Are You an Informed Investor?

Sorry, Your Adviser May Be a Fake

August 2026

Artificial intelligence (AI) is rapidly transforming the world around us. AI platforms can be useful tools for investors seeking to learn more about investing and financial products. Investors who are using AI, or are interested in investing in this industry, should be aware that scammers are exploiting the hype around this technology to create and pitch sophisticated investment scams.



How AI Is Being Used in Investment Scams

Scammers are using AI in a variety of ways, including offering fake trading products that will purportedly generate very high returns for investors. AI chatbots, programming tools, and image generators allow scammers to create professional looking online content and websites quickly and professionally. Gone are the days when typo-riddled websites or investment pitches helped people identify scams. Additionally, translation tools allow scammers to communicate with anyone, anywhere and in any language.

Here are some common AI-related investment scams that securities administrators are aware of:

Impersonation and Deepfake Scams

AI is used to create realistic videos or audio of well-known figures or celebrities that promote investments offering high and/or guaranteed rates of return. These scams are known as "deepfakes"[1] and they appear in social media posts or online ads. Scammers may also send them by text messages or share them in online investment groups or chats. This technology can be used to impersonate anyone, even your advisor, a family member, or a friend.

---

1 See NASAA's Informed Investor Advisory: Impersonation Scams (https://www.nasaa.org/78175/informed-investor-advisory-impersonation-scams/?qoid=investor-advisories)

Crypto and AI Trading Schemes

Scams that claim to use "proprietary" or "guaranteed" AI trading systems to trade crypto or investment products are commonly advertised online. Investors who respond to the ad are directed to the fake company and asked to pay a fee, usually using a cryptocurrency. These platforms are unregistered, difficult to verify, and may display fake account balances or fabricated profits to convince investors to send more money.

AI Voice and Messaging Scams

Scammers can use AI to clone anyone's voice, including celebrities, politicians, or even someone you know personally (like a family member, close friend

Continued

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

or your financial adviser). If you receive a call or text message from someone pressuring you to invest with them, it's probably a scam. It's generally illegal to offer investments or investment advice for a fee without being registered, so be very wary of anyone who is encouraging you to invest with them. Furthermore, if you receive an unsolicited call or message from your financial adviser, consider if it could be an AI deepfake. If you're at all unsure, contact your financial adviser directly to follow up.

Romance Scams

Scammers can use AI-generated images to create fake dating profiles. They can also deploy chatbots to converse and learn from conversations they have with you. Once scammers gain your trust, they will likely try to convince you to invest in things like cryptocurrency or startup companies. They will often ask you to open an account with a crypto trading platform, and request access to your online account or wallet. Once you deposit money, they will take it and it's gone.

Red Flags

AI may be new, but the warning signs of investment fraud generally remain the same. If something feels off, trust your instincts and pause before acting.

Be cautious if you encounter:

- Unexpected phone calls or text messages on your phone or messaging app.
- Online ads promoting investments from celebrities or public figures.
- Unusual facial or body movements in videos.
- Strange or awkward phrasing in voice messages or videos.
- Requests for payment in cryptocurrency or through unconventional methods.
- Reluctance to meet in person.
- Excuses or changing the topic when asked to verify credentials.
- Websites or platforms that are new, don't offer contact information, or mimic legitimate firms.

How to Protect Yourself

The first step in protecting yourself is to not act immediately. Scammers use pressure tactics and the fear of missing out (a.k.a. FOMO) to pressure investors into scams. Be patient and careful when investing in anything. It's your money, and you need to be comfortable with the investment and the risk you are taking when investing.

Here are some other steps that you can take to help avoid AI investment scams:

Verify Registration

Confirm that the individual or firm offering the investment is registered. Registration does not guarantee an investment is risk-free, but unregistered sellers are a major warning sign.

Continued

**To learn more, contact the Division of Securities,
Wisconsin Department of Financial Institutions**

**4822 Madison Yards Way, 4th Floor North Tower, Madison, WI 53705
dfi.wi.gov | (608) 266-2139 | DFISecurities@dfi.wisconsin.gov**

NASAA

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

Do Your Own Research

Independently verify claims, look up information online that may help determine if something is a scam. Run searches of the company offering the investment, the individual you are talking to, and their contact information. Often these searches reveal that the names or phone numbers of the people contacting you are fake and/or a part of a scheme.

Don't Rely on AI Alone

If you use AI tools yourself, know that this can generate inaccurate, outdated, or even fabricated information. Always crosscheck investment claims with reliable sources. Regulators provide investor education information about scams, and many of them publish Investor Alerts, or have investment warning lists.

Talk to a Registered Professional

Discuss potential investments with a registered investment professional. They can help you research the validity of an investment. Registered advisers should be able to discern whether an investment is a scam.

Report Suspicious Activity

If you suspect you have been hit by an AI investment scam or if you believe you have been targeted:

- Report the incident to your state or provincial securities regulator.
- File a complaint with appropriate national authorities, including the Federal Trade Commission (FTC) or the Internet Crime Complaint Center (IC3).
- Reporting scams helps regulators identify emerging threats and protect other investors. In addition, beware of anyone who offers to help recover your lost money. They may be part of the scam.

Bottom Line

AI is enabling fraudsters to change how investment scams look, but the underlying scams are often predictable. Scammers rely on pressure tactics, fake promises, and misplaced trust. Understanding how AI can be misused to pitch and develop investment scams can help you protect your money.

For more tips and information about how to be a better-informed investor, contact your state or provincial securities regulator. Contact information is available on the NASAA website (go to https://www.nasaa.org/contact-your-regulator/).

NASAA has provided this information as a service to investors. It is neither a legal interpretation nor an indication of a policy position by NASAA or any of its members, the state and provincial securities regulators. If you have questions concerning the meaning or application of a particular state law or rule or regulation, or a NASAA model rule, statement of policy, or other materials, please consult with an attorney who specializes in securities law.

**To learn more, contact the Division of Securities,
Wisconsin Department of Financial Institutions**

**4822 Madison Yards Way, 4th Floor North Tower, Madison, WI 53705
dfi.wi.gov | (608) 266-2139 | DFISecurities@dfi.wisconsin.gov**

DFI