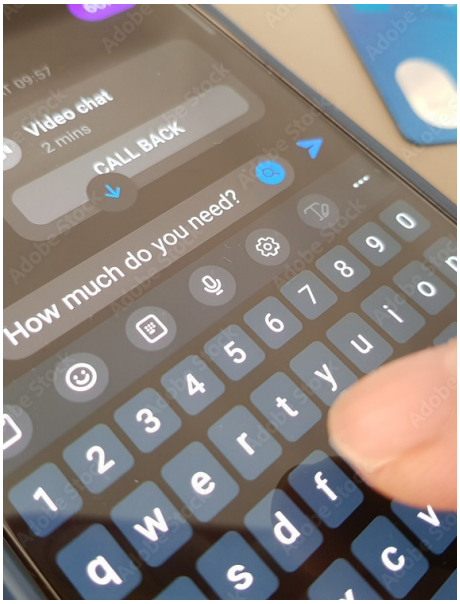
NASAA Investor Alert

Relationship Investment Scams

October 2024



The SEC's Office of Investor Education and Advocacy (OIEA), the Commodity Futures Trading Commission's Office of Customer Education and Outreach (OCEO), the Financial Industry Regulatory Authority (FINRA), and the North American Securities Administrators Association (NASAA) are issuing this Investor Alert to warn investors about relationship investment scams, where fraudsters — including criminals and other bad actors — often hide their true identities, reach out to unsuspecting targets (often online or through text messages), gain their trust over time, and then defraud them through fake investments. Relationship investment scams are sometimes referred to by various terms including romance scams, "cryptocurrency" investment scams, financial grooming scams, and even the distasteful term "pig butchering scams." These scams also sometimes involve "catfishing," where fraudsters might set up fake online identities to carry out crimes.

Fraudsters Might Seek Targets Online, on Social Media Platforms, or Through Text Messages.

Criminals and other fraudsters seek their targets in many different ways.

- They often initiate contact online or on social media platforms — including professional networking, dating, and messaging websites/apps.
- They might run advertisements or add targets to a group chat that the target didn't seek to join.
- Fraudsters might text a target pretending to be an old friend or claiming to have contacted the target accidentally. They might even use an auto dialer to blast out unsolicited text messages to thousands of people — these messages are designed to mimic ones intended for some other personal or business acquaintance, seeking to prompt a response from potential targets.
- They might offer financial advice or express romantic interest.
- Sometimes, these fraudsters quickly move communications away from the initial platform to a different, sometimes unmonitored space.

To learn more, contact the Wisconsin Department of Financial Institutions, 4822 Madison Yards Way, 4th Floor North Tower, Madison, Wisconsin 53705 | dfi.wi.gov | (608) 266-2139

NASAA
NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

Fraudsters Slowly Build Trust.

These scams sometimes are referred to as "long cons," meaning there's a long, slow build before the fraudster springs their trap.

Once they find a target who's willing to engage with them, these fraudsters begin the long process of building their trust, be it through friendship, romance, or an offer to help achieve financial goals. They might even suggest meeting in person but then come up with excuses so that this never happens. In romance scams, they often pledge their love very quickly. Their goal is to gain the target's trust and confidence.

Sometimes, the fraudster creates a fake identity as a financial professional with a prominent online presence, or they might impersonate — or "spoof" — legitimate investment professionals or brokerage firms. They sometimes use altered images or videos to lead their targets to believe that others have made money on their platform. New artificial intelligence (AI) technologies can make these images and videos convincingly realistic.

Once Fraudsters Gain Trust, They Convince Targets to "Invest" Their Money.

Once fraudsters have established a relationship or friendship with their target, they might offer their advice on trading, or claim to know about profitable opportunities. They might even indicate that they or someone they know is a financial advisor or is an "insider" and is able to provide valuable trading recommendations.

These fraudsters can lead their targets to believe they are doing well trading by sending fake screenshots, showing fake trading information, or manipulating the target's online account to make it appear that the "investments" and "earnings" are "legitimate," all of which is intended to build trust.

Fraudsters might also steer their targets towards investments involving crypto assets. For example, the target might think they're buying into a crypto asset investment like an "Initial Coin Offering" (or "ICO") when they're actually just sending money directly to fraudsters' crypto asset wallets or accounts.

Fraudsters might direct their targets to a legitimate looking (but fake) website or to a widely used app that can be downloaded from a well-known app store. However, just because an app is available on a well-known app store doesn't mean that the app itself, or the activities conducted within it, are legitimate. Fraudsters might tell their targets to wire cash or obtain crypto assets— such as bitcoin, ether, or tether—at a bitcoin ATM (or kiosk) or through a crypto asset platform in order to make investment deposits. An investment might not be legitimate if the investor is required to pay for it with crypto assets.

If you're directed to pay for an investment by wire transfer or check, be suspicious if:

- You're asked to pay an individual, a firm that is different than the one with which you thought you're investing, or a business that appears unrelated to your investment (for example, a nail salon or foot massage business);
- The address is suspicious (for example, an online search for the address suggests it's not an office building where the firm operates); or
- You're told to note that the payment is for a purpose unrelated to the investment (for example, luxury watches, goods, or furniture).

Continued

To learn more, contact the Wisconsin Department of Financial Institutions, 4822 Madison Yards Way, 4th Floor North Tower, Madison, Wisconsin 53705 | dfi.wi.gov | (608) 266-2139

Department of Financial Institutions
State of Wisconsin

If you wire money outside of the United States or use crypto assets for an investment that turns out to be a scam, you likely will never see your money again.

Don't Gain a False Sense of Comfort By Being Able to Make Early Withdrawals or Seeing "Profits" in Your Account.

Fraudsters sometimes deliberately falsify information to make their targets believe they've profited from whatever investment "opportunity" the fraudsters presented.

They might even allow a target to withdraw a portion of their "profits" to further gain their trust and falsely reassure them that the investment is legitimate. The fraudsters might provide what they claim is "real time" trading information that is, in fact, fake. They often lead targets to believe that other investors are making enormous profits too.

Fraudsters might then ask their targets to invest larger sums of money. But when the target wishes to withdraw their funds, the fraudsters often come up with an excuse why that isn't possible, say more money is required, or tell the target for the first time that they must pay more to cover fees or taxes. Frequently, the target will never recover their investment or any "profits," so paying additional funds only causes the target to lose more money.

Similarly, fraudsters might pretend to loan their targets funds for trading but require these "loans" to be repaid before any purported profits or principal can be withdrawn. This, too, is a further attempt to steal more money.

Beware of Fake Testimonials.

Fraudsters often use fake testimonials to convince targets that others have invested and made money.

Never rely solely on testimonials in making an investment decision. Fraudsters sometimes pay others — for example, actors to pose as ordinary people turned millionaires, social media influencers, and celebrities — to tout an investment on social media or in a video. If you're in a group chat, others in the group who claim to have made huge profits might be in on the fraud.

Fraudsters might also use altered or AI-generated photos or videos to make it falsely look like others have profited. For example, depictions of skyrocketing account balances often are fake. The potential for high investment returns usually involves high risk. Promises of high investment returns, with little or no risk, are classic warning signs of fraud.

Consider Reporting, Deleting, and Blocking Unsolicited Messages from Senders You Don't Know.

If you receive an email or text message from a person, number, or email address you don't know or recognize, be suspicious — especially if the message is vaguely worded or appears aimed at someone else. This is a red flag of fraud.

If the message purports to come from a business or financial institution that you do business with, do not use contact information or click on any link(s) provided in the message. Instead, call the customer service phone number or type in the url for the website found on the bill or statement you receive from the business itself to verify the authenticity of the message. Don't respond to unexpected

Continued

or unsolicited text messages received from unknown senders. Instead, consider reporting and blocking these senders from your phone or messaging app.

No matter how trustworthy someone might seem, don't make investment decisions based on the advice of anyone who makes unsolicited contact with you online or through an app or text message.

Do your own independent research and ask questions.

Similarly, don't share any information relating to your personal finances or identity (including your bank or brokerage account information, tax forms, credit card, Social Security number, passport, driver's license, birthdate, or utility bills) with someone you don't know who contacts you online, on a social media platform, or through text message.

Report possible securities fraud to the SEC (http://www.sec.gov/complaint/tipscomplaint.shtml).

Additional Information

- 5 Ways Fraudsters May Lure Victims into Scams Involving Crypto Asset Securities – Investor Alert (https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/crypto-scams)
- CFTC Fraud Alert: Romance Frauds (https://www.cftc.gov/LearnAndProtect/romancefrauds)
- CFTC article: Relationship Cons, Recovery Scams, & Money Laundering (https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/Fraudin3Acts.html)

FINRA Investor Insights:

- 'Pig Butchering' Scams: What They Are and How to Avoid Them (https://www.finra.org/investors/insights/pig-butchering-scams)
- Be Aware of Support Center Ad Scams (https://www.finra.org/investors/insights/support-center-ad-scams)
- Be Alert to Signs of Imposter Investment Scams This On Ramp Could Lead You to a Dump (https://www.finra.org/investors/insights/be-alert-signs-imposter-investment-scams)
- Following the Crowd: Investing and Social Media (https://www.finra.org/investors/insights/following-crowd-investing-and-social-media)

NASAA: Are you an informed investor?:

- Don't Get Swept Away by a Romance Scam (https://www.nasaa.org/72703/informed-investor-advisory-dont-get-swept-away-by-a-romance-scam/?qoid=investor-advisories)
- Stranger Texts: Don't Answer Unsolicited Messages (https://www.nasaa.org/66411/informed-investor-advisory-unsoliticed-text-messages/?qoid=investor-advisories)
- Spoofing/Phishing Scams (https://www.nasaa.org/73010/informed-investor-advisory-spoofing-phishing-scams/)

FinCEN Reminds the Public to be Wary of Fraudulent Correspondence and Phone Calls (https://www.fincen.gov/fincen-reminds-public-be-wary-fraudulent-correspondence-and-phone-calls)

Ask a question or report a problem to the SEC or FINRA concerning your investments, your investment account or a financial professional. Use FINRA BrokerCheck to research investment professionals and brokerage firms.

Visit Investor.gov, the SEC's website for individual investors. Receive Investor Alerts and Bulletins from OIEA by email or RSS feed.

To learn more, contact the Wisconsin Department of Financial Institutions, 4822 Madison Yards Way, 4th Floor North Tower, Madison, Wisconsin 53705 | dfi.wi.gov | (608) 266-2139