SCAM FACTSHEET

FINRA

How to Spot Broker Imposter Scams

In a broker imposter scam, a fraudster impersonates a registered investment professional or misuses a brokerage firm's name to create the appearance of legitimacy. The goal is to convince you that you're dealing with a reputable individual or firm, then steal your money or personal information.

LIFE CYCLE OF A BROKER IMPOSTER SCAM

Intro	Promotion	Legitimacy	Pressure	Closing
A scammer claiming to be a registered investment professional or satisfied customer might promote investments on social media, in encrypted group chats or via emails or cold calls.	They often tout investments that are "can't miss" or low risk/high reward and sometimes include glowing testimonials of past performance.	The scammer will attempt to create legitimacy by sending you websites or social media profiles that they claim belong to a prominent brokerage firm or its employees. They might send fake documents.	As with most investment scams, you'll face pressure to act quickly to avoid missing the opportunity.	Once you transfer assets, that's likely the last you'll hear from the scammer.

RECOGNIZE THE RED FLAGS

Broker imposter scams exploit the source credibility and familiarity of known individuals, entities or brands as a shortcut to gaining your trust. Be alert to the warning signs:

- **Unexpected Contact:** In some cases, you might be contacted directly. In others, you might see an ad on social media or see a comment from a supposedly satisfied investor detailing how much money they've made with a particular professional. While cold solicitations aren't necessarily scams, this tactic is one that fraudsters rely on.
- **Encrypted Communications:** Scammers often move the conversation to an encrypted chat on a messaging app such as WhatsApp or Telegram to make it more difficult to trace their communications. Legitimate firms rarely, if ever, allow these channels of communication.

How to Spot Broker Imposter Scams

- **Inconsistent Information:** If the seller has provided a registration number (called a CRD number) or a BrokerCheck report, go directly to FINRA BrokerCheck or the SEC's Investment Adviser Public Database to compare the information you find with what they've sent.
  - Does the associated firm of the individual align? And is the contact info for the firm that same as on its "Relationship Summary"?
  - Does the state or office location match the states in which the individual is licensed?
  - Have they provided a personal email address rather than one with the firm name?
- **Almost but Not Quite Right:** Imposters often create phony websites or social media pages that mimic legitimate ones, sometimes including names, photos or logos of real professionals or firms. Take notice of typos, poor grammar or awkward phrasing. Look closely at URLs and email addresses for a substituted character, like the number 1 in place of the letter l. Scammers hope you won't notice the subtle—but critical—differences.
- **Exaggerated Claims and Elevated Emotions:** Be skeptical of any pitch that offers guarantees or unrealistic promises, is accompanied by incomplete or unverifiable documentation or urges quick decisions. High emotions are a sign to slow down.
- **Unusual Funding Requests:** Sometimes a scammer will ask you to send money or personal information outside of official firm channels. If an individual pitches an investment that requires you to write a check directly to them or to a third party rather than the firm, or fund a securities investment through gift cards or crypto assets, that's a danger sign.
- **Requests for Secrecy:** If your contact urges you to keep secrets, do the opposite. One of your best defenses against scams is talking to someone else you trust who isn't connected to the opportunity.

DO YOU SUSPECT YOU'RE BEING TARGETED?

If you think you're being targeted in a broker imposter scam, take these immediate steps.

- **Cease Contact:** Stop communicating with the suspected scammer. Refuse any requests for more money.
- **Secure Your Accounts:** Change all of your passwords. Notify your financial institutions to be on alert. Save as much documentation as you can.
- **Alert the Impostered Firm:** Contact the real firm or individual and tell them that someone is using their name to commit fraud. This will enable them to take proactive steps to protect others.
- **Report:** Submit a regulatory tip to FINRA or the SEC, and report it to the FBI's Internet Crime Complaint Center (IC3.gov).
- **Ask for Help:** Scams can have both a financial and an emotional impact. Tell a trusted friend, family member or professional. You don't have to go it alone.

FINRA is a not-for-profit organization dedicated to investor protection and market integrity. FINRA regulates one critical part of the securities industry—member brokerage firms doing business in the U.S.