The Top 5 Financial Scams Targeting Older Adults

By Genevieve Waterman, Director, Economic and Financial Security – National Council on Aging

Key Takeaways

Scams targeting older adults are on the rise. In 2021, there were 92,371 older victims of fraud resulting in $1.7 billion in losses.

The most common financial scams targeting older people include government impersonation scams, sweepstakes scams, and robocall scams.

Financial crimes against older adults can be devastating, often leaving victims with no way to recoup their losses. Learn how to identify and stop the top 5 financial scams targeting seniors.

Financial scams targeting older adults are costly, widespread, and on the rise. According to the Federal Bureau of Investigation (FBI), in 2021 there were 92,371 older victims of fraud resulting in $1.7 billion in losses. This was a 74% increase in losses compared to 2020.[1]

Why do financial scammers target seniors?

Fraudsters and con artists tend to go after older adults because they believe this population has plenty of money in the bank. But it's not just wealthy older Americans who are targeted. Older adults with low income are also at risk for fraud.

Financial scams often go unreported or can be tough to prosecute, so they're viewed as a "low-risk" crime. However, they're devastating to many older adults and can leave them in a vulnerable position, with limited ability to recover their losses.

How common are financial scams targeting older adults?

In the five-year period ending December 31, 2020, the U.S. Senate Special Committee on Aging Fraud Hotline received more than 8,000 complaints nationwide.
The five scams outlined below made up more than 65% of these complaints.[2]

Government impersonation scams

In government impersonation scams (also known as government imposter scams), scammers call unsuspecting older adults and pretend to be from the Internal Revenue

Service (IRS), Social Security Administration, or Medicare. They may say the victim has unpaid taxes and threaten arrest or deportation if they don't pay up immediately. Or they may say Social Security or Medicare benefits will be cut off if the victim doesn't provide personal identifying information. This information can then be used to commit identity theft.

Government imposters may demand specific forms of payment, such as a prepaid debit card, cash, or wire transfer. Using special technology, they often "spoof" the actual phone number of a government agency or call from the same zip code (202 for Washington, D.C., for example). This can trick some people into thinking the caller is from a valid source.

Sweepstakes and lottery scams

The sweepstakes scam is one many people are familiar with. Here, scammers call an older adult to tell them they've won a lottery or prize of some kind. If they want to claim their winnings, the older adult must send money, cash, or gift cards up front—sometimes thousands of dollars' worth—to cover supposed taxes and processing fees.

Scammers may impersonate well-known sweepstakes organizations (like Publishers Clearing House) to build trust among their victims. Of course, no prize is ever delivered. Sometimes, fraudsters are able to convince the older adult to send even more money by telling them their winnings will arrive soon. Many continue to call their victims for months and even years after defrauding them out of an initial sum of money.

Robocalls and phone scams

One common robocall is the "Can you hear me?" call. When the older person says "yes," the scammer records their voice and hangs up.

Robocalls take advantage of sophisticated, automated phone technology to dial large numbers of households from anywhere in the world. While there are legal uses for this technology, robocalls can also be used to carry out a variety of scams on trusting older adults who answer the phone. Some robocalls may claim that a warranty is expiring on the victim's car or electronic device, and payment is needed to renew it. Like with government impersonation calls, scammers often spoof the number from which they're calling to make it appear as if the call is from a reputed organization.

One common robocall is the "Can you hear me?" call. When the older person says "yes," the scammer records their voice and hangs up. The criminal then has a voice signature to authorize unwanted charges on items like stolen credit cards.

Yet another popular phone scam is the "impending lawsuit" scam. In this case, the victim receives an urgent, frightening call from someone claiming to be from a

government or law enforcement agency (like the police). They are told if they don't pay a fine by a certain deadline, they will be sued or arrested for some made-up offense.

Computer tech support scams

Technical support scams prey on older people's lack of knowledge about computers and cybersecurity. A pop-up message or blank screen usually appears on a computer or phone, telling the victim their device is damaged and needs fixing. When they call the support number for help, the scammer may either request remote access to the older person's computer and/or demand they pay a fee to have it repaired. In 2021, the Internet Crime Complaint Center (IC3) fielded 13,900 tech support fraud complaints from older victims who suffered nearly $238 million in losses.[1]

"Tech support fraud is increasingly common and targets some of the most vulnerable individuals. Above all, remember that whether it's a phone call or a website, legitimate tech support won't ever proactively seek you out to fix an issue," said Emma McGowan, a privacy and Security expert at Avast.

Behind the numbers are real people who have endured devastating losses at the hands of cybercriminals. In 2021, a man from Illinois lost his life savings to scammers pretending to be an employee of a known antivirus company. Under the guise of giving the man a refund for unused software, these scam artists gained remote access to his bank account and home equity line of credit. They ultimately made away with nearly $200,000—money that was never recovered.

If you're wondering how to avoid tech support scams, there are a number of things you can do. Learn how to protect yourself and if you suspect you've been a victim, follow these steps from our partner Avast.

The grandparent scam

The grandparent scam is so simple and so devious because it uses one of older adults' most reliable assets, their hearts. Scammers call a would-be grandparent and say something along the lines of: "Hi, Grandma, do you know who this is?" When the unaware grandparent guesses the name of the grandchild the scammer most sounds like, the scammer is able to instantly secure their trust. The fake grandchild then asks for money to solve some urgent financial problem (such as overdue rent, car repairs, or jail bond). They may beg the grandparent not to tell anyone. Since fraudsters often ask to be paid via gift cards or money transfer, which don't always require identification to collect, the older adult may have no way of ever recovering their money.

In other versions of this scam, the caller claims to be an arresting police officer, doctor, or lawyer trying to help the grandchild. They then use high-pressure tactics that play on the emotions of their victim to get them to send cash as quickly as possible. There are

even reports of scammers showing up at older adults' homes, posing as a "courier" to pick up the money.

Other popular scams targeting older adults

Romance scams

As more people turn to online dating, con artists are seizing the opportunity. Romance scammers create elaborate fake profiles, often on social media, and exploit older adults' loneliness to get money. In some cases, these scammers may be (or pretend to be) overseas. They may request money to pay for visas, medical emergencies, and travel expenses to come visit the U.S. Since they tend to drag on for a long time, romance scams (also called sweetheart scams) can bilk an older person out of substantial funds. The FTC found that in 2020 alone, older adults lost $304 million to romance scams.[3] Get tips for avoiding sweetheart scams.

COVID-19 scams

By June 2021, the FTC had already logged more than 500,000 consumer complaints related to COVID-19 and stimulus payments. Seventy-three percent of those complaints involved fraud and identity theft.[2] Examples of COVID-19 scams include:

So-called miracle cures: Some companies have fraudulently marketed products as a "cure" to COVID-19 infection. These products are not backed by medical evidence nor are they FDA-approved.

Vaccines: Scammers may call older people to offer vaccination in exchange for money or personal information. Please keep in mind that you can get vaccinated against COVID-19 at no cost and without providing your banking information. Learn how to avoid COVID vaccine scams.

COVID-19 testing: Some older adults have reported offers of "free" COVID-19 tests or supplies from people claiming to be from Medicare or the Department of Health and Human Services. These fraudsters then use the victim's Medicare information to submit false health care claims.

Investment scams

This type of scam involves the illegal or alleged sale of financial instruments that typically offer the victim low risk and guaranteed returns. Investment schemes were responsible for more than $239 million in losses suffered by people age 60 and older in 2021. The use of cryptocurrency (digital assets, such as Bitcoin) is common in investment scams. In 2021, cryptocurrency was the basis for more than 5,100 fraud complaints received by IC3.[1]

Medicare and health insurance scams

Every U.S. citizen or permanent resident over age 65 qualifies for Medicare, making the program a prime tool for fraud. In Medicare scams, con artists may pose as a Medicare representative to get older adults to share their personal information. Scammers might also provide bogus services for older people at makeshift mobile clinics, then bill Medicare and pocket the money. Medicare scams often follow the latest trends in medical research, such as genetic testing and COVID-19 vaccines.

Internet and email fraud

The slower rate of technology adoption among some older people makes them easier targets for internet and email scams. Pop-up browser windows that look like anti-virus software can fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that exposes information on the user's computer to scammers. Their unfamiliarity with the less visible aspects of browsing the web (firewalls and built-in virus protection, for example) makes older adults especially vulnerable to such traps.

Phishing emails and text messages may appear to be from a well-known bank, credit card company, or online store. They request an older adult's personal data, such as a log-in or Social Security number, to verify that person's account, or they ask the older adult to update their credit card info. Then, they use that information to steal money or more personal information. Find out how to protect yourself against phishing scams.

What to do if you think you've been the victim of a scam?

Scams are specially designed to catch us off guard, and they can happen to anyone. There's nothing to be ashamed of if you think you're a victim. Keep handy the phone numbers of resources that can help, including the local police, your bank (if money has been taken from your accounts), and Adult Protective Services. To obtain the contact information for Adult Protective Services in your area, call the Eldercare Locator, a government sponsored national resource line, at: 1-800-677-1116, or visit their website. You can also report scams online to the FTC. Sharing your experience can help prevent it from happening to another older adult.

Sources

2021 Elder Fraud Report, Federal Bureau of Investigation. Found on the internet at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf

Top 5 Scams Targeting Our Nation's Seniors Since 2015 (2021), U.S. Sentate Special Committee on Aging. Found on the internet at https://www.aging.senate.gov/imo/media/doc/Fraud%20Book%202021.pdf

Romance scams take record dollars in 2020, FTC Consumer Protection Data Spotlight. Found on the internet at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/02/romance-scams-take-record-dollars-2020