



SEC

OFFICE of INVESTOR
EDUCATION and ADVOCACY

Investor Alert: Social Media and Investing - Avoiding Fraud

The SEC's Office of Investor Education and Advocacy is issuing this Investor Alert to help investors be better aware of fraudulent investment schemes that may involve social media. U.S. retail investors are increasingly turning to social media, including Facebook, YouTube, Twitter, LinkedIn and other online networks for information about investing. Whether it be for research on particular stocks, background information on a broker-dealer or investment adviser, guidance on an overall investing strategy, up-to-date news, or to simply discuss the markets with others, social media has become a key tool for U.S. investors.

While social media can provide many benefits for investors, it also presents opportunities for fraudsters. Social media, and the Internet generally, offer a number of attributes criminals may find attractive. Social media lets fraudsters contact many different people at a relatively low cost. It is also easy to create a site, account, email, direct message, or webpage that looks and feels legitimate – and that feeling of legitimacy gives criminals a better chance to convince you to send them your money. Finally, it can be difficult to track down the true account holders that use social media. That potential for anonymity can make it harder for fraudsters to be held accountable. As a result, investors need to use caution when using social media when considering an investment.

What You Can Do To Protect Yourself - Tips to Help Avoid Fraud Online

So, what can individual investors do to use social media, while at the same time protecting themselves? ***The key to avoiding investment fraud on the Internet is to be an educated investor.*** Below are five tips to help you avoid investment fraud on the Internet:

Be Wary of Unsolicited Offers to Invest

Investment fraud criminals look for victims on social media sites, chat rooms, and bulletin boards. If you see a new post on your wall, a tweet mentioning you, a direct message, an e-mail, or any other unsolicited – meaning you didn't ask for it and don't know the sender – communication regarding a so-called investment opportunity, you should exercise extreme caution. ***An unsolicited sales pitch may be part of a fraudulent investment scheme.*** Many scams use spam to reach potential victims. For example, with a bulk e-mail program, spammers can send personalized messages to millions of people at once for much less than the cost of cold calling or traditional mail. If you receive an unsolicited message from someone you don't know containing a "can't miss" investment, your best move is to pass up the "opportunity" and report it to the [SEC Complaint Center](#).

Look out for Common “Red Flags”

Wherever you come across a recommendation for an investment – be it on the Internet or from a personal friend (or both), the following “red flags” should cause you to use extreme caution in making an investment decision:

- **It sounds too good to be true.** Any investment that sounds too good to be true probably is. Compare any promised return with the returns on well-known stock indexes. Any investment opportunity that claims you’ll receive substantially more than that could be highly risky – or be an outright fraud. Be extremely wary of claims on a website that an investment will make “INCREDIBLE GAINS” or is a “BREAKOUT STOCK PICK” or has “HUGE UPSIDE AND ALMOST NO RISK!” ***Claims like these are hallmarks of extreme risk or outright fraud.***
- **The promise of “guaranteed” returns.** Every investment entails some level of risk, which is reflected in the rate of return you can expect to receive. If your investment is 100% safe, you’ll most likely get a low return. Most fraudsters spend a lot of time trying to convince investors that extremely high returns are “guaranteed” or that the investment “can’t miss.” Don’t believe it.
- **Pressure to buy RIGHT NOW.** Don’t be pressured or rushed into buying an investment before you have a chance to think about – and investigate – the “opportunity.” Be especially skeptical of investments that are pitched as “once-in-a-lifetime” opportunities, particularly when the promoter bases the recommendation on “inside” or confidential information.

Look out for “Affinity Fraud”

Never make an investment based solely on the recommendation of a member of an organization or group to which you belong, especially if the pitch is made online. An investment pitch made through an online group of which you are a member, or on a chat room or bulletin board catered to an interest you have, may be an affinity fraud. Affinity fraud refers to investment scams that prey upon members of identifiable groups, such as religious or ethnic communities, the elderly, or professional groups. ***Even if you do know the person making the investment offer, be sure to check out everything – no matter how trustworthy the person seems who brings the investment opportunity to your attention.*** Be aware that the person telling you about the investment may have been fooled into believing that the investment is legitimate when it is not.

Be Thoughtful About Privacy and Security Settings

Investors who use social media websites as a tool for investing should be mindful of the various features on these websites in order to protect their privacy and help avoid fraud. ***Understand that unless you guard personal information, it may be available not only for your friends, but for anyone with access to the Internet – including fraudsters.*** For more information on privacy and security settings, as well as other guidance regarding setting up on-line accounts with an eye toward avoiding investment fraud, see our Investor Bulletin [*Social Media and Investing: Understanding Your Accounts.*](#)

Ask Questions and Check Out Everything

Be skeptical and research every aspect of an offer before making a decision. ***Investigate the investment thoroughly and check the truth of every statement you are told about the investment.*** Never

rely on a testimonial or take a promoter's word at face value. You can check out many investments using the SEC's EDGAR filing system or your state's securities regulator. You can check out registered brokers at FINRA's [BrokerCheck website](#) and registered investment advisers at the SEC's [Investment Adviser Public Disclosure website](#). See our publication "[Ask Questions](#)" for more about information you should gather before making an investment.

A Few Common Investment Scams Using Social Media and the Internet

While fraudsters are constantly changing the way they approach victims on the Internet, there are a number of common scams of which you should be aware. Here are a few examples of the types of schemes you should be on the lookout for when using social media:

"Pump-and-Dumps" and Market Manipulations

"Pump-and-dump" schemes involve the touting of a company's stock (typically small, so-called "microcap" companies) through false and misleading statements to the marketplace. These false claims could be made on social media such as Facebook and Twitter, as well as on bulletin boards and chat rooms. Pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. ***Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.***

For an example of an actual case, see [Securities and Exchange Commission v. Carol McKeown, Daniel F. Ryan, Meadow Vista Financial Corp.](#)

[and Downshire Capital, Inc.](#), Civil Action No. 10-80748-CIV-COHN (S.D. Fla. June 23, 2010).

Fraud Using "Research Opinions," Online Investment Newsletters, and Spam Blasts

While legitimate online newsletters may contain useful information about investing, others are merely tools for fraud. Some companies pay online newsletters to "tout" or recommend their stocks. Touting isn't illegal as long as the newsletters disclose who paid them, how much they're getting paid, and the form of the payment, usually cash or stock. But fraudsters often lie about the payments they receive and their track records in recommending stocks. Fraudulent promoters may claim to offer independent, unbiased recommendations in newsletters when they stand to profit from convincing others to buy or sell certain stocks – often, but not always, penny stocks. ***The fact that these so-called "newsletters" may be advertised on legitimate websites, including on the online financial pages of news organizations, does not mean that they are not fraudulent.*** To learn more, read our [tips for checking out newsletters](#).

For an example of an actual case, see [Securities and Exchange Commission v. Wall Street Capital Funding LLC, Philip Cardwell, Roy Campbell, and Aaron Hume](#), Civil Action No. 11-cv-20413-DLG (S.D. Fla. February 7, 2011).

High Yield Investment Programs

The Internet is awash in so-called "high-yield investment programs" or "HYIPs." These are unregistered investments typically run by unlicensed individuals – and they are often frauds. The hallmark of an HYIP scam is the promise of incredible returns at little or no risk to the investor. A HYIP website might promise annual (or even monthly, weekly, or daily!) returns of 30 or 40 percent – or more. Some of these scams may use the term "prime bank" program. ***If you are approached online to invest in one of these, you should exercise extreme caution – they are likely frauds.***

For an example of an actual case, see [Securities and Exchange Commission v. David Tanner, individually and d/b/a Capital Enhancement Club, Rocky D. Spencer, Marroc Corp. and Richard P. Kringen, Defendants, and Margaret Spencer, Omnibus LLC, Vectra Resources LLC and Dynamic Environmental Solutions, Inc., Relief Defendants](#), Civil Action No. 05-4057-SAC, (United States District Court; District of Kansas; Topeka Division May 4, 2005).

Internet-Based Offerings

Offering frauds come in many different forms. Generally speaking, an offering fraud involves a security of some sort that is offered to the public, where the terms of the offer are materially misrepresented. The offerings, which can be made online, may make misrepresentations about the likelihood of a return. For example, in a recent case, [Securities and Exchange Commission v. Imperia Invest IBC](#) (listed below), the fraudsters allegedly used a website to offer investors a “guaranteed return” of 1.2% per day. Other online offerings may not be fraudulent *per se*, but may nonetheless fail to comply with the applicable registration provisions of the federal securities laws. While the federal securities laws require the registration of solicitations or “offerings,” some offerings are exempt. ***Always determine if a securities offering is registered with the SEC or a state, or is otherwise exempt from registration, before investing.***

For an example of an actual case, see [Securities and Exchange Commission v. Imperia Invest IBC](#), Civil Action No. 2:10-cv-00986-B (D. Utah). See also [In the Matter of Migliozi and Flatow](#), SEC Rel. 9216 (June 8, 2011) (settled order).

contact the SEC, FINRA, or your state securities regulator to report the fraud and to get assistance.

[U.S. Securities and Exchange Commission](#)
Office of Investor Education and Advocacy
100 F Street, NE
Washington, DC 20549-0213
Telephone: (800) 732-0330
Fax: (202) 772-9295

[Financial Industry Regulatory Authority \(FINRA\)](#)
FINRA Complaints and Tips
9509 Key West Avenue
Rockville, MD 20850
Telephone: (301) 590-6500
Fax: (866) 397-3290

[North American Securities Administrators Association \(NASAA\)](#)
750 First Street, NE
Suite 1140
Washington, DC 20002
Telephone: (202) 737-0900
Fax: (202) 783-3571

Where can I go for help?

Investors who learn of investing opportunities from social media should always be on the lookout for fraud. If you have a question or concern about an investment, or you think you have encountered fraud, please

Related Information

For additional educational information for investors generally, see the SEC's website for individual investors, Investor.gov. For additional information about securities fraud, see:

[NASAA Informed Investor Advisory: Social Networking](#)

[Operation Broken Trust](#)

[Avoiding Fraud](#)

[Stopping Affinity Fraud in Your Community](#)

[FINRA Warns Investors of Social Media-Linked Ponzi Schemes, High-Yield Investment Programs](#)

The Office of Investor Education and Advocacy has provided this information as a service to investors. It is neither a legal interpretation nor a statement of SEC policy. If you have questions concerning the meaning or application of a particular law or rule, please consult with an attorney who specializes in securities law.

