Customer Advisory: Six Warning Signs of Online Financial Romance Frauds

Beware of unsolicited financial or investment advice you receive from people you meet online. That "wrong number" text or "like" you receive from an attractive stranger may actually be from an international criminal organization using a fake name and photo. Financial romance and grooming gangs stole more than $3.5 billion in 2023 by convincing people they were starting a friendship or romantic relationship with an actual person. Conversations turn to money and soon the "friend" wants you to trade crypto assets or foreign currency. Building the relationship or "grooming" can take several weeks before the crypto-confidence fraud occurs. The gangs committing these frauds call it "sha zhu pan" otherwise known as pig butchering.

Warning Signs:

1. Your new online "friend" wants to move the conversation to a private messaging app.
2. They message frequently but can never meet in person.
3. They claim to be wealthy due to crypto or foreign currency trading successes. They sometimes claim this success is based on inside information from an uncle or other insider.
4. They encourage you to open an account and recommend a trading website that only accepts cryptocurrency.
5. They tell you to invest in crypto and send the funds to their wallet or a particular trading platform.
6. You follow their directions and make a lot of money quickly or easily.

At first, you may be encouraged to withdraw some of your profits and invest more. Eventually, you are "locked out" of your account and forced to pay more money (commonly in fake fees or "taxes") or have your ID verified to get any of your money back. Finally, the scammer vanishes along with your money.

Steps You Can Take:

- Remember the warning: If it sounds too good to be true, it probably is.
- Keep conversations on the dating/social media platform.
- Never mix money with long-distance relationships.
- Screen capture the potential scammer's picture and use reverse image searches to see if the photos have been used in other scams or by other people.
- Do everything you can to verify their identity. Conduct online searches to verify your new friend's identity and check his or her registration status at **cftc.gov/check**.
- Check the trading website you're sent to see how long it has been registered at **lookup.icann.org**.
- Report the fraud to **cftc.gov/complaint** or the FBI at **ic3.gov**, as well as to the relevant social media or dating platform and digital exchange.

Blow the Whistle:

- If you know of U.S.-based financial grooming gang operations, such as individuals opening bank or digital asset accounts for these gangs, submit a tip at **whistleblower.gov**. Whistleblowers do not need to be victims or insiders.
- Whistleblowers may receive 10 percent to 30 percent of what the CFTC collects if their tip leads to a successful CFTC enforcement action. To learn more, read the CFTC's Romance Investment Fraud Whistleblower Alert at **whistleblower.gov/whistleblower-alerts**.