, as fraud-related losses continue to rise. According to the Canadian Anti-Fraud Centre (CAFC), Canadians lost more than \$379 million in 2021 due to fraud, an increase of 130% since 2020.¹

In addition, investment scams topped the CAFC’s list of fraud types in 2021, with almost \$164 million in reported losses, compared to just \$17 million in 2020. These numbers are just the tip of the iceberg, since most fraud goes unreported—the CAFC estimates that fewer than 5% of victims ever file a fraud report.

This increase in the amount of investment fraud is not surprising, given that more and more Canadians are looking for investment opportunities. In fact, in the past few years, there has been a surge in the number of Canadians that have become investors. The increase in investing is partly driven by technology advances, which have made it easier for Canadians to participate in the capital markets.

As the number of people interested in investing goes up, so does the number of potential targets for fraudsters. As we’ll discuss further, they are also taking advantage of the latest technology and insights into human behaviour to manipulate us and find potential victims.

Did you know?
Investment scams topped the list of fraud in 2021, with almost \$164 million in reported losses.

Types of Fraud

Fraudsters are continually finding new ways to defraud honest people. While one fraud may involve stealing your ID and passwords to gain access to your bank account, another fraud may prey on your desire as an investor to make higher returns.

Highlighted below are some of the more common investment frauds:

Crypto Scams: These scams can involve fraudsters using clone websites to get investors to purchase and transfer crypto assets to fake accounts. In some cases, victims are tricked into giving fraudsters remote access to their computers to carry out the scam.

Fraudsters may also try to make you believe they have created a new type of cryptocurrency that promises to generate huge returns for investors. There are also cases of investors opening accounts with crypto exchanges that are not registered in Canada, which may not properly protect your assets and could turn out to be a scam operating from a foreign country.

Ponzi Schemes: Victims are offered investments with guaranteed high returns, but they are paid with funds received from other investors, rather than from real profits. With no legitimate earnings, Ponzi schemes require a constant flow of money from new investors to survive.

When it becomes hard to recruit more investors, or when large numbers of existing investors cash out, these schemes collapse, leaving those still invested in the scheme with nothing. Ponzi schemes can go on for months or years and are often hard to detect until it is too late.

Pyramid Schemes: Similar to Ponzi schemes, except investors are rewarded for bringing new investors into the scheme. In other words, you may unintentionally contribute to victimizing other investors by encouraging them to invest as well.

Pump and Dump: This usually involves a low-priced penny stock that is heavily promoted or “pumped” by the perpetrators to get investors interested in buying the stock. As more investors get involved, pushing up the stock price, the perpetrators will suddenly sell or “dump” their own stocks in the company. After the dump, you’re left with significant losses in your investment.

Romance Fraud: Scammers use social media and online dating apps to manipulate victims into virtual relationships. Once trust is established, the scammer uses the illusion of a romantic or close relationship to request money for an investment opportunity. Sometimes they convince you to continue investing, leading to larger losses.

Advance-Fee Scams: Investors are persuaded to pay money upfront to take advantage of an investment promising high returns. The scammer disappears with the advanced money, and you are left with nothing.

Did you know?

Scammers may use social media and online dating apps to manipulate victims into virtual relationships.



How is Fraud Changing?

Most types of investment fraud we described, other than perhaps crypto scams, have existed in one form or another for a long time. The core elements of a Ponzi scheme, for example, haven't changed since they were first widely reported in the 1920s, when Charles Ponzi lured victims into investing in a scam involving postage stamps.²

What has changed is the information and digital tools available to fraudsters to target their next victim and exploit human tendencies and impulses to their advantage. We explore some of these changes and the impact they have on investors.

New Technology Brings New Opportunities – Good and Bad

Information technology has dramatically changed the way we connect with each other. More Canadians are interacting online or through social media. The COVID-19 pandemic accelerated the demand for online customer experiences that provide fast and easy interactions. There is also an ever-increasing amount of our personal information available to anyone who has an Internet connection.

It's not only the younger generations who are comfortable using online applications—everyone is getting used to banking apps, mobile payment solutions, and are trusting technology to input personal data on their devices.

While technology brings a lot of welcomed and positive changes to our lives, fraudsters can also use it to exploit investors.

Most investors today rely on their smart phones to communicate through email or text messages and social media apps. They post information about their personal lives and get news from their favourite online sources, such as Facebook or Reddit. Anyone can contact you at any time from anywhere, by simply connecting to an online network.

These are all wonderful developments that have improved our ability to stay connected with the world. While technology brings a lot of welcomed and positive changes to our lives, fraudsters can also use it to exploit investors. Our increased comfort level and the readily available personal information about us, unfortunately, also makes it easier for fraudsters to build trust with their targeted victim—a key ingredient to help ensure a scam succeeds.

Here's how fraudsters are exploiting the new digital world:

More Information on Potential Victims: There is a lot more information about potential victims freely available to fraudsters over the Internet. Every time you post something on Facebook, click a like button, or retweet a post, you may be giving fraudsters information they can use to target you. Fraudsters may also try to trick you into giving them personal information, or hack your computer or cell phone to steal details about you for their next scam. The more they learn about you, the more convincing they sound when contacting you about “an awesome investment opportunity”.

Easier to Appear Legitimate: It is easier and less expensive for them to appear legitimate. Before using websites and email messages, fraudsters would sometimes rent office space to appear legitimate, or need to operate call centres in the hopes of finding enough victims to achieve their financial schemes.

Today, it's relatively easy to create fake websites that look legitimate, or email messages that can be sent to thousands of potential targets with a click of a button. Fraudsters can also hide their identities using private messages, or create fake accounts and business addresses.

Little Experience Required: Fraudsters with limited technical knowledge can take advantage of easily accessible tools to exploit their targets through fake email messages and websites.

For example, they can download ready-made phishing kits.

These generally include the software utilities needed to create and send phony email or text messages that are designed to trick you into revealing personal or sensitive information. They can also use “exploit kits” to hijack a legitimate website by redirecting you to a website created by the fraudster.

Did you know?

Many fraudsters live outside of Canada, but can still target Canadian victims online or by telephone.

Less Personal Interactions and More Anonymity

Another factor influencing today's investment fraud is what well-known ex-con artist Frank Abagnale refers to as the dehumanizing process. In the past, perpetrators needed to meet their targets in person to establish a personal connection. Nowadays, technology enables scammers to target numerous people online without ever meeting them. Abagnale, who was portrayed by Leonardo DiCaprio in the 2002 movie *Catch Me If You Can*, explained that this anonymity dehumanizes the process and today's scammers “will take you for everything you have, without any compassion whatsoever.”³

Fraudsters Can Operate From Anywhere

While we may know of people in our communities that have been victimized by fraud, not all fraudsters necessarily live in our communities. Many fraudsters live outside of Canada, but can still target Canadian victims online or by telephone.

This makes it very difficult to identify, investigate, and bring them to justice. In many cases, there is little hope of ever recovering your money, which could already have been spent, or hidden in an offshore account halfway around the world.

Why Do Investors Continue to Fall for Fraud?



Understanding why people fall for fraud is no easy task, with many factors potentially at play.

One thing is certain: if a scam is executed well enough, anyone can become a victim. It is also true that no two fraud victims are exactly alike—every individual is influenced by their own personal motivations, inclinations, and behavioural tendencies.

To protect yourself against fraud, it is important to understand how fraudsters manipulate people. Research indicates that there are some common characteristics and

psychological factors that can make an individual more susceptible to investment fraud.⁴

A key tactic of fraudsters involves putting pressure on their target to invest now before it's too late. This takes advantage of investors who may have a fear of missing out or FOMO.

The following are some of the more common reasons why people become victims of fraud:

Fear of Missing Out (FOMO)

A key tactic of fraudsters involves putting pressure on their target to invest now before it's too late. This takes advantage of investors who may have a fear of missing out or FOMO. According to research by the British Columbia Securities Commission (BCSC), FOMO is especially intense among young adults, with 40% of Canadians between the ages of 18 and 34 reporting that they have experienced FOMO.⁵

Investor Overconfidence

When making investment decisions, overconfidence can hinder your ability to assess risk and make you more susceptible to scams. Some behavioural examples of investor overconfidence include:

Over Ranking: Believing your level of understanding or skill is better than it actually is.

Illusion of Control: Believing you have power or control over a situation when in fact you do not.

Wishful Thinking: Convincing yourself it is “a great investment” without evidence to support that belief.

Not Recognizing the Red Flags

The inability to identify fraud red flags, such as an offer of guaranteed high returns, leaves investors much more vulnerable to potential investment fraud. Perhaps investors may not understand what a reasonable rate of return would be for the product being offered. Or perhaps their desire to make a greater-than-average return on their investment blinds them from seeing the red flag.

We provide a list of red flags to look out for in the following section titled, *Tips on How to Spot a Scam*. Identifying red flags is closely connected with understanding the techniques used by fraudsters when trying to persuade their targets.

Persuasion Techniques

Fraudsters apply many different persuasion techniques to influence emotions that can affect an investor’s judgment and financial decision-making.

Some key persuasion techniques include:

Credible Sources: To add credibility to the scheme, fraudsters may try to associate themselves with experts, influencers, or other respected figures to promote their scams. Appearing to be credible is important because it helps to influence people’s behaviours and thoughts.

Phantom Riches: Fraudsters will dangle the prospect of guaranteed profits, or entice you with something you want but can’t have.

Scarcity: This involves telling you this is a rare or the last opportunity to invest. An example is where the investment offer has an expiration date or involves an exclusive investment opportunity.

Reciprocity: The fraudster gives you a free coupon/gift and then asks you to sign up for an investment, taking advantage of your desire to show appreciation for their gift.

Similarity: Many of us tend to like and trust people who are similar to us. If someone just like us has done well with an investment, we may be more likely to follow their lead. As a result, fraudsters often try to find out personal information about their target; for example, where they grew up, went to school, or where they work. Then they pretend to share some experiences in common based on that information.

Did you know?
Fraudsters apply persuasion techniques to influence emotions that can affect an investor’s judgment and financial decision-making.

Tips on How to Spot a Scam



You can be proactive by looking out for these red flags:

This investment is guaranteed to have returns with no risk: There is no such thing as no investment risk. This tactic targets investors who are not risk takers, but who need to earn income through their investments. Remember, all investments come with risks and, usually, the higher the returns, the greater the risks.

You need to get in before this opportunity disappears: If it's a legitimate opportunity, it will be available tomorrow. This tactic creates a false sense of pressure or urgency and preys on investors' fear of missing out. Do not feel pressured into making a quick decision; take time to discuss it with someone else. After all, it's your money and you should not part with it unless you feel comfortable with your decision.

Beware of promoters who tell you they have an exclusive offer that is only being offered to select people like you.

This is a tax-free investment opportunity located overseas: This tactic is used to target people who may believe they pay too much tax or oppose government spending. All legitimate investments, however, require some tax reporting to authorities. While you can defer paying taxes, you can't avoid paying them at some point.

You get a phone call or email message out of the blue: Receiving a call or email message from a stranger offering you an "amazing investment opportunity" is a big red flag. So is a phone call from a stranger asking you to provide them with personal information about where you bank or invest.

Hot tip, or exclusive offer: Everyone wants to get the inside scoop of the next big opportunity. Fraudsters often take advantage of this by telling you they have a hot tip about "a fabulous investment opportunity," or they have an exclusive offer that is only being offered to select people like you. When you get this type of sales pitch, take time to think "why me" or "who else are they pitching this to"?

Everyone is buying it: Watch out for pitches that stress how "everyone is investing in this now, so you should, too." They are trying to prey on your fear of missing out.

Unusual payment mechanisms: Sometimes, fraudsters will insist that you pay using an alternative method, such as an unfamiliar payment app, with a gift card, or with cryptocurrency. This tactic is used to help them hide the money from authorities, making it harder to ever get it back.

Not responding to your questions: If the person contacting you tries to avoid answering your questions through distraction or refusals, chances are they are hiding the truth from you. If you're dealing with a legitimate investment opportunity, they will want to answer all your questions because they have nothing to hide.

What Can You Do to Protect Yourself?

When thinking about fraud, an ounce of prevention is worth a pound of cure.

There are times we get so busy in our daily lives that we may let our guard down and become too trusting, especially with someone who appears to be a nice person trying to help us. Unfortunately, we sometimes spend more time planning our next holiday or researching a new vehicle purchase, than we do on investment decisions that affect our financial wellbeing.



You can reduce your chances of fraud and potential losses by making a conscious effort to do your homework to learn more about the salesperson, firm and/or investments before you invest.

You are more likely to become a victim of fraud if you don't take the time to fully understand the investment product.

Use the following tips to help protect yourself from investment scams:

Check Who You Are Dealing With Before You Invest

- People who offer you investment opportunities or advice need to be registered with securities regulators in Canada. You can easily check their registration at [CSA National Registration Check](#). It only takes a minute and can save you a lot of hardship.
- You can also quickly check the [Disciplined List](#) for details of any disciplinary action taken by a regulator against the individual or firm that has contacted you.
- Another good source to check is the [Investor Alerts](#) issued by regulators concerning scams.
- You may also want to check out [Cease Trade Orders](#) for decisions by Canadian securities regulators against a company or an individual.
- Research the profile of the person you are dealing with using online searches to see if the person's image, name, or details have been used elsewhere.

Don't Invest in What You Don't Understand

- You are more likely to become a victim of fraud if you don't fully understand the investment product.
- Ask questions to be sure you fully understand what you are being sold, including who is offering you the investment.

Be Careful When Investing in the Next Big Thing

- In January 2022, the North American Securities Administrators Association ranked crypto investments at the top of its annual list of investor threats for the year.
- To be proactive against crypto scams, check for [investor alerts](#) issued by securities regulators.

Never send money to a stranger you have only communicated with online or by telephone.

Don't Rush Into Investing

- If someone is pressuring you into an investment opportunity, refuse to make a rushed decision. Genuine investment professionals will give you time to think about any recommended investment opportunity.

Do Not Feel You Have to Respond to, or Talk to Strangers

- Do not act on an unsolicited offer to buy any investment product. Keep your personal financial details private and do not share account numbers, usernames, logins, passwords, or personal identification numbers with anyone.
- Never send money to a stranger you have only communicated with online or by telephone.

Be Careful Relying on Social Media

- More and more investors use information from the Internet and social media to help make investment decisions. For example, Reddit is a social-based website that's commonly used for investment advice, including subreddit community groups with millions of members. TikTok is another social platform investors visit for information.
- It's risky relying on these social platforms because anyone can post information and the content is rarely checked by platform operators. Be sure to follow the tips we previously mentioned in the section titled, *Check Who You Are Dealing With Before You Invest*.

Ask Questions

- Ask about costs, risks and what's in it for the salesperson. Verify information with a trusted advisor.
- Before investing, consult with those around you to verify the legitimacy of the offer. This strategy is helpful because it gathers collective knowledge about scams and persuasion tactics from friends, family, neighbours, and whoever else is present at the time of the offer.

And remember, if it sounds too good to be true, it probably is.



It's Important to Report Fraud

Many victims are embarrassed to report fraud, as it's not easy to admit being victimized by a scam. But reporting fraud is important as it will help the authorities to catch the perpetrators and protect other potential victims. If you suspect fraud or if you are a victim of fraud, you should:

- Report the incident to your [local securities regulator](#) and law enforcement agency.
- Report the incident to the [Canadian Anti-Fraud Centre](#).
- If you're being lured into a fraudulent investment through social media, report the scam website to the social media platform.
- If you become aware of a fraudulent website, report it to the host of the legitimate website.
- File a report with the [Competition Bureau](#).

Investor Resources

There are many resources available to help you with investment decisions:

[FAIRCanada.ca](#): Learn about starting your investment journey and how to protect yourself from scams.

[GetSmarterAboutMoney.ca](#): Receive helpful information about investing and fraud from the Ontario Securities Commission.

[InvestRight.ca](#): Take a free course on recognizing, reporting, and rejecting investment fraud from the British Columbia Securities Commission.

Sources:

1 [Top 10 frauds targeting Canadians in 2020 \(antifraudcentre-centreantifraude.ca\)](#), and [Top 10 frauds in 2021 \(antifraudcentre-centreantifraude.ca\)](#), Canadian Anti-Fraud Centre.

2 Ponzi Scheme: https://en.wikipedia.org/wiki/Ponzi_scheme.

3 [The Real 'Catch Me If You Can' Con Artist Says Every Scam Involves These Red Flags](#), CNBC.com, 2019.

4 [Understanding and Combating Investment Fraud](#), Christine N. Kieffer and Gary R. Mottola, The Wharton School, University of Pennsylvania, 2016; Regulators in the U.S., led by the Financial Industry Regulatory Authority (FINRA), also looked at why consumers become victims of financial fraud: [Exposed to Scams: Can Challenging Consumers' Beliefs Protect Them From Fraud?](#), 2021.

5 [Younger, FOMO-Inclined Adults View Social Media As Source For Investment Tips](#), British Columbia Securities Commission, 2021.

To learn more about FAIR Canada, our advocacy for investor rights, and helpful resources for investors, please visit [FAIRCanada.ca](#). Follow us on [LinkedIn](#) and [Twitter](#).