

Wyoming Secretary of State

Compliance Division
Herschler Building East
122 West 25th Street, Suite 100
Cheyenne, WY 82002-0020
Ph. 307.777.7370

Email: Investing@wyo.gov

INVESTOR BEWARE: Schemes to Watch for and How to Protect Yourself

The Wyoming Secretary of State's Office provides the following guidance and tips to help investors avoid anticipated schemes seeking to take advantage of unsuspecting consumers and investors.

Schemes to Watch For

- Private placements and off-market securities. Scammers will take advantage of concerns with
 the regulated securities market to promote off-market private deals. These schemes will continue
 to pose a threat to retail investors because private securities transactions are not subject to
 review by federal or state regulators. Retail investors must continue to investigate before they
 invest in private offerings and independently verify the facts for themselves.
- Gold, silver and other commodities. Scammers may also take advantage of the decline in the
 public securities markets by selling fraudulent investments in gold, silver and other commodities
 that are not tied to the stock market. These assets may also be attractive because they are often
 promoted as "safe" or "guaranteed" as hedging against inflation and mitigating systematic risks.
 However, scammers may conceal hidden fees and mark-ups, and the illiquidity of the assets may
 prevent retail investors from selling the assets for fair market value. The bottom line is there really
 are no "can't miss" opportunities.
- Recovery schemes. Retail investors should be wary of buy-low sell-high recovery schemes. For example, scammers will begin promoting investments tied to oil and gas, encouraging investors to purchase working or direct interests now so they can recognize significant gains after the price of oil recovers. Scammers will also begin selling equity at a discount, promising the value of the investments will significantly increase when the markets strengthen. Investors need to appreciate the risks associated with any prediction of future performance and recognize that gains in the markets may not correlate with the profitability of their investments.
- **Get-rich-quick schemes**. Scammers will capitalize on the increased unemployment rate. They falsely tout their ability to quickly earn guaranteed returns that can be used to pay for rent, utilities or other expenses. They also target retirees and senior citizens, falsely claiming they can quickly and safely recoup any losses to their retirement portfolios. Remember: if it sounds too good to be true, it probably is.
- Replacement and swap schemes. Investors should be wary of any unlicensed person
 encouraging them to liquidate their investments and use the proceeds to invest in more stable,
 more profitable products. Investors may pay considerable fees when liquidating the investments,
 and the new products often fail to provide the promised stability or profitability. Advisors may
 need to be registered before promoting these transactions and legally required to disclose hidden
 fees, mark-ups and other costs.

Real estate schemes. Real estate investments may prove appealing because the real estate
market has been strong and low interest rates have been increasing the demand for housing.
Scammers often promote these schemes as safe and secure, claiming real estate can be sold
and the proceeds can be used to cover any losses. However, real estate investments present
significant risks, and changes to the economy and the real estate market may negatively impact
the performance of the products.

How to Protect Yourself

- Ask questions and research the investment and person offering it. Investors should always
 ask if the salesperson and the investment itself are properly licensed or registered. This
 information can be confirmed by the Wyoming Secretary of State's Office. Investors also can
 check the <u>SEC's Investment Adviser Public Disclosure</u> database, <u>FINRA's BrokerCheck</u>, or, in
 Canada, use the <u>National Registration Search</u>. Avoid doing business with anyone who is not
 properly licensed.
- Don't fall for phishing scams. Phishing scams may be perpetrated by foreign or domestic parties claiming an association with the Centers for Disease Control and Prevention or the World Health Organization, or by individuals claiming to offer novel or expert medical advice or services. Con artists offering "opportunities" in research and development are scamming you. They may even be perpetrated by persons impersonating government personnel, spoofing their email addresses and encouraging their audience to click links or access malicious attachments. These emails may look real and sound good, but any unsolicited emails that have attachments and web links can point to dangerous websites and malicious attachments that can steal information from your computer, lock it up for ransom, or steal your identity. Don't do it.
- There are no miracle cures. Scientists and medical professionals have yet to discover a medical breakthrough or have developed a vaccine or means to cure COVID-19. Not surprisingly, the vaccines being sold by online pharmacies are not real. You should not send money or make payments over the phone to anyone claiming they can prevent COVID-19, have a vaccine or other preventive medicine.
- Avoid fraudulent charity schemes. White-collar criminals may pose as charities soliciting
 money for those affected by COVID-19. Before donating, you should independently verify any
 charity that is raising money for the sick or secure donations to help uninsured persons pay for
 medical treatment. You should also avoid online solicitations for cash and gift cards, as these
 schemes have become a popular way for scammers to steal money. Think with your head and
 not with your heart. If you want to donate to a cause, you should work with a legitimate,
 established organization.
- Be wary of schemes tied to government assistance or economic relief. The federal government may send checks to the public as part of an economic stimulus effort. It will not, however, require the prepayment of fees, taxes on the income, the advance payment of a processing fee or any other type of charge. Anyone who demands prepayment will almost certainly steal your money. And don't give out or verify any personal information either. Government officials already have your information. No federal or state government agency will call you and ask for personal information.