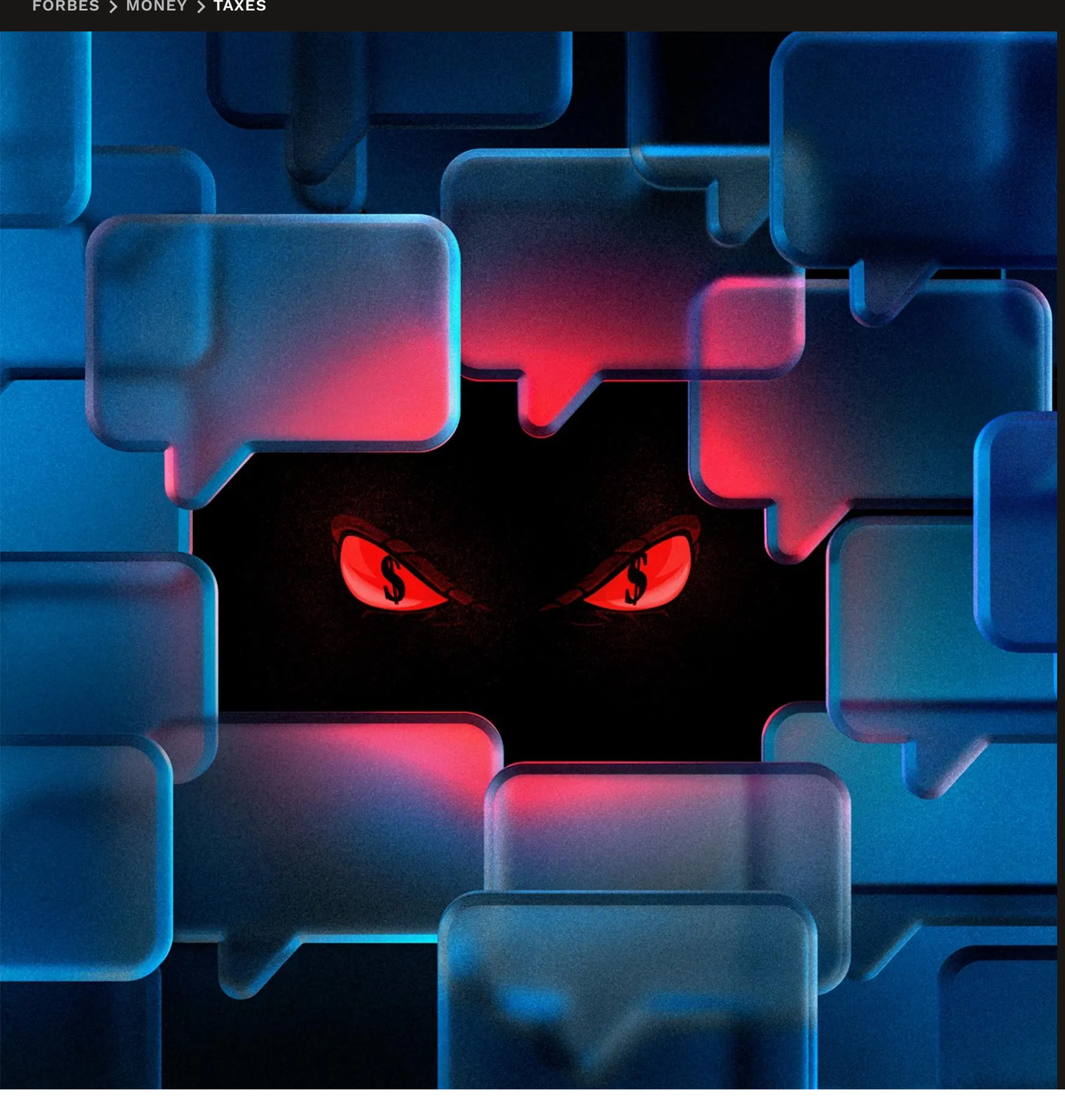

PREMIUM • DAILY COVER

How To Prevent Grandma, Grandpa–And Yourself–From Getting Ripped Off Online

ILLUSTRATION BY ALEX CASTRO FOR FORBES; PHOTO BY ISTOCK / GETTY IMAGES

Aug 17, 2024, 06:30am EDT
Updated Aug 19, 2024, 09:31am EDT

Elder fraud is exploding, while crypto and speedy money transfers are making it tougher to recover stolen funds. Here are tips for staying safe.

By Kelly Phillips Erb, Forbes Staff

The call began with a seemingly routine request. "I was wondering if you could help me with an international inheritance case," the older woman said. She'd searched on Google for an "international estate lawyer" and since she lives near me in southeastern Pennsylvania, my name had popped up. (While I'm the senior tax writer at Forbes, I'm also an estate and tax lawyer and still practice a bit on the side.)

Then the alarm bells sounded. The woman confided she was trying to settle a foreign estate *for a friend*. Carol (as we'll call her, since she asked we protect her identity) explained her friend's father had died 20 years ago while working in England, but her friend, his sole heir, hadn't been able to access the funds in his estate. The son lived in the United States and the laws in England, he told her, required that he find a third party to act as an intermediary. He asked Carol to help out by fronting some cash for legal bills and putting money in as a sort of "escrow" for the transfer. She felt sorry for him. Plus, he was offering to pay her back with a share of his inheritance, once he got it.

When Carol asked for the name of the person handling the estate, the friend gave her a business card for a barrister with a London office. It didn't look like a traditional business card and a quick Google search showed the address it listed was a home, not an office building. I pointed out that the average estate in the U.S. takes just two years to administer and if the money was guaranteed to ultimately go to her friend—as he said it was—a good attorney would be willing to work with the heir, maybe even delaying his fee.

It smelled like a scam, I told Carol. Her voice–and the fact that she had been smart and wary enough to reach out–suggested she had suspected as much. Yet she was still too invested in the friendship to accept that conclusion. She had met this young friend online three months ago in a chat group, and they'd been texting since. They'd even met once in person.

The next day, Carol called with new information for me to check out. Her friend had turned over a copy of a document from "the High Court of Justice from London, England" that was supposedly issued 20 years ago and looked similar to the "Letters of Administration" a U.S. court issues if a person dies without a will.

There were several red flags on the document. It gave her friend the right to administer the estate, even though he would have been a minor at the time of his purported father's death. It included an address for the son at a New Jersey apartment building that wasn't around 20 years ago. Plus, it listed specific assets (not something that you'd normally see on Letters of Administration), including shares in a Russian oil company and properties in Russia and Dubai that "cannot be liquidated by the HM Treasury"—an odd description meant to give credence to the idea that a third party had to step in to effect the international transfers.

Despite the fancy stamps and signatures, the document appeared fake. I urged Carol to reach out to law enforcement. She hesitated. "I'll bet he has told you that I don't know what I'm talking about," I said. "That's exactly what he said," she responded. His suggestion was that I couldn't know about English law because I'm an American lawyer.

I offered to contact an attorney in England for yet another opinion. Steen Rosenfalck, a partner at EBL Miller Rosenfalck, which has offices in London, confirmed that the document was fake. He cited the use of the word "inheritor" (a term that it turns out isn't used on English probate documents) and a mistake in the title of the document; the correct terminology in both the U.S. and England is "Letters of Administration" but the document said Letter, singular. (Both Rosenfalck and I helped Carol pro bono–meaning, for free)

With confirmation from England, Carol accepted the unpleasant truth about her faux friend.

She had been the intended victim of a "pigeon drop"—a centuries old scam in which the victim is persuaded to pay over a small amount of money in order to get a larger sum. In the old days, a fraudster might claim to have found a valuable object such as a ring on the ground and ask a stranger passing by to help him sell it. The mark would be offered a share of the proceeds, and asked to put up good faith money as a security deposit for taking possession of the ring. In the 1990s, a flood of emails from "Nigerian princes" expecting inheritances became synonymous with the pigeon drop scam, which the Federal Bureau of Investigation (FBI) calls "advance fee fraud." This decade, fraudsters are using texting to develop relationships with marks for pigeon drops, as well as for various crypto and investment frauds.

Online scams targeting individuals aged 60 and older—often called "elder fraud"—have been exploding, causing more than $3.4 billion in losses in 2023, up from $1.7 billion in 2021 and $835 million in 2019, according to the FBI Internet Crime Complaint Center (IC3). The average loss reported for 101,068 older victims in 2023 was $33,915, with 5,920 losing more than $100,000.

Those numbers capture the rapid growth of the problem, but vastly understate its full scale, since many scams are never reported and only about half of the complaints IC3 received in 2023 included the age of the victim. But when ages are reported, older folks are the biggest losers. That's because they have the most assets to lose and are sometimes more vulnerable for other reasons, including social isolation, cognitive changes, a desire among older folks to be helpful and the fact that while seniors are now mostly online, they're not necessarily the most internet savvy. (According to Pew Research Center, 76% of U.S. adults 65 and older have smart phones and 70% have home broadband.)

Tellingly, older folks are particularly susceptible to tech support schemes. Scammers target a home computer or cell phone with pop-up windows or texts, advising that there is a security flaw that you need to fix—typically by calling a number that they provide. Once they have their mark on the line, they'll ask for money to address the problem, or even more dangerously, remote access to the victim's computer.

But the biggest reported online losses for seniors in 2023 came from investment scams, these days often involving cryptocurrency or real estate. The scammer meets a potential victim online (say, through a dating or social media app or a seemingly random "wrong number" text) and begins to build a relationship. Eventually, the talk turns to the opportunity to get into some "proven" or "risk-free" investment strategy. A small upfront investment can turn into a bigger one as the scammer produces assurances and even fake records showing how well the initial investment is doing. This long-con game has become so prevalent that it's got its own nickname–pig-butchering.

Also inflating losses: the increasing speed with which funds are moved–from bank account to bank account, out of the U.S., or into crypto. The IC3 has a special asset recovery team that can freeze allegedly stolen funds quickly if they're still in a U.S. bank. In 2023 that team recovered a paltry $32 million. Once cash leaves a victim's account, it's often moved into multiple accounts and then out of the country within 24 hours, making it very difficult to trace, says Matt O'Neill, a security consultant who spent more than 25 years in the U.S. Secret Service.

Zelle, the banks' fast growing quick money transfer app (it's run by Early Warning Services, a fintech co-owned by JPMorgan Chase, Bank of America, Capital One, PNC Bank, Truist, U.S. Bank and Wells Fargo), has faced Senate scrutiny for doing too little to protect or reimburse victims of fraud. At a hearing last month, the banks defended their fraud prevention efforts and pointed out they warn customers to only use Zelle to send money to people they know and trust. Bank of America, for example, provides this speed-bump message before every transaction: "This payment is like cash, and the money you send is unlikely to be recovered…Don't send money as a result of an unexpected call or text."

An even bigger problem: According to IC3 reports, online fraudsters used cryptocurrency or crypto wallets as tools to move money in almost half the 2023 losses 60-plus victims sustained, up from under 15% in 2021.

With money disappearing so fast, the only real defense is to head robbers off before they get their hands on your (or a loved one's) money. Knowing the warning signs of fraud is crucial (we'll spell some out below), but so too is having another person do a gut-check, as happened in Carol's case.

One arguably underutilized option: the "trusted contact." Since 2018, the Financial Industry Regulatory Authority (FINRA) has required investment companies to ask customers whether they'd like to designate another adult the firm can reach out to. This trusted contact doesn't control a customer's accounts or even usually have the ability to see what's in them. But the investment company can contact this designee if they see suspicious activity in an account and can't reach its owner or if they suspect a senior is being financially exploited or suffering from cognitive decline. (Current FINRA rules also permit financial firms to put a hold on funds for up to 55 days if they suspect someone over 65 if being defrauded, but don't count on this happening.)

While banks and credit unions aren't required to ask for a trusted contact name, the Consumer Financial Protection Bureau (CFPB) reports more are offering customers the option. (Be sure to read the form and see what you're agreeing to.)

A slightly more intrusive backstop is offered at some financial firms. For example, both Fidelity Investments and The Vanguard Group allow you to give another customer "view only" access to see your accounts, but not make transactions in them.

Both these options cede less control than giving a child or someone else a power of attorney over your account. A POA holder can make transactions. That can be helpful, but keep in mind that family financial exploitation of elders is itself a big problem. The CFPB suggests that if one person has authority to make transactions in your account, you consider naming a different one as a trusted contact for a financial institution to reach out to if something the POA does looks suspicious.

Whatever you do, don't just tack the name of a child or friend onto your account as a joint account owner–in addition to the trust issues with a POA, this approach can have nasty tax consequences and could undermine the intended distribution of assets if one account owner dies.

Some of the red flags to watch out for when it comes to online financial fraud are new, while others have long applied whether you're being pitched an investment by phone, mail or in person—say at the country club or church. Be wary if:

- ***Promised returns sound too good to be true.*** That tried but true advice is offered by Raj Dasgupta, a senior director at BioCatch, a tech company which uses the latest behavioral biometrics to assist financial institutions to more effectively fight fraud.
- ***You're asked to keep secrets.*** Seniors will often be "manipulated into believing they are assisting a legitimate cause," says O'Neill, and urged not to tell family members, their financial advisor or authorities. For example, in one common tactic, the fraudsters will tell their target that they've already been victimized and are helping to secretly investigate the crime.
- ***You're told to wire money, send bitcoin, or buy gift cards to pay taxes, tickets, or attorney's fees.*** Scammers may ask you to pay by unconventional means so they can launder money quickly.
- ***You receive a phone call or text from what seems to be an official number.*** Scams often begin with communication from someone claiming to be from the IRS, the Social Security Administration, or your bank. If you believe it's a legitimate call, say you'll call them back—then call a trusted, direct number. (Don't simply use caller ID or a number provided to you by the caller, as those may be "spoofed" to trick you.)
- ***You're pressured to act fast.*** Fraudsters often employ a sense of urgency or heightened pressure to prompt immediate action from their targets.
- ***You're asked to help someone that you've never met in person.*** A key to online fraud is scammers' ability to create a sense that you know them, when you don't.
- ***You receive communications or documents that include multiple typos or poor English.*** Look, too, for indications that scammers may be trying to shoehorn official terms into a fake document, like referring to the "Bureau of Internal Revenue"—that's not the IRS. Be aware, however, that with artificial intelligence, it's easier than ever for scammers (even those based abroad) to clean up their grammar and accurately mimic official titles and communications.

If you know you've fallen for a fraudulent scheme, immediately stop communicating with the scammer. If you've turned over personal information, change your passwords, consider closing your accounts, and start monitoring your bank and other personal accounts for suspicious activity.

Finally, immediately report bad behavior, which many scam victims never do. You just might get some money recovered–or at least help protect the next victim. You can call the National Elder Fraud Hotline at 1.833.FRAUD11 (1-833–372–8311) Monday through Friday, 10:00 a.m. to 6:00 p.m. Eastern time; file a report online with the IC3; or contact any IRS-Criminal Investigation field offices (see p.22 of the annual report to find an office near you)–since CI agents are trained to "follow the money," they often play a key role in investigating financial fraud.

Follow me on Twitter or LinkedIn. Send me a secure tip.

Kelly Phillips Erb
Following

Kelly Phillips Erb is a Philadelphia-area Forbes senior writer who covers tax and financial crimes. As a tax attorney, Phillips Erb brings a legal perspective to her tax coverage. This has… **Read More**