AICPA & CIMA
Together as the Association of International Certified Professional Accountants

FVS Eye on Fraud

The AICPA Forensic and Valuation Services quarterly report on fraud trends and topics

Evolution of elder fraud in the era of COVID-19

Issued by the AICPA® FLS Fraud Task Force
Lead authors: **Irina Balashova, CPA, CIA, CFE, and Howard Silverstone, MBE, CPA/CFF**

The actor and comedian Groucho Marx once said, "Getting older is no problem. You just have to live long enough." To that point, according to the U.S. Census Bureau, the population of those 65 and older has grown rapidly since 2010, mainly due to the aging of the baby boomer generation, those born between 1946 and 1964. Although the COVID-19 pandemic resulted in a higher death rate among older Americans, the growth of this demographic has continued. According to forecasts, by 2040, there will be almost 81 million Americans over age 65.

Summer 2022, Issue 3

Inside this issue

Having a larger population that is susceptible to elder fraud and abuse means that the potential of such schemes is also increasing. Elder abuse takes different forms but is broadly defined as action — or lack of appropriate action — toward an elderly person that intentionally harms them or puts them at risk of harm. The U.S. National Council on Aging recognizes seven types of elder abuse: physical, sexual, financial, emotional, neglect, self-neglect, and abandonment. Financial abuse occurs when someone takes money or assets from an older person without their consent, full knowledge, or understanding.

The 65-and-older population is particularly vulnerable to fraud for several reasons. Many older adults have less debt, or perhaps no debt, through a combination of accumulated retirement savings, pension, and investment income. Other seniors rely on a consistent income stream in the form of government retirement benefits. Irrespective of the source of funds, elders' money is a tempting target for many fraudsters.

Unfortunately, the aging process comes with health-related difficulties, often including mental challenges. A reduced capacity for judgment may result in flawed financial choices, making seniors more vulnerable to fraud than people in other age groups. The decline in mental capabilities does not happen abruptly, but instead comes as a gradual decrease in thinking and cognitive functioning. Affected elders and those around them do not immediately realize that the elders' judgment and ability to make decisions have been impacted. As a consequence, older people who maintain control over their financial resources and assets may become ideal potential victims for fraudsters.

According to the Alzheimer's Association, approximately 12% to 18% of people aged 60 or older are living with mild cognitive impairment. This is a condition that precedes the development of more profound cognitive diseases and may itself impair someone's daily life in many ways. For example, individuals diagnosed with mild cognitive impairment may experience forgetfulness or feel increasingly overwhelmed by making decisions and plans. They may have trouble understanding directions or instructions and lose the ability to organize tasks. The natural decline in health that accompanies aging and results in added vulnerability has been compounded by the many new challenges brought about by the COVID-19 pandemic. Among the additional risks are the following.

Increased isolation, anxiety, and depression

With the COVID-19 pandemic came a level of isolation that most had never experienced before. The COVID-19-related fatality rate for patients over 65 years old remains the highest of any age group, even after the introduction of vaccines. Unsurprisingly, older people have generally been more cautious and more vigilant about social distancing throughout the pandemic and, as such, have been among those most affected by social isolation.

Even though pandemic lockdowns and quarantining seem to be easing, many people have elected to continue isolating for a range of health and personal reasons. One study revealed that as many as 80% of seniors predicted they would be spending more time at home in the future compared to before the pandemic.

Psychology Today cites several studies linking increased isolation with the onset or increase of depression and anxiety. The link seems to be related to the fact that those who are isolated are less likely to experience much-needed affection, validation, and a sense of connection and, instead, may experience more negative feelings. These negative feelings, in turn, result in an increased risk of financial exploitation and fraud vulnerability.

Heavier reliance on technology

With isolation and the lack of in-person social contact, including with family, friends, and work circles, comes an increased reliance on technology, which has its risks. Many older people started using platforms like Zoom and FaceTime to stay in touch with their families and started using online resources to obtain goods and services, like groceries and household supplies.

Fraudsters have not missed the opportunity to leverage this additional avenue for fraud. Seniors are more connected to the internet than ever before and have become increasingly susceptible to fraud, as many are only just developing technical skills. The main points of vulnerability are inadequate protection of devices, including the use of simple passwords, if any; not using multi-factor authentication; clicking on infected links; trusting fraudulent promotions and offers; and volunteering credit or debit card information.

Increased need for medical help

The increased demand for health care services has led to new and expanding telehealth solutions. Even before the COVID-19 pandemic, telehealth was a growing segment of the health care industry. By 2019, over 90% of employer-sponsored health plans had started covering this form of medical care, and the American Bar Association (ABA) reported that, in April 2020, 43.5% of Medicare primary visits were done via telemedicine.[1] This growing field has become a target for fraudsters. According to the Department of Justice, health care fraud resulted in about $1.4 billion in losses by the end of 2021; the majority of reported cases were related to telemedicine. Some of these schemes lead patients to believe that they need testing that turns out to be unnecessary or result in patients receiving unlawfully prescribed drugs. According to the same ABA report mentioned earlier, other telehealth schemes include inflating time spent on services and billing for services not rendered, among others.

Rollover of government-supported programs

The U.S. government has initiated several relief programs since the beginning of the pandemic, including rental assistance, mortgage relief, tax credits, bill payment assistance, and medical coverage. It is estimated that by the end of 2022, the U.S. government will have spent over $4 trillion in response to COVID-19. Many of the programs were developed to directly support individuals, and over 14 million people received aid. This created an opportunity for fraudsters to swindle individuals using a variety of scam techniques.

Increased need for the latest medical information

Since the beginning of the COVID-19 pandemic, many have followed the news regarding the spread of the virus, the development of vaccines, and social distancing guidelines. Unfortunately, not all information outlets genuinely serve the purpose of informing the public. The evolution of COVID-19 testing, treatment options, vaccinations, and potential cures all have led to fraudsters using various channels to their benefit.

Fraud types that have increased during the COVID-19 pandemic

The FBI, in its 2021 Elder Fraud Report,[2] estimated financial abuse losses totaling $1.7 billion, which represented a 74% increase from 2020. According to the Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse of October 2021 and the 2021 report of the U.S. Senate Special Committee on Aging,[3] the following fraud schemes, among others, became more prevalent in 2020 and 2021.

Technical support fraud

This type of fraud is undertaken in several ways, but the first point of contact with the potential victim is usually a phone call or an email. Fraudsters pretend to be computer technicians associated with a well-known company or provider and claim that the computer of the victim is infected with malware or has other technical difficulties. A simple solution is then offered by way of allowing the "technician" remote access to the victim's computer. Thereafter, the fraudsters "diagnose" a nonexistent problem and ask for payment for unnecessary services, install malware, or both. Another potential loss associated with this type of scam is related to sensitive information. Personal information including an individual's Social Security number or banking details may be stolen. In June 2021, Romana Leyva pled guilty to conspiracy to commit wire fraud and conspiracy to intentionally damage a protected computer — he admitted that he was a leader of an organization that defrauded at least 7,500 victims for over $10 million over four years. He utilized pop-up messages to get victims' attention; the messages led them to believe that their computer was infected with malware. Then a linked phone number connected the victim to a member of the fraudster's team.

---

[1] Miranda Hooker, Allison DeLaurentis, Sharon Klein, and Jason Kurtyka, "Fraud Emerges as Telehealth Surges," *The White Collar Crime Committee Newsletter*, American Bar Association, Winter/Spring 2021, americanbar.org/content/dam/aba/publications/criminaljustice/2021/telehealth_fraud.pdf.

[2] Federal Bureau of Investigation, 2021 Elder Fraud Report, ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf.

[3] U.S. Department of Justice, Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse, October 2021, justice.gov/file/1443096/download?utm_medium=email&utm_source=govdelivery.

Romance fraud

Romance scams climbed sharply during the COVID-19 pandemic. This type of fraud is fueled by a sense of increased loneliness and isolation that disproportionately affects the older generation. In addition to isolating to avoid direct health threats, over the past two years, elders have had to cope with the efforts of their adult children and others to limit contact for their protection. There were no more visits from grandchildren, no more get-togethers with friends, and no more social or religious gatherings. Unsurprisingly, the longing for human connection has led many seniors to more extensive use of social media, where they may be preyed upon by fraudsters. The Federal Trade Commission estimated that losses from romance scams increased by about $50 million in 2020 compared to the previous year. Fraudsters first focus on building trust in an online relationship and then use their influence to convince potential victims to provide money, using plausible reasons including fake hospital bills, plane trips to facilitate an in-person meeting, or to address financial problems.

Grandparent fraud

This type of fraud takes advantage of family relationships and fear for loved ones' wellbeing. Fraudsters impersonate close relatives of potential victims and create a false sense of emergency. With the pandemic, scammers modified their pitch: instead of asking for money to tackle financial difficulties, they started claiming an emergent health situation like being in the hospital or needing expensive treatment. These cries for help fall on the unprotected and well-meaning ears of victims. Victims often do not stop to question whether the voice sounds familiar, whether the word selection is similar to that of someone in need, or whether the caller's story seems odd.

A simple call back to a familiar number to speak to the person being impersonated would reveal the scam, but fraudsters build a sense of urgency, convincing victims that they must act immediately or something terrible will happen to their child, grandchild, or other loved one. The Federal Trade Commission estimates that, in 2020, $1.2 billion in losses were due to imposter scams; that number increased by $1.1 billion in 2021.

Government imposter fraud

As noted earlier, government agencies introduced several new assistance programs to support people during the pandemic. Usually, government-imposter fraud starts with the scammer contacting the potential victim and posing as a government agent. One of several scenarios then plays out. The fraudster may claim to be an IRS agent and request payment of alleged back taxes due. They may impersonate Medicare or Medicaid representatives and demand payment on past-due medical bills or state that they are from the Social Security Administration and need additional personal information to process benefits. All these schemes have one thing in common — impersonating a government official to request immediate payment or obtain personal information. Psychologically, older victims may be less equipped to withstand this type of fraud because they tend to have more respect for authority than those in other age groups.

In April 2021, Darlens Renard and four others were convicted in Indiana for carrying out an enormous grandparent scam, defrauding at least 60 older victims for at least $350,000 in total.[4] A separate but similar incident involved a scammer defrauding an elderly individual by telling her that her daughter had been in an accident and was in legal trouble as a result. The scammer claimed that she needed over $10,000 to settle the claim in person before it escalated. Importantly, the scammer instructed the victim to keep silent, obviously understanding that this type of fraud is easy to expose if the story is shared with family members. Another victim was presented with a story of an alleged motor vehicle accident that resulted in bad injuries to children in the other car.[5]

We have discussed a few of the most prominent scams, but there are several other fraud schemes that the elderly should be aware of, including telemarketing fraud, lottery and sweepstakes fraud, and identity theft.

Action plan

The COVID-19 pandemic created a unique landscape of opportunity for fraudsters. Because of this increased risk, members of the professional community have an increased responsibility to protect the vulnerable. An action plan may include the following programs and other recommendations.

[4] United States Attorney's Office, Sourthern District of Indiana, Five Face Federal Charges for Alleged Nationwide Elder Fraud Scam, U.S. Department of Justice, March 24, 2021, justice.gov/usao-sdin/pr/five-face-federal-charges-alleged-nationwide-elder-fraud-scam.

[5] Ibid.

Public outreach

Even though the problem of elder fraud has received additional attention in recent years, there is still significant underreporting, and the true extent of such fraud is likely higher than statistics suggest. It is estimated that over 80% of all fraud cases targeting the older population are never prosecuted, and consequently, scammers are not stopped or punished. Such significant underreporting occurs because victims do not have social support, are scared, or lack knowledge, including knowledge about how to report fraud to the authorities. Therefore, the first and most important task in preventing elder fraud is disseminating relevant information to the public. Numerous resources (including those listed later in this article) are available to older adults, caregivers, family members, and professionals. Raising awareness is the foundation for reducing instances of fraud.

Help your clients, family, and friends avoid scams

You can help your own advising clients, family members, and friends avoid scams by sharing some simple tips and advice, such as the following:

- Do not respond to calls or texts from unknown numbers.
- Be careful clicking on links in emails or advertising banners on web pages.
- Avoid sharing your personal information, including your address, Social Security number and passwords.
- If something looks suspicious, it probably is — look for red flags, including words indicating urgency, a demand for immediate action, or a caller acting distressed.
- It never hurts to double-check information by doing research or talking to someone.
- Extreme situations create psychological distress, emotional vulnerability, and impaired judgment. Fraudsters know this. Be especially cautious if you receive news that sounds extremely good (for example, winning the lottery) or extremely bad (for instance, a relative is in trouble).

How CPAs can help

As CPAs, we know that quality client service starts with active listening. Here are some additional tips for assisting your older clients:

- Subtle clues can convey more than words, and social interactions can be valuable in identifying financial vulnerabilities.
- Know the signs of cognitive decline and how to spot them in your clients. Timely discussions with an elderly client may help prevent future troubles.
- Be ready to share various resources (such as those listed later), if needed.
- Be aware that one of the best ways to connect with and warn a potential victim of a dangerous financial situation is through storytelling. At the end of this article is a list of resources available to learn about real-world fraud cases, including details of mistakes victims make that leave them especially vulnerable. Familiarize yourself with these accounts so that you can pass on the lessons learned to your clients.
- Identify and discuss with clients any increases or decreases in spending, unusual expenses, changes in bank account practices, or changes in ownership of assets.
- Be alert to other red flags including unauthorized withdrawals using an ATM or debit card, unpaid bills, unexplained fund transfers, or the emergence of previously inattentive relatives claiming control over the elder's financial matters. CPAs are equipped with a unique set of knowledge that helps them identify the many red flags indicating potential financial abuse. For example, if you provide routine and recurring services to a client, any change should be viewed as a potential concern.

Government resources

Government agencies are aware of the fraud problem and have developed fraud-fighting tools, including hotlines and educational materials, to help individuals. The following are some of the government resources available:

- U.S. Department of Health and Human Services Office of Inspector General's Operation CARE. This is a set of programs and resources developed to fight elder fraud.
- The U.S. Department of Justice Elder Justice Initiative (EJI). This is a great source of information related to elder fraud, including statistical data, tips, descriptions of programs and activities, and news related to the prosecution of real-life cases.
- The Federal Trade Commission (FTC), whose mission is "protecting America's consumers." The FTC produces valuable research and analysis and lists several tools that are useful in combatting elder fraud, including effective strategies to protect the older population.
- COVID-19 News from the FBI. The FBI has established a COVID-19 working group to address a variety of topics, including tools to combat elder fraud.

Additional learning resources:

- "COVID-19 related elder abuse scams"
- "Elder abuse concerns heightened amid COVID-19 isolation"
- "How isolation and COVID make seniors more vulnerable to fraud and exploitation"
- "Coronavirus scams targeting older Americans"
- "Older adults lost $100 million to COVID-related fraud in 2020: report"
- "Elder abuse & COVID-19"
- "Worst COVID-19 scams targeting seniors"
- "6 Coronavirus scams and hoaxes targeting the elderly"

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

aicpa.org
aicpa-cima.com
cgma.org
cimaglobal.com

2205-401308