

## PRACTICE AND CLIENT MANAGEMENT

# Online scams are growing, but advisors can help protect clients

By [Amanda Chen](#) July 30, 2025, 1:58 p.m. EDT 5 Min Read



Kamitana - stock.adobe.com

What starts with a casual text message might end in financial ruin.

Pig butchering, a type of scam that became widespread during the COVID-19 pandemic, is on the rise and continues to evolve. It begins with a [fraudulent message](#) – often designed to look like it's from a friend, family member or a trusted company, or a potential romantic interest – and ends with the victim being manipulated into turning over their [savings](#).

# Financial Planning

"Before you say, 'I wouldn't fall for this,' [it] doesn't matter if you would or you wouldn't," said Erin West, the founder of Operation Shamrock, a nonprofit that combats online scams, during a North American Securities Administrators Association webinar earlier this month. "I guarantee you know somebody that this has happened to."

AARP recently reported that nearly [41% of American adults](#) have lost money to fraud. And in its latest annual release on internet crime, the FBI said that victims reported losing [\\$6.5 billion](#) in 2024 to online cryptocurrency fraud alone; total losses exceeded \$16 billion, with people over 60 submitting the most complaints and suffering the most losses, at nearly \$5 billion. And blockchain data platform Chainalysis found that fraudsters' hauls from pig butchering scams, specifically, [increased 40% year-over-year](#) in 2024.

READ MORE: [Rising scam risk calls for coordinated prevention strategy, study says](#)

---

## Advances in Tech

Learn about some of the latest software and technologies that are helping financial planning professionals move forward. Discover how you can better help...

### FINANCIAL PLANNING

---

## How scams work: Establish contact and trust — then exploit

The cycle of pig butchering follows a "textbook" pattern, West said during the webinar. Scammers often start by sending [text messages](#) that look like package delivery updates, government notices, job offers or messages from someone the victim hasn't heard from in a while. They might also send direct messages through social media using a fake profile or add a potential victim to group chats. These communications often span different messaging apps and might contain links that install malware on devices if clicked.

Once a victim responds to a message, the scammers will slowly cultivate trust. One way they do this is by grooming the victim to enter an online romantic relationship. In their communications, the scammers often show off signs of wealth or drop hints about how they've supposedly made money through cryptocurrency. After gaining a victim's trust, scammers then aim for their savings, often guiding a victim step-by-step on how to transfer their money, often into a [crypto](#) exchange platform.

Generally, the scammer sends the victim a link to the trading platform, which they control on the back end. Because victims initially see their balance grow, they continue to transfer more money into the platform. But eventually, when they try to withdraw, the platform will prohibit them from doing so, saying they owe tax and management fees. By that point, their money is gone, under the scammers' control.

READ MORE: [FINRA warns of AI use in sophisticated scams](#)

"This is not just a crime where you've had a lot of money stolen from you because you thought you were investing in it," West said. "This is also a crime where you've entered into a relationship that is very real to you and made you think you found the love of your life, so there's a double sense of shame for people."

## Victims on the other side of the keyboard as well

West said during the NASAA event that pig butchering is a massive criminal industry, primarily run by Chinese organized crime networks in countries like Cambodia and Myanmar. After COVID-19 disrupted Myanmar's economy, many buildings were repurposed into [scam compounds](#).

But there are victims on both sides of the equation, West said. Those sending the phishing and romance scam messages that aim to trick investors into turning over their savings may well be victims of human trafficking from Africa or Southeast Asia, lured by ads promising high-paying tech or data entry jobs. West described a man from Uganda who said he was trafficked into Cambodia after he was told that he would be paid \$1,000 per month for a legitimate job. Upon

# Financial Planning

READ MORE: [AI scams are getting harder to spot. How advisors can help](#)

"It is beyond what you can imagine," West said. "This is like nothing you've ever seen before, but it is jaw dropping the size and scale of what's happening."

## What can financial advisors do?

The first major red flag that a client may be a scam victim is that they are suddenly withdrawing large sums of money frequently, said Kashif Ahmed, the founder and president of American Private Wealth, who spoke to FP independently of the NASAA webinar.

"If they've never done it on their own before and all of a sudden you start seeing transactions that's happening, reach out and say 'Hey, I noticed this. Did you initiate this? What is it for?'" he said.

He said that financial advisors shouldn't feel intrusive about starting this conversation, but that they remain nonjudgmental and explain that they are just trying to [protect the client's assets](#).

"Just be very straightforward [because] it happens to a lot of people," Ahmed said. "But now that it has happened, let's try to fix as much as we possibly can."

READ MORE: [How advisors can protect older clients from financial scams](#)

If a client has already lost money to a scam, law enforcement may not be able to provide much assistance, as these scams often operate internationally. West suggested that victims who feel overlooked by law enforcement can report their experiences to Operation Shamrock, AARP Fraud Watch Network, Identity Theft Resource Center and Better Business Bureau, all of which can provide further guidance and offer emotional support.

Ahmed added that if a client's accounts have been hacked, the advisor should immediately alert the credit agencies and shut down the account.

"Even when they realize that they've been a victim of this, they're ashamed to admit it," Ahmed said. "If you're a good financial advisor, you should instill in the clients that 'I am on your side. I am here to take care of you.'"

Amanda Chen Reporter

---

For reprint and licensing requests for this article, [click here](#).

---

[PRACTICE AND CLIENT MANAGEMENT](#) [REGULATION AND COMPLIANCE](#) [FRAUD DETECTION](#) [FRAUD PREVENTION](#) [FRAUD](#)