

Table of contents

Introduction	3
What is senior financial exploitation?	3
Who are the victims? Who are the perpetrators?	4
How do these schemes work?	4
COVID-19 scams targeting seniors	7
Tips for avoiding scams	8
Warning signs of financial exploitation	8
Have the talk	9
Helpful resources	.10
Endnotes	. 10

"Bank of America" is a marketing name for the Retirement Services business of Bank of America Corporation ("BofA Corp."). Banking activities may be performed by wholly owned banking affiliates of BofA Corp., including Bank of America, N.A., Member FDIC. Brokerage and investment advisory services are provided by wholly owned nonbank affiliates of BofA Corp., including Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill"), a dually registered broker-dealer and investment adviser and Member SIPC.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value
/iic Hot i Die insuica	And Hot Built Guaranteea	may Lose value

Introduction

Senior financial exploitation — addressing a hidden threat

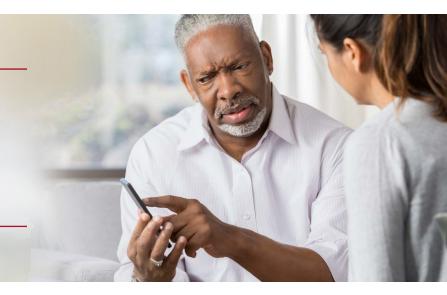
While the elderly population in the United States has grown steadily during the past century, the rate of growth of people over the age of 65 has accelerated since 2011. This is the year when the oldest baby boomers first turned 65. Over the next 40 years, the number of older adults is expected to increase from 56 million in 2020 to 94.7 million in 2060. The number of adults over the age of 85 is expected to almost triple, from 6.7 million to 19 million over that same time period.¹

As the elderly population in the United States continues to grow, the number of crimes involving financial exploitation of this group is also increasing. It is estimated that the cost to seniors who fall victim to financial exploitation is at least \$2.9 billion annually today, and that it will continue to grow as this segment of the population expands.² This article describes common financial scams that target the elderly and lists warning signs that a senior may be falling victim to a scheme to defraud them of their hard-earned savings or retirement income.

What is senior financial exploitation?

While definitions of financial exploitation vary by jurisdiction, the National Adult Protective Services Association (NAPSA) states that, "Financial exploitation occurs when a person misuses or takes the assets of a vulnerable adult for his/her own personal benefit. This frequently occurs without the explicit knowledge or consent of a senior or disabled adult, depriving him/her of vital financial resources for his/her personal needs." Quite often, when such exploitation occurs, the older adult doesn't even realize that they have been victimized.

As the elderly population in the United States continues to grow, the number of crimes involving financial exploitation of this group is also increasing.



Assets are commonly stolen from the older adult through deception, coercion, harassment, false pretenses, duress and threats. Seniors are perceived to be easy targets for such exploitation because they tend to be trusting and polite, and they are likely to have financial savings, own a home and have good credit. These seniors may be isolated, lonely, disabled, uncertain about how to handle their own finances or recently widowed. All of these characteristics make them particularly vulnerable to scammers who are looking to separate them from their money.⁴

Seniors may be reluctant to report that they have become a victim of fraud because they don't know how to report it, or they may be too ashamed of having been scammed. Many of these crimes are perpetrated by loved ones, making reporting of the crime that much more difficult. Believing that their relatives will lose confidence in their ability to keep their financial house in order, scammed seniors may also fear that they will lose their independence if they admit they have been taken advantage of.

Who are the victims? Who are the perpetrators?

Most victims of senior financial exploitation are between 80 and 89 years old. The majority of seniors within this age range are women, and victims are twice as likely to be female. Most victims live alone and require some assistance with health care, home maintenance and other needs. It may come as a surprise that many of these crimes are not committed by strangers. It is estimated that about half of senior financial exploitation is perpetrated by strangers (51%), while 34% is committed by family, friends and neighbors. Sixty percent of known perpetrators are men, typically falling between the ages of 30 and 59. Female perpetrators tend to be between the ages of 30 and 49.5

Most victims live alone and require some assistance with health care, home maintenance and other needs.

How do these schemes work?

The type of exploitation depends on how well the perpetrator knows the elderly victim. According to NAPSA, there are several ways in which family members or other trusted individuals attempt to defraud seniors, including:



Abusing a power of attorney—

The perpetrator attempts to steal the victim's money for their own personal use by using a power of attorney, granted by the victim.



Joint bank accounts —

The perpetrator withdraws funds for their own personal use from a bank account held jointly with the victim.



ATM cards/ checks—

The perpetrator uses ATM cards or checks to withdraw money for their own personal use.



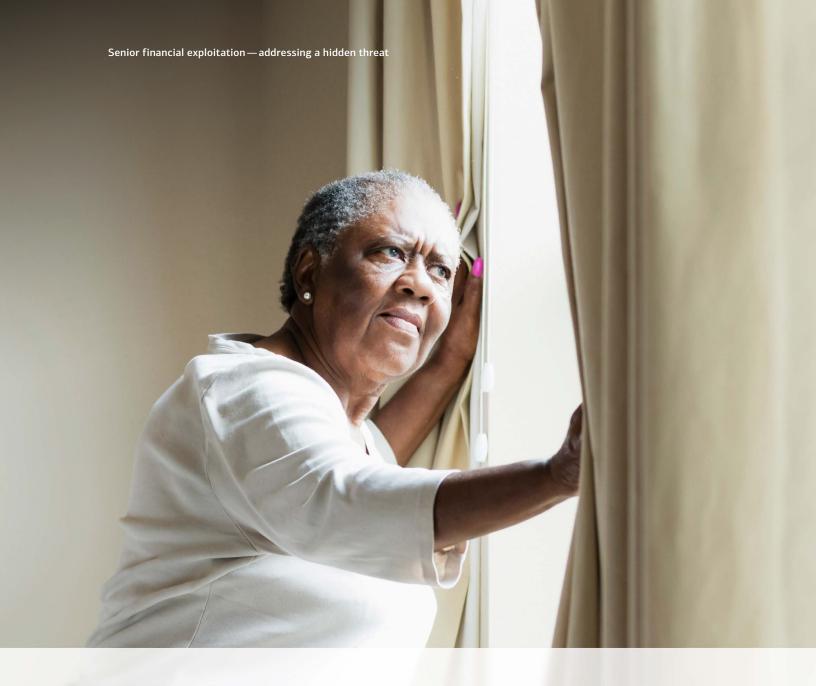
Threats—

The perpetrator threatens to abandon or harm the victim unless they are given what they want.



Withholding medical care —

The perpetrator refuses to obtain needed medical care or services in order to preserve the victim's money for their own use.



In addition, in-home providers may charge for services, keep change from errands, pay their own bills using the vulnerable adult's money, or spend their work time doing things not related to the care of the older adult.

Abuses by strangers can be very creative. Some of the top scams perpetrated by strangers include:

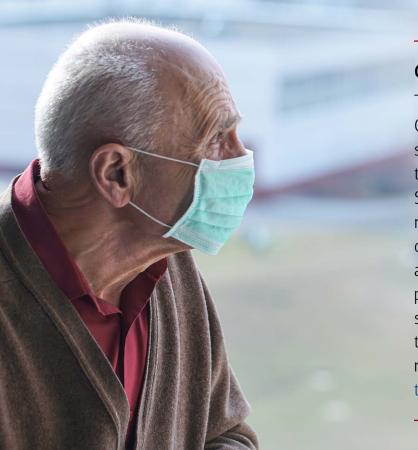
• Telemarketing and internet fraud — These scams involve targeting victims by mail, phone and email. Since many reputable companies use telemarketing to conduct legitimate business, perpetrators will often use this method to scam seniors into giving their credit card information or identity and then use that information to make unauthorized purchases. Scammers may solicit funds for a fake charity, or they might convince the elder that a relative is hospitalized and requires emergency funds. Scammers may also share the elder person's telephone number and personal information with other scammers, leading to the same person being defrauded multiple times.

Scammers may solicit funds for a fake charity, or they might convince the elder that a relative is hospitalized and requires emergency funds.

• Advanced fee scam — Advanced fee scams are telemarketing scams where the criminal encourages the victim to advance large sums of money in the hope that they will receive an unusually high rate of return on their funds. An example of this is the Nigerian Letter scam. In this swindle, the perpetrators convinced victims to disclose their credit card information to help a Nigerian prince travel to the United States to escape persecution. The scammers promised that a portion of the prince's fortune would be paid to the victim in exchange for their help. The criminal then uses the credit card information to make unauthorized purchases.⁸

- Identity theft Identity theft occurs when
 the scammer gains access to the older victim's
 personal information in order to rob them of money
 or property. This includes tax ID theft, where a
 scammer may use a senior's Social Security number
 in various ways, including by impersonating the IRS
 to coerce the victim into sending money that they
 supposedly owe to the government.
- Sweepstakes scams Scammers tell elders that they've won a monetary prize and mail them a check. The scammers ask the seniors to send money in return to cover the prize's taxes or fees. The scammers collect this money, but the original "prize" check bounces.
- Grandparent scam Scammers call elders and convince them that they're a grandchild. The scammer presents a problem that can be solved if the grandparent sends money. Problems could include getting out of jail, paying a hospital bill or getting home from a foreign country. Scammers appeal to the victim's emotions and trick them into wiring money. The scammer may also ask the grandparent to keep the arrangement secret from family members to avoid family discord. The nature of this scam is so personal that many seniors will never reveal that they've been deceived this way.
- Computer tech support scams The scammers try to gain the victim's trust by posing as a technology company with a highly recognizable name. They falsely claim that the victim's computer has been infected with a virus or needs an update and convince the victim to reveal their personal information and grant access to their computer. They may also convince the victim to turn over credit card information to pay for fixing the so-called virus.⁹

- Romance scams Online dating among seniors has risen in recent years. Some con artists appeal to a senior's loneliness and vulnerability by conducting a cyber-romance. Many times, the perpetrator will create an elaborate online profile to lend credibility to their story. They may call and chat with the senior over the phone to prove that they are legitimate, as a means to gain the senior's trust. These conversations may take place over several weeks or even months. In some cases, the perpetrator will even propose marriage. After gaining the senior's trust, the perpetrator will start to ask for money for various things, including medical emergencies, losses due to a temporary financial setback, or even travel expenses so that they can come visit the victim. In addition to losing their money to these con artists, the senior may get caught up in other nefarious activities like money laundering or aiding in shipping stolen merchandise.10
- Social Security scams Social Security scams are becoming more frequent. There are several variations, but the caller generally attempts to acquire personal information like a Social Security number, date of birth and bank account number. According to the Social Security Administration, SSA employees will only reach out to beneficiaries over the phone in limited circumstances for "customer service purposes," and they will always provide a call-back number and extension. Social Security will not send an email asking for personal information.¹¹



COVID-19 scams targeting seniors

The Federal Communications
Commission has identified several
scams that have targeted seniors in
the age of COVID-19. These include
Social Security scams, imposter scams
relating to stimulus checks, the filing
of tax extensions and other tax-related
actions, fake stock offerings, and a
pandemic version of the grandparent
scam.¹² For more information on
these COVID-related scams, please
refer to fcc.gov/coronavirus-scamstargeting-older-americans.

Tips for avoiding scams

The U.S. Senate Special Committee on Aging offers the following as signs that you may be being scammed.¹³

- Being pressured to make decisions quickly or being threatened
- Seeing a caller ID or phone number that seems suspicious (con artists often disguise their real numbers)
- Receiving a call from someone pretending to be with the government

- Being asked to provide personal information like your Social Security number or account numbers
- Being asked to give out your credit card number or money (if you have any doubts at all, ask a friend or family member about it)
- Being offered free travel

Warning signs of financial exploitation

If a senior seems confused about recent financial transactions or is reluctant to discuss recent financial activity, this could be an indication that they are being manipulated. If they have recently made changes to property titles, wills, powers of attorney, or other documents, this could indicate that someone else is exercising undue influence. Unexplained credit card activity, uncharacteristically frequent or excessive withdrawals from accounts, and newly authorized signers on accounts could also signal exploitation. Checks written to cash, assets transferred to unfamiliar people, the giving away of money, unexplained disappearances of cash or valuables, or any other out-of-character changes in financial behavior may also indicate a problem.

If you suspect your elder family member has been victimized, refer to the Department of Justice's Elder Justice website at justice.gov/elderjustice.

If a senior seems confused about recent financial transactions or is reluctant to discuss recent financial activity, this could be an indication that they are being manipulated.

Have the talk

Exploitation of an elder family member can result in devastating financial losses and emotional consequences. When we recognize the signs of senior financial exploitation and understand its risk factors, we can reduce the chance that our loved ones will end up a target. Start a conversation with an older loved one about this topic soon. It might be one of the most important conversations you ever have.



Helpful resources

Following is a list of helpful resources with their web addresses:

- National Resource Center on Women and Retirement Planning – wiserwomen.org
- National Adult Protective Services Resource Center – napsa-now.org
- National Center on Elder Abuse ncea.acl.gov
- Federal Bureau of Investigation fbi.gov

- National Center for Victims of Crime, Financial Crime Resource Center – victims of Crime.org
- Consumer Financial Protection Bureau – consumerfinance.gov
- Federal Trade Commission ftc.gov
- U.S. Administration on Aging eldercare.gov

Endnotes

- ¹ Mather, Mark, et al. "What the 2020 Census Will Tell Us About a Changing America," Population Bulletin 74, no. 1 (2019).
- United States Senate Special Commission on Aging. (2019). Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors. aging.senate.gov/fraudbook/index.html.
- ³ National Adult Protective Services Association. (2021). What is Financial Exploitation? napsa-now.org/get-informed/what-is-financial-exploitation.
- ⁴ Elder Fraud. (n.d.). FBI. Retrieved January 28, 2021, from fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud.
- ⁵ Women's Institute for a Secure Retirement. (2016). Just the Facts: Senior Financial Fraud and Abuse. wiserwomen.org/wp-content/uploads/2019/11/ SENIOR3.pdf.
- ⁶ National Adult Protective Services Association. (2021). Elder Financial Exploitation. napsa-org/get-informed/exploitation-resources.
- ⁷ Cornell University Legal Information Institute. Phone and Telemarketing Fraud. Retrieved February 2, 2021 from law.cornell.edu.
- 8 Ihid
- ⁹ United States Senate Special Commission on Aging. (2019). Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting our Nation's Seniors. aging.senate.gov/fraudbook/index.html.
- 10 Ibid.
- 11 Ibid.
- ¹² Federal Communications Commission. (May 27, 2020). Coronavirus Scams Targeting Older Americans. Retrieved February 2, 2021, from fcc.gov/coronavirus-scams-targeting-older-americans.
- 13 Ibid.



Bank of America, its affiliates and financial advisors do not provide legal, tax or accounting advice. You should consult your legal and/or tax advisors before making any financial decisions. This material should be regarded as general information on health care considerations and is not intended to provide specific health care advice. If you have questions regarding your particular situation, please contact your legal or tax advisor.

 $@\ 2022\ Bank\ of\ America\ Corporation.\ All\ rights\ reserved.\ |\ MAP4327219\ |\ WP-02-22-0306.B\ |\ ADA\ |\ 03/2022$

To learn about Bank of America's environmental goals and initiatives, go to bankofamerica.com/environment. Leaf icon is a registered trademark of Bank of America Corporation.