

"Pump-and-Dump" scams are targeting advised clients

What is happening:

Fraudsters are promoting fake investment opportunities through social media (like X, formerly Twitter) and messaging apps (like Whatsapp and Telegram), encouraging victims to join so-called "exclusive investor groups". Often, these malefactors will use identities stolen from Schwab professionals, advisor firms, or public figures to appear more legitimate.

Once they join the "exclusive investor group", the criminals will encourage targeted clients to open new accounts at certain broker-dealers, then tell them which stocks to buy, how much, and when they should submit their trades. Why? Often, it's part of a "pump-and-dump" scheme.

"Pump and dump" scams

In these schemes, a group purchases large positions in a security—usually these securities are volatile and relatively cheap, and these fraudsters are trying to inflate the price of a specific security. Once the group has stimulated the price by convincing others to buy in, they "dump" their position, and pocket the profits from the price they have deliberately inflated. Not only are unsuspecting investors left holding a potentially worthless stock, but the criminals may even charge them a percentage for their advice and claiming to protect them against losses.

What you can do to prevent these scams:

- **Listen carefully and ask questions:** Clients may not immediately understand that they've been targeted. If a client mentions an investment opportunity received via social media or messaging apps, probe further.
- **Be attentive to mentions of:** unexpected fees, new accounts, too-good-to-be-true investment opportunities, initiating out of character transactions.
- **To avoid detection,** fraudsters may manipulate clients into initiating transactions without contacting their advisor—in some cases, the perpetrators offer scripts telling victims what to say if questioned about their activities.
- **Educate and advise:** Remind clients to be wary of unsolicited investment offers and check the credentials of anyone promoting stocks. And if clients receive any suspicious communications, remind them never to click on links or call numbers in that message.
- **Take digital precautions:** Encourage clients to choose heightened security options on messaging apps to prevent strangers from adding them to group chats.
- **Document and report the interaction:** Clients should report all details of the suspicious communications—including links or phone numbers—to your firm and the Schwab Alliance team at **800-515-2157**.

Remember: Sharing information about current fraud trends with your staff and clients is the best defense to prevent future incidents.

Resources:

Find tools and resources for your firm and clients on the [Fraud Prevention](#) site of the [Cybersecurity Resource Center](#).

Clients can visit [SchwabSafe](#) [🔗](#) for guidance on recognizing phishing attacks. Also, encourage them to report fraudulent phishing messages to the platform the message appeared on, as well as to us at phishing@schwab.com—including the suspicious emails themselves, as well as images of any questionable text messages.

Read about privacy at Schwab at www.schwab.com/privacy.

For general informational and educational purposes only.

This material is for institutional investor use only. This material may not be forwarded or made available, in part or in whole, to any party that is not an institutional investor.

Schwab Advisor Services™ provides custody, trading, and the support services of Charles Schwab & Co., Inc. ("Schwab"), member SIPC, to independent investment advisors and Charles Schwab Investment Management, Inc. ("CSIM"). Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

© 2025 Charles Schwab & Co., Inc. ("Schwab") All rights reserved. Member [SIPC](#) .

Own your tomorrow.