



Customer Advisory:

There's Nothing to Like about Scammers on Social Media

The Commodity Futures Trading Commission (CFTC) wants the public to watch for unregistered brokers and advisers, as well as fake testimonials and so-called trading experts on social media platforms. Fraud offenders can create many online profiles or anonymous identities, and use them in a coordinated way to lure people into schemes.

Common schemes include those that tout trade signals, automated trading software, trading platforms, and training in “secret” or failsafe trading strategies. Often these frauds target those who are interested in trading foreign currencies (forex), binary options, digital currencies, or precious metals. Imposter schemes may also prey on those who were recently defrauded by promising to get stolen money back. The imposters often pose as law enforcement, attorneys or government officials.

Easy Money – No Experience Necessary

Fraudulent profiles can be easy to spot if you know what to look for. They typically flaunt wealth or brag about their huge “win” percentages. Photos of exotic vacations, sports cars, and mansions are common. Details or verifiable facts about the person’s background, credentials, and experience are scarce. The profiles commonly appear to be new with few connections to family, friends, or colleagues. Bogus profiles are designed to build a façade of success, and an enviable lifestyle. Posts may even feature screen shots of “winning trades” or huge account balances.

The profiles often promote:

- Products, services, or secrets that require little or no experience, but return hundreds or thousands of dollars a day.
- Fan comments or videos that tell stories of dead-end jobs or being deep in debt before taking the plunge and sharing in the success.
- Market “geniuses” or ex-professionals who want to share their insider know-how with you. (They are so successful they feel guilty keeping their secrets to themselves.)
- Deep discounts, free trials, or guarantees to help you get started.
- A risk-free opportunity to earn millions of dollars with little effort.

But once people take that first “risk-free” step, the trap is sprung.

Unfriend these frauds

Recently, the CFTC has issued alerts or filed enforcement cases about:

- **Virtual currency pump-and-dumps:** Victims are lured into bidding up a thinly traded digital currency, usually based on social media tips or rumors.
- **Fraudulent binary options sites:** Offshore, unregistered trading platforms use fake brokers or phony customer testimonies to lure people into opening accounts.
- **Imposter frauds:** Fraudsters pose as government, law enforcement, or other officials and demand fines, fees, or taxes.
- **Marketing frauds:** Unscrupulous marketing firms create slick videos or launch multi-level-marketing schemes to bring victims into frauds.
- **Trading signals, software, or education:** These are supposed to signal traders when to buy or sell, but often come with hidden costs or don’t perform as promised.



A Net of Lies

Commenting on a video or responding to another member in a group discussion may seem innocent enough, but these interactions are just the bait. Fraudsters are often successful because they target their victims. Expressing interest, or even participating in the same groups, could make some users potential targets. Fraudsters can easily size up your profile information, and gather details from profiles on other platforms too. They go after targets they believe will be the most profitable. Professionals, retirees, people willing to take some risks with their money, or people who recently experienced some financial strain are commonly targeted.

Frauds often occur incrementally. First, you register on the fraudster's website with your email address. You receive a welcoming email with an invitation to join a webinar or receive personalized help during your free trial. The introductions are designed to build rapport and get you to commit an initial payment. Once you're invested, the pressure increases. If you appear to make money, you're pressured to invest more; if you lose money, you may be offered additional classes, upgrades, or "loss insurance." Eventually, it becomes evident the advice, signals, products, services, platforms, webinars, or workshops will never live up to the hype.

When you try to get your money back all communication stops. A few weeks later, the imposter frauds begin. You might receive an email or phone call from a law firm suing the people who took your money. Fraudsters also will pose as the IRS, CFTC, SEC or other government agencies. For an immediate up-front payment, the fraudsters claim, you can sue to get your money back, or pay off taxes and fines you've supposedly incurred.

Social Media Safety Tips

- Don't rely on tips or claims you see online.
- Scrutinize the source of the information. Is the broker or adviser currently or formerly registered with the National Futures Association (NFA), Financial Industry Regulatory Authority (FINRA), or your state securities regulator?¹ Check disciplinary histories or verify claims of experience.
- Only work with advisers and platforms that are registered to do business in the United States, or in your state, to ensure you retain your protections under the law.
- Be sure you fully understand what you're being sold, how it will make you money, and how much it will cost over the long-term, including knowing the risks of losing money, as well as recurring fees and penalties.
- Remember, there is no such thing as a risk-free investment.
- Sleep on it. Sometimes fear of losing out is a bigger motivator than winning big, so fraudsters commonly fake urgency to get a commitment. Don't take the bait.
- Never pay more money up-front to get your stolen losses back.
- Remember, government agencies will never demand money by phone or email.

To learn more, visit cftc.gov/LearnAndProtect.

¹ Visit nfa.futures.org/basicnet/ or brokercheck.finra.org to verify registrations and view disciplinary histories.