BROADHURST
Financial Advisors, Inc.

Tales of Fraud

April 01, 2025

A recent survey of more than 1,000 financial planners asked whether they had experienced any attempted or real scams with their clients. Many had and reported varying levels of success dealing with what appears to be a dramatic upsurge in sophisticated ways to separate people from their assets.

The stories were remarkably diverse, although they can be put into categories. The simplest were people posing as advisor clients, asking for money. In many cases, they had hacked into the clients' email accounts, so they were able to provide recent information and comfortably refer to past email exchanges between advisor and client. Fortunately, most firms have checks and balances in place; they call the client to make sure this is an actual request, and an increasing number of advisors have assigned a code word that only they and their individual clients know about. If the scammer can't provide that secret code, the money remains safely where it belongs.

Another category is financial abuse by a family member, and the victim is often elderly. In one case, a family caregiver was bullying her elderly mother into signing over assets and putting her name on the mother's checking account, so she could write increasingly large checks to deposit in her own account. Another caregiver had her mother take out a home equity line of credit and absconded with the funds. After a female client's spouse passed away, a black sheep son moved in (uninvited) with his girlfriend and forced her to sign over the deed to the house. This last story had a happy ending; an elder law attorney threatened the son with charges of elder abuse, and the home ownership was returned.

Other similar stories involve caretakers or even 'helpful' neighbors, who seem to be offering care, but are actually stealing valuable collectibles or paintings off the walls. An advisor who has dealt with these cases has recommended that, when an elderly person begins receiving home care, take videos of the home and record all valuable items, which might make it easier to trace who was in the home when an item went missing.

Some of the most disturbing—and embarrassing—scams would start with an urgent phone call from somebody posing as an authority. In one case, the scammer pretended to be the local sheriff, calling to tell an elderly couple that they had missed jury duty twice, and were therefore subject to incarceration. But the caller assured them that he could take care of it with a simple payment of a $4,000 fine that the couple paid. More seriously, a scammer pretended to be an investigator with the Federal Trade Commission, who had gotten the victim's name, employee number, phone number and Social Security number off the Dark Web. The victim was told that the government was going to shut down his account, but he could avoid that by transferring the assets into a new account. That victim lost $200,000, but fortunately his financial planner prevented him from sending out another $1 million to the scammer's account.

Yet another category might be labeled 'bank errors.' In one case, a client received an unexpected—and large—check. It was too much money to leave lying around, so he deposited the check and tried to figure out what it was for.

He didn't have to wait long. He received a call from someone identifying himself as a bank executive, who said that the check was a mistake, and the client needed to pay the whole amount back. The client wrote a check, not realizing that in five days that original check would bounce.

A more insidious story involved a fraudster posing as a bank investigator, who asked the client whether he had made a large credit card purchase in a foreign country. Of course, the answer was no. The fraudulent bank investigator assured the victim that he would take care of it; all he needed was for this person to click on a link he was sending and log into his (the victim's) bank account. Of course, the link took the victim to a plausible looking (but bogus) bank home page, where the victim input his user name and password.

Now the fraudster had the victim's credentials to get into his account—but he still needed the third-party authorization code. He gave instructions to re-deposit a certain amount (in this case $16,000) but when the client hit 'enter,' this immediately turned into $160,000. The fraudster expressed shock, advised the victim to close out of the website, and go back into his account to reverse the transaction. This time the client entered his credentials into the real banking website, and the fraudster asked for the third-party authorization code so he could correct the situation personally.

At that point, he had full access to the victim's bank account, and he made short work of it.

A number of the stories involved a surprise phone call informing the victim that he or she has just won the Jamaican lottery—which is a real surprise since the victim had never purchased a ticket. But in order to receive millions of dollars, the victim will have to pay just $10,000 or

$15,000 to cover the local taxes—and of course after the 'taxes' are paid, the lottery money never shows up.

The final category is remote romances, where the victim is wooed by a romantic individual who he or she has never actually met, but who plans for them to meet as soon as the romantic individual is able to get clear of a nasty financial obligation—and could the victim help out so they can get together? This accounted for a surprisingly high number of cases; smart people who otherwise wouldn't be fooled by one of the aforementioned scams will do what they can to help, look forward to getting together in person, and never see the money again.

There's no easy way to keep people from being fooled by the growing sophistication of these scams, but the advisors who experienced these unfortunate events offer some real-world advice. One best practice is to only keep as much money as is actually needed in the checking account; money in a custodial account, under the watch of a financial planner, will have another pair of eyes on the requests for money, and in many cases the advisor can contact a son or daughter to come into the situation and evaluate the validity of the FTC examiner or bank executive before any money goes out the door.

Another is to monitor any caregiver or home health nurse—a job that typically falls on the more responsible children in the family.

Finally, where a person is convinced that an implausible scam is real, the best practice is to bring in as many other sets of eyes on the situation as possible—ideally a family meeting, with the financial planner and perhaps the victim's accountant. Many of these stories fall apart when the victim has to try to defend them logically.

The overarching lesson is that the world is becoming increasingly dangerous to innocent, generally nice, helping people, as a new ecosystem of sophisticated scammers trolls for victims. The more awareness we can muster, the harder it will be for them to make off with peoples' hard-earned dollars.

Sources:

https://bobveres.com/december-2024/

If you have any questions about this article or want to discuss your family finances, investment portfolio, or financial planning advice, please call on me anytime at my number (215) 325-1595 or you can click here to schedule a meeting.

Please feel free to forward this article and offer to anyone you know who might have financial questions or need some unbiased advice. Most financial advice is sales advice. In stark contrast, we are fee-only (non-commissioned) fiduciary advisors. We just provide truthful, unbiased advice to our clients.

Jeffrey Broadhurst
MBA, CFA, CFP
Broadhurst Financial Advisors, Inc.

PRIVACY NOTICE

Our physical and mail address:
1911 West Point Pike
P.O. Box 301
West Point, PA 19486-0301

Contact us:
Phone: (215) 325-1595
Email: jeff@broadhurstfinancial.com