How to help protect yourself from fraud

RBC Wealth Management

How to help protect yourself from fraud

According to recent regulatory notices from the Financial Industry Regulatory Authority (FINRA), fraud targeting senior investors is a growing problem. At RBC Wealth Management, we believe helping you protect yourself is a top priority. And the good news is: a little education can go a long ways toward prevention.

Please read this educational material and share it with people you care about. If you have questions — or believe you may be a victim of fraud — please contact your RBC Wealth Management financial advisor. As an objective financial professional, he or she can help you understand your options and choose appropriate next steps.

Who is at risk?

A surprising finding of the FINRA report is that victims of investment fraud scored highly on financial literacy tests, suggesting that financial literacy alone is not enough to avoid fraud.

Another result that you may not expect is that married men with higher levels of education and income than the general population are especially vulnerable. Although the report did not say why, it may be because this demographic is attractive to fraudsters (i.e., educated, upper-income men may have more money and a greater interest in investing than the general population).

Other key findings include the tendency for fraud victims to be more optimistic about the future and that they dramatically under report fraud. Indeed, many seniors do not know how to prevent themselves from being victimized, do not recognize a scam when it is happening to them and often are not even aware they have been defrauded after the fact. Regardless of financial knowledge, gender, income level or outlook, it is clear that everyone must be alert to possible fraud.

Common scams

Criminals use an array of tactics, including friendship, to commit fraud. They often tailor elaborate pitches to the specific needs or interests of the people they intend to defraud. Here are five "gotchas" to watch out for. Please keep in mind that the tactical details are changing all the time, so it's best to have a general understanding of the underlying concepts.

Scam #1: phishing (pronounced "fishing")

One common way criminals collect Social Security numbers, bank or investment account numbers, birthdays and other forms of personal information is by sending emails purporting to be from a reputable business. In these emails, the businesses ask you to help them "update their records" by providing the requested information. Once they have your personal information, it can be used for fraudulent purposes, such as opening credit card accounts or making unauthorized credit card purchases. This is frequently called "identity theft."

The emails may include graphics from the businesses, such as logos. The emails may even include links to realistic looking websites where you can type in your personal information.

As a general rule, reputable companies do not use the internet to gather or verify their customers' private information. For example, RBC Wealth Management never asks you to provide personal information either via email or through our website.

If you receive emails "fishing" for personal information, it's best not to reply to them. Nor should you click any links these emails include. Just delete these emails.

Scam #2: charitable giving/socially responsible investment opportunities

As you know, the charitable organizations that are important to you depend on your generosity to do their good work. Unfortunately, criminals can take advantage of our deep desire to help the less fortunate by creating bogus charitable organizations that claim to provide assistance to those in need.

For example, after the hurricanes devastated the Gulf Coast a couple of years ago, some phony nonprofits and businesses sprang up to capitalize on our nation's grief and our citizens'

goodwill. These sham organizations created realistic-looking websites, printed high quality promotional literature and ran advertisements — all soliciting dollars to provide care and help rebuild. Sadly, the money collected went in the fraudsters' pockets instead of to fulfilling its intended purpose.

Before you donate or invest, check to make sure the charity or company is legitimate. The Federal Trade Commission website is one place to look. Go to *www.ftc.gov/charityfraud* for a variety of resources to help you determine if the charity is on the up and up.

Scam #3: affinity fraud

These scams exploit the trust among members of groups of people who have something in common, such as senior citizens. Criminals who use this approach frequently are, or pretend to be, members of the group. They also often persuade group leaders to help them convince group members that the scam is legitimate.

Affinity scams often are based on pyramid schemes, where new investor money is used to pay earlier investors and keep the illusion of authenticity going. In reality, the fraudster steals the money collected for personal use. Of course, when the group can find no more new investors, the scheme collapses and the victims of the ruse discover most or all of the money they invested is gone.

To avoid affinity fraud, never make an investment based solely on the recommendation of a member of a group to which you belong — no matter how trustworthy he or she may seem. He or she may have been fooled into believing the investment is legitimate. Get as much information as you can, in writing, and be skeptical of any opportunity that does not have written documentation. Don't fall for promises of guaranteed returns. If it sounds too good to be true, it probably is. You should also take your time to fully understand the investment and avoid being rushed into making an investment decision.

Scam #4: internet investment fraud

While the internet is a vast resource of reliable investment information, cyberspace is also home to criminal schemes of which to beware. Which is why you should always think twice before you invest in opportunities you find out about from the internet.

- **Pump and dump ploys —** Fraudsters often use investment e-newsletters, emails, bulletin board messages and blogs to hype a certain stock in which they hold a position. Writers may claim they have inside information or an infallible process for picking stocks. Once gullible investors have bought the stock and driven up its price, these fraudsters sell ("dump") their shares and stop "pumping" the stock. Then the stock price typically falls and the investors lose their money.

  Small, thinly traded stocks are frequently used for pump and dump ploys, because it is easier to manipulate a stock's price when information about the company is limited.
- **Pyramid schemes —** The classic "ponzi" or pyramid scheme described in the affinity fraud section (scam #3) is also widespread on the internet. Emails promising to turn a small investment into a big payday are designed to recruit new participants into the program.
- **Risk-free offers —** Emails promising low risk opportunities to participate in sophisticated-sounding investments that imply a high or safe return, like prime bank securities, are commonplace. Sometimes these risk-free offers are for investments in companies touting desirable but non-existent technologies or products, such as a revolutionary, pollution free, source of unlimited energy.

  Unsolicited emails describing "can't miss" investment opportunities are a red flag. Should you receive one of these emails, you can forward it to the Securities and Exchange Commission at *enforcement@sec.gov*.
- **Off-shore scams —** The internet makes it possible for criminals to commit fraud from anywhere in the world. A popular international scheme is a request to invest in a developing country (very similar to the "heartstrings" approach taken in scam #2, charitable giving and socially responsible investing).

  Another widespread problem are emails asking Americans to help someone — perhaps a highly paid professional, maybe even a church or civic leader — get their money out of a foreign bank by sending the writer money. Usually these emails promise that once the writer has liquidated the account, he or she will return the loan with substantial interest.

  Be extra careful when considering any investment opportunity in another country, because it is difficult for law enforcement agencies of the United States to investigate and prosecute fraud perpetrated from foreign jurisdictions.

  Clearly, when it comes to the internet, you can't believe everything you read. As with any investment, always check it out thoroughly before putting any money into it. Never invest in something that you don't fully understand. Taken at face value, most of these scams don't pass the "smell" test. And again, the age-old adage applies: if a deal sounds too good to be true, it probably is.

Scam #5: "boiler room" cold calls

Criminal enterprises can make a lot of money fairly quickly by visiting your community, grabbing a telephone book and renting a room where slick-talking fraudsters make calls posing as stock brokers. To avoid capture and prosecution, these boiler room cold call operations rarely stay in one place for very long.

Cold callers may try to "warm you up" with kind words and may try to put you off guard by chatting with you about your hometown or even suggesting that they've spoken with you or someone you trust before. Watch out for these tricks.

- **High-pressure sales tactics —** Aggressive cold callers use scripts including answers to overcome common objections. As long as you stay on the phone, they will try to give you the hard sell — and they won't let you get a word in edgewise until you say "yes."
- **"Once-in-a-lifetime" opportunities —** Someone who calls to pitch you a "once in a lifetime" opportunity — especially if it is based on "inside" or "confidential" information is your sign to hang up the phone.
- **Investments in companies with amazing new technologies —** Callers touting companies with "breakthrough technologies" can sound legitimate, especially when they describe enhancements to real products or technologies.
- **Callers who refuse to send you written information about the investment —** Hang up the phone immediately. Investments that don't include the proper documentation are nothing but a risk you don't want to take.
- **Calls from unsupervised sales people —** Cold calling "brokers" and their bosses may not be properly registered to sell securities. You can verify if the caller is registered by using the BrokerCheck feature on the FINRA website. Type *www.finra.org* in your web browser, to find out if a broker is legitimate — and if any disciplinary action has been taken against him or her.

If you wish to stop receiving cold calls, add your name to the Federal Trade Commission's Do Not Call Registry by going to *www.donotcall.gov* or by calling 1 (888) 382-1222.

Protection checklist

It's important to always investigate before you invest. Here are four steps you can take to help verify that an investment opportunity is legitimate and avoid being taken in.

1. Request written financial information, such as a prospectus, annual report, offering circular or other financial statements. Compare the documents you receive to what you've been told or read online.
2. Don't invest in small, thinly traded companies unless you are prepared to lose every penny.
3. Contact the Securities and Exchange Commission and your state's securities regulatory agency to see if they have information about the investment you are considering.
4. Get a qualified second opinion. Ask your financial advisor or another trusted professional, such as your banker, attorney or accountant if the investment is legitimate and if it is appropriate for you.

Beware of the "other" form of fraud

Unfortunately, criminals are not the only ones to prey on seniors. The sad fact is many seniors are victimized by people they care about and trust. Please be aware of other forms of financial abuse that constitute fraud.

- **Coercion —** Sometimes, a loved one may try to use their influence to make you do something you do not wish to do, such as giving them stock certificates or family heirlooms for safe keeping. Or they may pressure you to sign a deed, will, power of attorney or other document that is not written with your best interests in mind. Coercion can be overt and can be based on threat or intimidation. But just as often, someone trying to force you to give something up to them may use tactics designed to confuse you or conceal information from you.
- **Theft —** Other times, fraud can be more direct. A trusted person may try to steal a credit card or a credit card number to make unauthorized purchases. Or they may try to forge your signature or otherwise steal your identity for fraudulent purposes. They may even try to use your property or possessions without your permission.
- **Deception —** Finally, there may be times when people you trust may simply lie to you. For example, a loved one may promise that if you give them money or property today, they will provide lifelong care to you in the future — while never intending to fulfill their obligation when the time comes.

Additional resources

The Federal Trade Commission website (*www.ftc.gov*) includes an extensive library of educational content about fraud protection. Go to the "consumer protection" tab and click "consumer information" to browse subjects by category. The Financial Industry Regulatory Authority also has educational material for senior investors at *www.saveandinvest.org*. The Securities and Exchange Commission has a wealth of practical consumer awareness information on its website (*www.sec.gov/investor/pubs*).

Sources:

Financial Industry Regulatory Authority, *http://www.finra.org/*

Securities and Exchange Commission website: *www.sec.gov*