

lautorite.qc.ca



Red-flagging financial fraud

**Protect yourself against
financial scams**



**AUTORITÉ
DES MARCHÉS
FINANCIERS**



WHO ARE WE?

The *Autorité des marchés financiers* (AMF) is the body mandated by the Québec government to regulate Québec's financial sector and assist consumers of financial products and services. The AMF is an integrated regulator, ensuring oversight of, in particular, the insurance, securities, derivatives and mortgage brokerage sectors, deposit institutions (other than banks) and the distribution of financial products and services.

NOTICE

The AMF and its management and staff are not responsible for the consequences of any errors contained in this document. This guide is intended for information purposes only. It does not offer any advice on the purchase or use of specific financial products and services. The published texts have no legal value.

The information in this publication is current as at April 2022.

This document is available on the AMF's website.

Legal deposit – Bibliothèque et Archives nationales du Québec, 2019
978-2-550-85738-9 (PDF)

In Québec, **1 person in 11** think they've been approached with a fraudulent investment opportunity.¹ Would you be able to detect fraud?

The first section of this guide sets out five steps to help you avoid financial fraud. The second section presents the main types of financial fraud. By familiarizing yourself with them, you can reduce the risk of fraud and avoid a lot of problems.

Table of Contents

Step 1	4
Step 2	5
Step 3	7
Step 4	8
Step 5	9
1. Phishing	10
2. Ponzi schemes	13
3. Pyramid investment schemes	14
4. Fraudulent on-line trading platforms	15
5. Fraud using an initial cryptocurrency offering (ICO)	17
6. Tax havens	18
7. Pump and dump	19
8. Trash and cash	19
9. Recovery scam.....	20
10. RRSP fraud or RRSP borrowing schemes	21
11. Telemarketing investment schemes.....	23
12. Affinity groups.....	24
13. A friend or family member in distress	24
14. Insurance fraud.....	25

1 Source: Canadian Securities Administrators (CSA). 2017 CSA Investor Index

Step 1

When approached about an investment opportunity or insurance, check that the person or firm offering it to you is authorized to do so.

You can do this by calling the AMF Information Centre at 1-877-525-0337.

You can also check the *Register of firms and individuals authorized to practise* at www.lautorite.qc.ca.

If the person or firm offering you an investment opportunity or insurance is not authorized to do so, report them to the AMF.

Don't be swayed by a mere business card or diploma on the wall.

DID YOU KNOW?

1/25

Proportion of respondents to the 2017 CSA Index survey who believed that they had been victims of financial fraud.

Step 2

Before you invest, insist on being given documents explaining the investment. Make sure you read and understand them.

The documents should include such information as:

- › The type of investment (stock, bond, etc.)
- › The risks associated with the investment
- › Whether and under what conditions you will be able to access your funds if you need them
- › The related fees

A fraudster may give you fake disclosure documents. Check whether the documents received are available on the SEDAR website at www.sedar.com. This site contains information required by members of the Canadian Securities Administrators (CSA), which includes the AMF. If you're not provided with written, reliable information, it's best not to invest.

Make sure the account and transaction statements you receive for your investments come from the institution where your money is invested, not just your representative. The institution should also be listed in the AMF *Register of firms and individuals authorized to practise*.



Step 2 (continued)

If you want to take out insurance, you may not receive the contract prior to purchase. However, insist on having the key points in the contract (policy) explained to you, including the coverage provided, cost of the insurance and exclusions.

As soon as you receive your insurance contract, read it over to make sure it matches what you were sold and review all the terms and conditions. If you're not satisfied, let the insurer know immediately. Many insurers will let you cancel the policy free of charge within 10 days of receipt of the contract.

Never place confidential documents such as investment statements, credit card statements or income tax returns in your recycling bin. A fraudster could use the information they contain. Shred them instead.



Step 3

Make sure the investment being offered isn't too good to be true.

With very rare exception, the higher the return you expect on an investment, the higher the risk you have to be willing to take on. This is a rule of thumb in investing.

If someone presents you with an opportunity to earn a higher return than what is offered in the market without any risk, then it's likely a scam.

If you're told an investment is guaranteed, ask yourself:

- ▶ Who is guaranteeing the investment? If it's an individual, that's a red flag. Normally, investments can be guaranteed by a financial institution or, in the case of deposits, under the AMF deposit protection plan or the Canada Deposit Insurance Corporation deposit insurance framework.
- ▶ What is guaranteed: the return, the invested amount, or both?
- ▶ Do you have to pay a fee to benefit from the guarantee?
- ▶ What conditions have to be met in order to take advantage of the guarantee? Do you have to hold the investment for 5 years? 10 years? 20 years?

Likewise, if someone offers you an insurance product that sounds too good to be true, beware!

If someone promises you a high return with low risk, ask yourself questions about the investment opportunity and the person proposing it. There's no such thing as a high-return investment with no risk. If there were, everyone would invest in it. And don't be fooled by statements like "quantities are limited" or "the opportunity is only being offered to a lucky few".

Step 4

Beware if you hear statements like:

- › “I have it from a reliable source that this investment will skyrocket. It’s a sure bet.”
- › I invested all my money in it, and my parents’ money, too.”
- › “If you’re not satisfied, I’ll reimburse you.”

Statements like these are often used by scammers to reassure their targets that the investment is risk-free and suitable for everyone. In fact, they provide no guarantees.

- › “You’re part of a select club. You’re one of a handful of people to be given the privilege of taking advantage of this incredible offer.”
- › “Very few people know this, but the company is about to be bought and its value will double.”
- › “The company will soon be publicly listed.”
- › “The government is going to grant them a patent.”

Statements like these are designed to make you believe the scammer possesses privileged information when, in reality, the information is fake.

Beware of illegal insider trading!

Insider trading is illegal if it consists of buying or selling securities using information that is not available to the public. The disclosure of privileged information is also illegal and is called “tipping”. Privileged information is information that, if made public, could influence the price of a share traded on an exchange.

- › “It’s imperative that you invest today: tomorrow will be too late.”
- › “There’s a loophole in the law that can help us avoid paying taxes. But you have to keep it secret, even from your family or the law might be amended.”

Fraudsters don’t want to give you time to think or consult with your friends, your family or an organization like the AMF.

- › “The AMF has approved the investment.”

The AMF does not approve investments: it authorizes individuals and firms to offer investments or insurance.

Step 5

Don't invest with or buy insurance from someone who exhibits the following behaviours:

- › Too often finds similarities between your situation and his or her own.
- › Brags excessively about their skills and accomplishments.
- › Tries to make you feel guilty if you decline the investment or question some statements.
- › Refuses to say which firm he or she works for or tries to change the subject after providing only scant information.
- › Contacts you repeatedly.
- › Pressures you to invest in the proposed offering.
- › Asks you to invest by giving him or her a cheque made out in his or her name or cash.
- › Doesn't ask you questions to determine your investor profile.

WARNING!

Although the above behaviours do not necessarily mask a fraud attempt, they may lead to fraud. Be extra careful if you encounter them!

APPEARANCES ARE SOMETIMES DECEIVING!

Beware of people who offer you investments while flaunting their supposed wealth or pretending to know influential people. Before you do anything, carry out the appropriate checks, both on them and the firms they represent, with the AMF.

HERE ARE 14 OF THE MOST COMMON TYPES OF FINANCIAL FRAUD AND SOME TIPS TO AVOID THEM.

1. Phishing

Phishing is a fraud technique in which the scammers make their victims believe they are dealing with a trusted entity like a financial institution or government in order to steal personal information and money.

Example: You receive an unsolicited e-mail or text message from a company you do business with in which you're asked to immediately update your personal information.

Scammers are always inventing new ways to get their hands on your money and may use a number of reasons to get what they want. For example:

- ▶ "The company has been a victim of fraud."
- ▶ "Unusual transactions have been detected in your account."
- ▶ "A new law requires the institution to request that you update your personal information."

If you click on a link in the e-mail or text message in order to fill out a form, you may see a replica of your institution's website. Any information you enter on this FAKE website would go directly into the fraudsters' database. The crooks would then be able to empty your account, steal your identity and cause you a lot of problems for years to come.



To avoid this type of fraud:

- ▶ If you feel you must reply to a message asking for personal information, use the contact information you have in your records. Above all else, don't use any contact information, click on any hyperlinks or open any attachments contained in the e-mail or text message. NEVER click on a link appearing in an unsolicited e-mail or text message asking you for banking or personal information.
- ▶ Don't be intimidated by an e-mail or text message warning you about the disastrous consequences that may result from not following the instructions it contains.
- ▶ Immediately report the phishing attempt to the institution or organization concerned by calling the phone number listed on its website, not the one indicated in the e-mail.
- ▶ Type in the complete web address yourself for the site you want to visit.



Phishing also targets businesses.

Phishing is a truly global problem and targets both individuals and businesses.

In the case of businesses, the scammers may pass themselves off as the CEO of the targeted firm, then send an e-mail to an actual employee and attempt to convince the person to take certain actions. For example, they may ask the employee to transfer funds from one account to another.

To lend more credibility to their e-mails, which appear to be sent from the CEO's e-mail address, the scammers may indicate that certain steps must be taken in order, for example, to comply with AMF regulations.

They may even state that the recipient of the e-mail was chosen because of his or her trustworthiness. The employee is then asked to provide banking information or transfer funds to an external person and to be discreet so as to respect the AMF's or another regulator's procedures.

To avoid being a victim of phishing and potential identity theft, never answer this type of e-mail and quickly report the situation to the AMF Information Centre. Always check the legitimacy of the request by calling the institution involved yourself.



2. Ponzi schemes

Ponzi schemes involve taking an investor's money to pay bogus returns to other investors or reimburse investors who want their money back. Fraudsters may therefore create the false impression that the investment is generating positive returns and you won't have any problem recovering your investment.

Most Ponzi schemes are uncovered after the fraudsters vanish or are no longer able to meet investment withdrawal requests. By then it's too late because the money is no longer in the accounts. Ponzi schemes may be combined with one or more other types of fraud.

Example

You put \$1,000 in an investment offered by Paul, a con artist. After only a week, you receive a \$100 cheque from Paul, who explains that the amount is the income generated by your \$1,000 investment.

Unfortunately, your \$1,000 investment did not actually generate any return. Paul used a portion of your investment to pay you \$100 in fake "profits." By doing this, he is hoping to get you to pour more money into the investment or to convince others to invest in it. Paul is also using much of the money you've paid to him on personal expenses.



3. Pyramid investment schemes

A pyramid investment scheme is a system of selling products (investments, for example) that earns money from the recruitment of new members. The product sold is merely a pretext for recruiting members.

People who use this technique won't tell you it's a pyramid scheme.

This fraud has many variations.

Example

You're offered a very promising investment that is expected to generate a high return. You have to hold the investment for a certain period of time (e.g., six months). In addition to the excellent return, you can make even more money by recruiting investors who will benefit from the same "one-of-a-kind" investment opportunity. You may, for instance, be asked to recruit two people. For each person you bring in, you'll receive a commission—usually a percentage of the amounts invested by the people you recruit. You will then pocket an additional commission for each investor who is enlisted by your recruits.

THE FRAUD

The "one-of-a-kind" investment doesn't actually exist: the fraudsters use your money to pay you your investment income and recruitment commissions (Ponzi scheme). When they sense they're about to get caught, they disappear with your money.

Be careful if someone promises you money to recruit new people, whether the fraudsters refer to them as investors, partners, associates or by some other term.

BE CAREFUL!

The people who orchestrate pyramid schemes and those who participate in them may be prosecuted.

4. Fraudulent on-line trading platforms (fake on-line brokerage sites)

You want to invest on-line and you find a promising trading site. Or fraudsters contact you to get you to invest on a trading platform where, they say, you'll earn huge profits without too much risk. They go on to tell you that you can invest as little as \$100. So you do. The next day, your \$100 investment is worth \$150. The fraudsters call you back to ask if you want to invest more.

Be careful!

- ▶ Some promoters of these types of fraudulent platforms will falsely represent themselves as individuals registered with the AMF and refer you to our *Register of firms and individuals authorized to practise* so you can check them out.
- ▶ In many cases, they offer actual financial products (e.g., currencies, crypto derivatives, shares of companies like Amazon, Google and Apple). The products offered change with current trends and tend to be ones generating the most media interest at the time. If you accept their offer, they'll pocket your money and you won't receive the financial products.
- ▶ The fraudsters post positive testimonials on review sites (e.g., user communities and blogs) and social media platforms.
- ▶ In some cases, fraudsters will offer free training touting the benefits of investing on their on-line trading site.
- ▶ In other cases, you'll be invited to try to practise trading on the trading platform provided. During the practice runs, the platform may be rigged so that you win often. This will prompt you to invest more, but the reality could be far different when you invest with real money.
- ▶ Be wary of promises that sound too good to be true such as:
 - “Become a FOREX pro in just a few days!”
 - “You can't lose.”
 - “Invest risk-free!”
 - “Make easy money working from home!”
 - “Use our foolproof software to make money!”

To avoid this type of fraud

- › Make sure the dealer is registered with the AMF by calling the person back at the phone number listed in the AMF's register (not the number the person gave you).
- › If you're asked to invest using a credit card, this should raise a red flag. You should never invest with a credit card!

For more information about this type of fraud, visit the AMF website.

Beware of currency market fraud – FOREX

Although there's nothing illegal about investing in the foreign exchange market, beware of fake transaction sites and make sure your investments suit your investor profile. Fraudsters tend to follow trends and new products so they can make them the centrepiece of their fraud schemes, which all share the same goal: to operate without authorization in order to steal your money and personal information.



5. Cryptoasset fraud

Although investing in crypto assets isn't illegal, it's a very risky activity in a sector plagued by scams. Know how to recognize scams and follow our advice to help avoid them.

- ▶ Some scammers operate by offering bogus crypto assets. They may cloak themselves in good intentions to stand out from the crowd and attract victims (as a community, humanitarian or socially responsible project, for example). The transactions **aren't recorded on a public blockchain**; they're only recorded on the scammers' network.
- ▶ Others operate **fake crypto asset trading platforms**. If, for example, you buy crypto assets on the platform, you will see your investment track upward in value in line with the scammers' false promises. However, the scammers have actually programmed the platform to make it appear as if this is the case. The amounts invested actually go straight into their pockets without your even noticing it. While the platform may be very professional-looking, what you see on screen is just an illusion.
- ▶ Scammers may begin by convincing you to purchase cryptoassets on a platform. After falsely building a relationship of trust with you, they will encourage you to **move your cryptoassets to another platform** under the guise of helping you get higher returns. The second platform is **fraudulent** and shows false results. Your cryptoassets have been stolen without any chance of being recovered by you.
- ▶ Some fraudsters might also use the funds raised through an initial coin offering (ICO) for purposes other than those indicated in the project presentation.
- ▶ Some scammers may offer to help you recover the money you lost in a crypto-asset fraud scheme. They will ask you to pay an advance fee but won't provide you with any service. In some cases, they may also ask you to share personal information that they will then use to defraud you without helping you get your money back.

To help you avoid fraud

- › Be on guard if the company that manages the platform does not have a civic address in Canada or if the person who contacts you and that you want to deal with is based outside the country.
- › Check several sources and feel free to [contact the AMF](#).
- › Offers that sound too good to be true should raise red flags. There's no such thing as high returns without risk.
- › Do not transfer your cryptoassets from one platform to another platform that is not registered with the AMF.
- › Never give your passwords or control of your computer to anyone and especially not to strangers who claim to want to help you with your investments.
- › Avoid investment offers that are made on social networks or by strangers that were not contacted by you.

6. Tax havens

Scammers may entice you with an opportunity to invest in a tax haven, meaning a jurisdiction in the world where there is little or no income tax. They may tell you that it's legal but not to let anyone else know or else the laws might be amended to close the "loophole" in the system.

Investing abroad is not illegal. However, it is illegal not to report the income or gains on those investments. A person who is willing to help you skirt the law so you pay less income tax may have no qualms about running away with your money!

Fraudsters didn't choose the tax haven at random. They chose it because it's a country where it's almost impossible for law enforcement agencies to trace the funds.



7. Pump and dump

You're led to believe when reading press releases and items on discussion forums and social media that the value of a security (usually a stock) is going to rise significantly, so you, along with many other investors, purchase the security, which pushes the price up. Now all you have to do is wait for the value of the security to increase even further, as expected. This turns out to be a big mistake. The security's value abruptly drops to virtually zero and you lose everything. What happened?

When a security is not very liquid (demand for it is relatively low), a single buyer can make the price shoot up. Conversely, a single seller can cause the security's value to plunge. The scammers owned a large quantity of the security you purchased. They bought it at a very low price and sold it to you at a high price that was reached by fraudulently generating demand. You therefore overpaid for a worthless security. As the company you invested in does not have any assets, you were left holding an investment that has no value.

To avoid this fraud, ask yourself what people are getting out of giving you "hot tips" on investments.

8. Trash and cash

This is the opposite of a pump and dump scheme. Here, the fraudsters circulate information that leads you to believe that a relatively illiquid security is likely to plunge in value and should be sold off. You, along with many other people who saw the information, sell the security, causing the price to plummet. The fraudsters then swoop in to buy it up at a low price.

9. Recovery scam

You've taken a beating on your investments. Now beware of fraudsters!

Some con artists will take advantage of the fact that you lost money on your investments by making you an offer that's hard to refuse: they'll offer to buy your investments from you for more than their actual value. For example, the stock you paid \$2 per share for is currently worth only \$0.06 per share. Someone will offer to buy them from you at \$1 per share, explaining that some people are prepared to pay more than what the shares are actually worth because they can then report capital losses and save a lot on income tax.

However, if you accept the offer, you'll have to pay a hefty transfer fee. Once you've handed over the money, the crooks will vanish and "forget" to buy your shares.

10. RRSP fraud or RRSP borrowing schemes*

You're told that you can withdraw money from your RRSP* right now without paying income tax. To do this, you'll need to transfer the funds to an investment that will earn you a huge return. You're told that this investment is also RRSP-eligible, which is why you won't pay any income tax.

The fraudsters are so confident about this investment that they'll offer to give you a cash advance against future returns. For instance, if you invest \$50,000, they could give you a \$25,000 cash advance. They explain that you're not risking anything and tell you: "In any case, if you had taken the money out of your RRSP, you would have had to pay half of it as income tax."

* A locked-in retirement account (LIRA), pension plan or other registered fund may also be used.



What are you risking with this investment?

- ▶ The investment at the “huge” rate of return never happens. Instead, your money may end up being invested in a company that’s worthless or belongs to the fraudsters. You will therefore lose your \$50,000. What’s more, contrary to what you were told, the investment is not RRSP-eligible.
- ▶ You could receive a notice from Canada Revenue Agency stating that you withdrew amounts from your RRSP and did not pay the applicable income tax. You may have to pay the applicable income tax. Paying the income tax may mean losing the \$25,000 so generously advanced by the fraudsters (which is actually your own money).

Amounts withdrawn from your RRSP, LIRA or pension fund are taxable.

This fraud has many variations. For example, some fraudsters will tell you that, in order to withdraw money from your RRSP without paying income tax, you will have to first transfer your RRSP to an “on-line broker” (discount broker). To give their scheme a veneer of credibility, the fraudsters will let you select the broker. They will then ask you for your passwords so they can access your accounts, telling you that they will manage them on your behalf. The fraudsters will then use this information to empty your accounts the first chance they get.

BE CAREFUL!

Some fraudsters ask you to sign powers of attorney supposedly so you can benefit from seemingly attractive offers. Actually, they use the powers of attorney to clean out your accounts.

11. Telemarketing investment schemes

You receive a phone call from a stranger offering you a once-in-a-lifetime investment opportunity. In addition to yielding a much higher return than any other form of investment, the person tells you the investment carries no risk.

Never let yourself be fooled into investing over the phone by a stranger making this type of unsolicited call. You could end up putting your money directly into the hands of fraudsters.

Fake voicemail messages

You have a voicemail message.

“Linda, it’s Paul. I lost your old number and Jane told me that this is your new one. I hope I got it right. Do you remember the guy who helped me with my investments? He gave my father a hot tip. The investment doubled in less than a month and, if I remember correctly, you were disappointed that I didn’t share the tip with you. Well, I have a new hot tip from my friend.

Company XYZ is about to launch a revolutionary new product. It will be announced later this week. Now’s the time to buy shares: the price will soon increase dramatically. My friend says we have to invest right away. I’m buying some tomorrow and so’s my dad. I’m on the road today, so call my cell at XXX-XXXX. Talk to you soon.”

You don’t know Paul or Linda. The caller is trying to manipulate you. If you call the number left on your voicemail, you’ll be offered a (fraudulent) investment opportunity. If you take it, you’ll lose your money.

The same message may have been left in thousands of voicemail boxes. This scam is also carried out via e-mail, text messaging and the Internet.



12. Affinity groups

Fraudsters associate with people who share the same beliefs or interests so they can identify potential victims. As with other types of fraud, they will make a subtle, then gradually more open show of their wealth and success. They will build a relationship with you and then offer you exceptional investment opportunities. Their victims may take the first steps themselves to invest and reap the promised rewards. In some case, the scammers will ask you to keep quiet because it's a golden opportunity and they only want to share it with their friends. The truth is, the only people who will profit are the fraudsters!

When a friend offers you an investment opportunity, view it through the same critical lens as if the person were a stranger. That also means checking whether the friend is authorized to sell the investment he or she is offering (see page 4).

13. A friend or family member in distress

Scammers impersonating a friend or family member will call you or write you on Facebook or another social network. They will tell you they're in need of your immediate financial assistance in order, for example, to avoid being imprisoned in horrific conditions for not paying a fine after being unjustly arrested.

Be careful! Some fraudsters will assume the identity of someone you know in order to extort money from you. If a friend or family member appears to be in a crazy situation and is seeking your financial help, get the person to provide answers to questions only the actual friend or family member would know, such as the name of a mutual friend's spouse. First and foremost, don't do anything without first verifying the person's identity and talking with friends or family members.

14. Insurance fraud

A representative of insurance company XYZ assesses your insurance needs and sells you insurance at a very competitive price. He tells you that, to activate your policy, you must pay the premium in cash or send him a cheque made out in his name. His commission will be taken out of the cheque and the difference will be transferred electronically to the insurer. You will therefore be insured that same day.

A few months later, when putting your papers in order, you realize you never received a confirmation of insurance. You try to call the representative only to learn that the number he gave you belongs to a pizzeria in a neighbouring town. You then call XYZ. You learn that the representative doesn't work for the company! In fact, he doesn't work for any insurer: he works for himself.

You gave money to a fraudster. He sells fake life, car and home insurance and pockets the premiums paid by clients. He even sells investments!



You don't hear much about this type of fraud. Victims often lose only the amount of the premium—a much smaller sum than in some investment scams. But what would happen if you were to suffer a “covered” loss? The amount could be very high.

To avoid this type of fraud:

- 】 Check that the person offering the insurance is authorized to do so by calling the AMF Information Centre. You can also search the *Register of firms and individuals authorized to practise* on the AMF website.
- 】 Call the insurer to confirm that your insurance is in force.
- 】 When paying your premium, make your payment out to the company (insurance firm or insurer) registered with the AMF. Never make a cheque payable to the person offering you the insurance.



HAS YOUR PERSONAL INFORMATION BEEN STOLEN?

Someone has stolen important personal information from you such as a password, your date of birth, your credit card number, the amount of your salary or your social insurance number (SIN)? Unfortunately, ill-intentioned people could use your personal information to commit fraud. Here are a few tips to help you avoid any problems.

If you're able to sign up for a free credit monitoring service, do it. Your credit report will be monitored for unusual activity and you'll receive an alert if there's an unusual transaction.

BE VIGILANT!

Despite all its advantages, signing up for a credit report monitoring service is not an absolute guarantee against fraud.

- 】 Keep a regular eye on your bank and credit card statements and any new invoices you receive in the mail. Immediately report any suspicious activity to your financial institution.
- 】 Regularly check your credit reports from the main credit bureaus (Equifax and TransUnion) for errors.
- 】 You could also ask those credit bureaus to place a fraud alert in your file (an extra fee may be charged). A fraud alert lets lenders know that they should pay special attention to credit applications involving you and that they must confirm your identity before approving any applications.
- 】 If necessary, contact your local police.

BEWARE OF THE FOLLOWING SITUATIONS

Don't blindly trust your caller ID!

Some fraudsters may modify the name and number on your caller ID to make it appear as if the call is from a financial institution or government agency, for example.

- ▶ You receive an e-mail or text message that appears to be from a government agency or company you do business with. You're asked to immediately update your personal information or click on a link provided in the e-mail message. Be careful! It could be a phishing attempt (see Fraud 1).
- ▶ Someone offers to protect your computer by accessing it remotely in order to install the necessary updates, antivirus software and other systems.

Never give a stranger remote access to your computer.

- ▶ You receive a credit card statement in the mail showing expenses you didn't incur.

Call your credit card issuer using the issuer's actual phone number, not the one on the statement. Some fraudsters create fake statements showing a phone number belonging to them. If you contact them, they'll request personal information supposedly to make sure you're the person you say you are.

- ▶ Someone offers to provide you with a new SIN for a fee.

SAY NO! Service Canada does not issue new SINs after personal data leaks. Don't keep your SIN with you: store it in a safe place.



DID YOU KNOW?

Cybersurveillance

The AMF has a team of investigators specializing in cybersurveillance. The team uses specialized software programs to uncover individuals and businesses offering financial products to Québec investors without being authorized to do so.

The investigators also monitor the activities of certain sites that are considered suspicious. Depending on the circumstances, these investigators are able to infiltrate operations. Based on their findings, the AMF files cease trade and freeze orders to safeguard assets during investigations. The AMF also files legal proceedings with the courts. Report suspicious websites to the AMF!

AMF SUPPORT SERVICES

Information Centre – 1-877-525-0337

Contact the AMF Information Centre if you think someone has tried to commit financial fraud against you. Our agents can answer your questions and assist you if necessary.

Financial services compensation fund

This fund can provide compensation up to \$200,000 per claim to individuals who were defrauded while doing business with an insurance representative, a mutual fund representative, a scholarship plan representative, a claims adjuster, a financial planner or, as of May 1, 2020, a mortgage broker.

Some conditions apply. Visit the AMF website or contact the Information Centre for more details.

Whistleblower Program – 1-866-332-0115

The AMF has set up a secure window through which whistleblowers can report information. The information they disclose is dealt with in complete confidence by a specialized team.

A dark blue banner with a blurred background of people. At the top, a yellow banner says "SOUND THE ALARM!". Below it, a white box contains "WHISTLEBLOWER PROGRAM" and to the right, "HELP US PROTECT YOU". The main text in white reads: "Report any fraud attempt against you to the AMF. It could help prevent others from being defrauded." Below this, two horizontal white lines separate the text "Fighting fraud is everyone's business!".

SOUND THE ALARM!

WHISTLEBLOWER PROGRAM **HELP US PROTECT YOU**

Report any fraud attempt against you to the AMF. It could help prevent others from being defrauded.

Fighting fraud is everyone's business!



**AUTORITÉ
DES MARCHÉS
FINANCIERS**

To contact
the Autorité des marchés financiers

QUÉBEC CITY

Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

MONTRÉAL

800, rue du Square-Victoria, 22^e étage
C.P. 246, Place Victoria
Montréal (Québec) H4Z 1G3

INFORMATION CENTRE

Québec City: 418-525-0337
Montréal: 514-395-0337
Toll-free: 1-877-525-0337

lautorite.qc.ca