NORTH Dakota | Securities
Be Legendary.

Securities Regulators Announce Top Investor Threats for 2022

The North Dakota Securities Department has released its annual list of top investor threats and urges caution before purchasing popular and volatile unregulated investments – especially those involving cryptocurrency and digital assets. Along with the list of top investor threats, the Department also provides guidance for investors, including steps to take to protect against fraud in the new year.

Top Investor Threats

The top 2022 investor threats were determined by a survey of securities regulators conducted by the North American Securities Administrators Association (NASAA). The annual survey is designed to identify the most problematic products, practices or schemes facing investors. The following were cited most often by state and provincial securities regulators:

1. Investments tied to cryptocurrencies and digital assets,
2. Fraudulent offerings related to promissory notes,
3. Money scams offered through social media and internet investment offers and,
4. Financial schemes connected to Self-Directed Individual Retirement Accounts.

Notably, many of the fraud threats facing investors today involve private placement offerings that are exempted by federal law from registration requirements, and states are pre-empted from enforcing important investor protection laws. Unregistered private offerings generally are high-risk investments and don't have the same investor protection requirements as those sold through public markets.

How Investors Can Avoid Fraud

Investors are urged to take the following steps to identify and avoid investment scams:

1. Anyone can be anyone on the Internet. Scammers are spoofing websites and using fake social media accounts to obscure their identities. Investors should always take steps to identify phony accounts by looking closely at content, analyzing dates of inception and considering the quality of engagement. To ensure investors do not accidently deal with an

imposter firm, pay careful attention to domain names and learn more about how to protect your online accounts.

2. Beware of fake client reviews. Scammers often reference or publish positive, yet bogus testimonials purportedly drafted by satisfied customers. These testimonials create the appearance the promoter is reliable – he or she has already earned significant profits in the past, and new investors can reap the same financial benefits as prior investors. In many cases, though, the reviews are drafted not by a satisfied customer but by the scammer. Learn how to protect yourself with NASAA's Informed Investor Advisory on social media, online trading and investing.

3. If it sounds too good to be true, it probably is. Bad actors often entice new investors by promising the payment of safe, lucrative, guaranteed returns over relatively short terms – sometimes measured in hours or days instead of months or years. These representations are often a red flag for fraud, as all investments carry some degree of risk, and the potential profits are typically correlated with the degree of risk. Learn more about the warning signs of investment fraud .

Verify Through Trusted Resources

The Securities Department recommends investors independently research the registration of investment firms. They should not use hyperlinks provided by the parties and instead contact their state securities regulator, search the SEC's Investment Adviser Public Disclosure website or FINRA's BrokerCheck platform. Investors should be aware that scammers may misappropriate the CRD numbers of registered firms and individuals. Investors should contact their regulator if they suspect the firm is engaging in this type of tactic.

Individuals offering investments are obligated to truthfully disclose all material facts, and they must disclose the risks associated with each product. On the other hand, bad actors will often minimize or conceal risks, and use hyperbole to tout profits and payouts. Investors should pay attention to these details, as they can provide clues about a potential scam.

Bad actors may be impersonating licensed parties by using phony websites that place viruses or malicious software on victim's computers. Investors should continue to observe best practices for cybersecurity. The FDIC has issued guidance to assist consumers in protecting themselves from cyber-attacks.