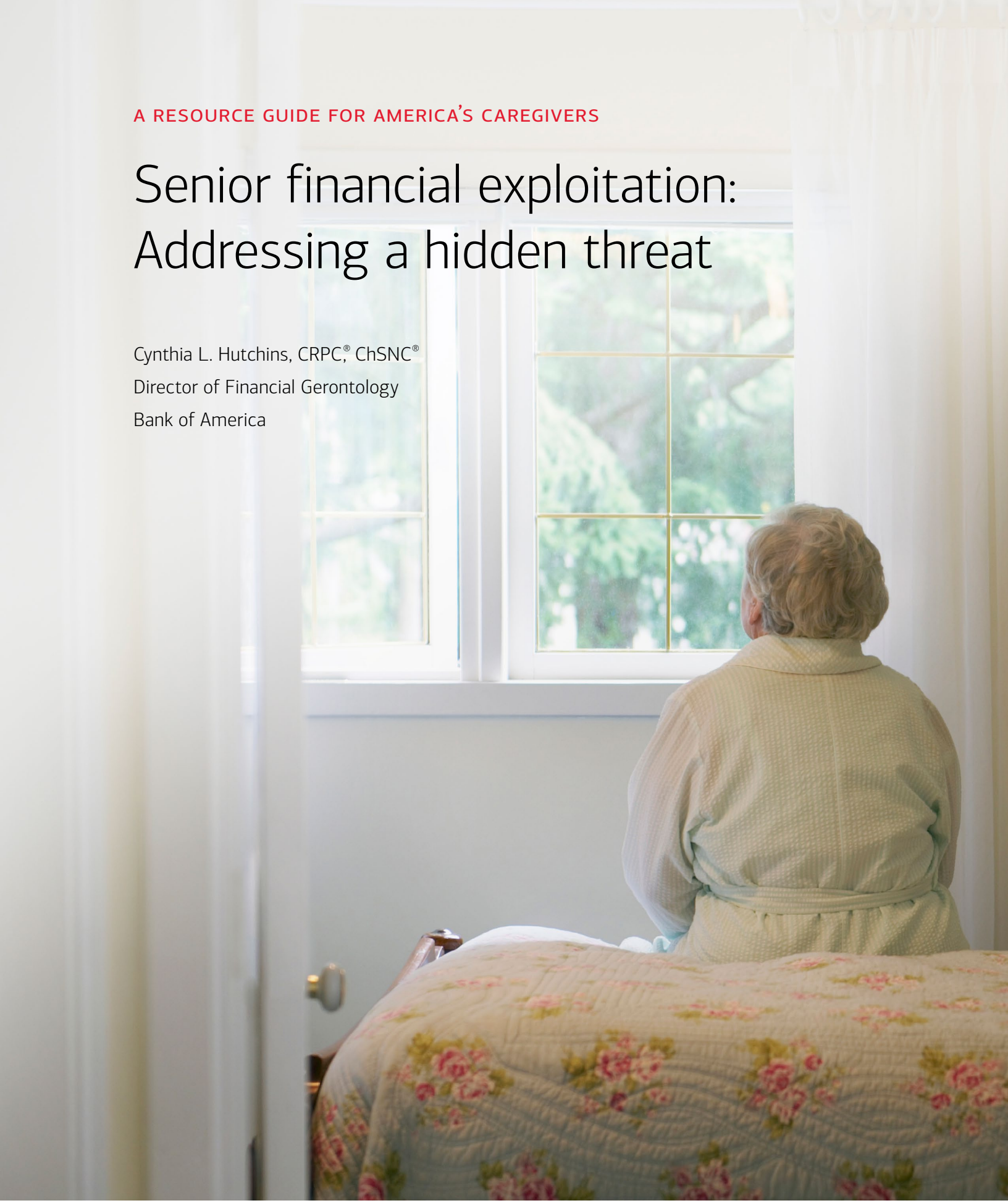
A RESOURCE GUIDE FOR AMERICA'S CAREGIVERS

Senior financial exploitation: Addressing a hidden threat

Cynthia L. Hutchins, CRPC,® ChSNC®
Director of Financial Gerontology
Bank of America



BANK OF AMERICA

Contents

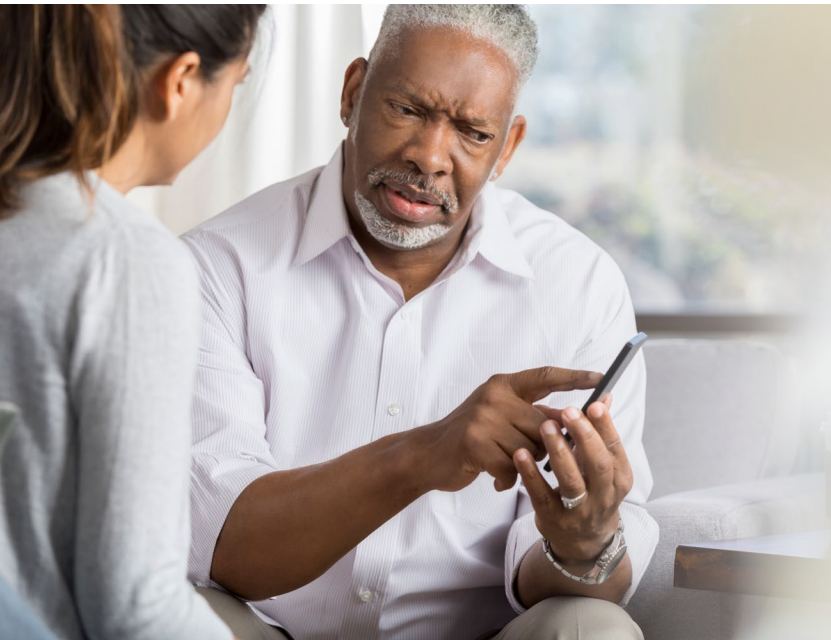
Introduction

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 in the U.S. is expected to increase from 56 million in 2020 to 94.7 million in 2060.[1] 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.[2]

As the elderly population in the U.S. continues to grow, the number of crimes involving financial fraud and exploitation of this group is also increasing. It's estimated that the cost to seniors who fall victim to financial exploitation is at least $3 billion annually.[3] According to the *Consumer Sentinel Network Data Book 2021*, there was a 47% increase in fraud and identity theft reports from 2019 to 2020, rising from 3.24 million to 4.7 million. Furthermore, reported losses in 2020 were $3.3 billion, representing a $1.5 billion increase over 2019.[4] These alarming numbers are expected to continue to grow as the segment of the population over the age of 65 expands. The Federal Trade Commission has reported that the phone is the top fraud contact method used, the second most common being online.[5]

This brochure includes:

- Common scams that target the elderly
- Warning signs that seniors may be falling victim to a scheme to defraud them of their hard-earned savings or retirement income
- Advice for those who suspect that they or a loved one may have fallen victim to a scam
- A comprehensive list of helpful resources



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

What is senior 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."[6] Quite often, when such exploitation occurs, older adults don't even realize that they've been victimized.

Assets are commonly stolen from older adults 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're 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.[7]

Seniors may be reluctant to report that they've 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 much more difficult. Believing that their relatives may lose confidence in their ability to manage their own finances, scammed seniors may also fear that they'll lose their independence if they admit they've been scammed.

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 aren't committed by strangers. It's 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.[8]

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:[9]

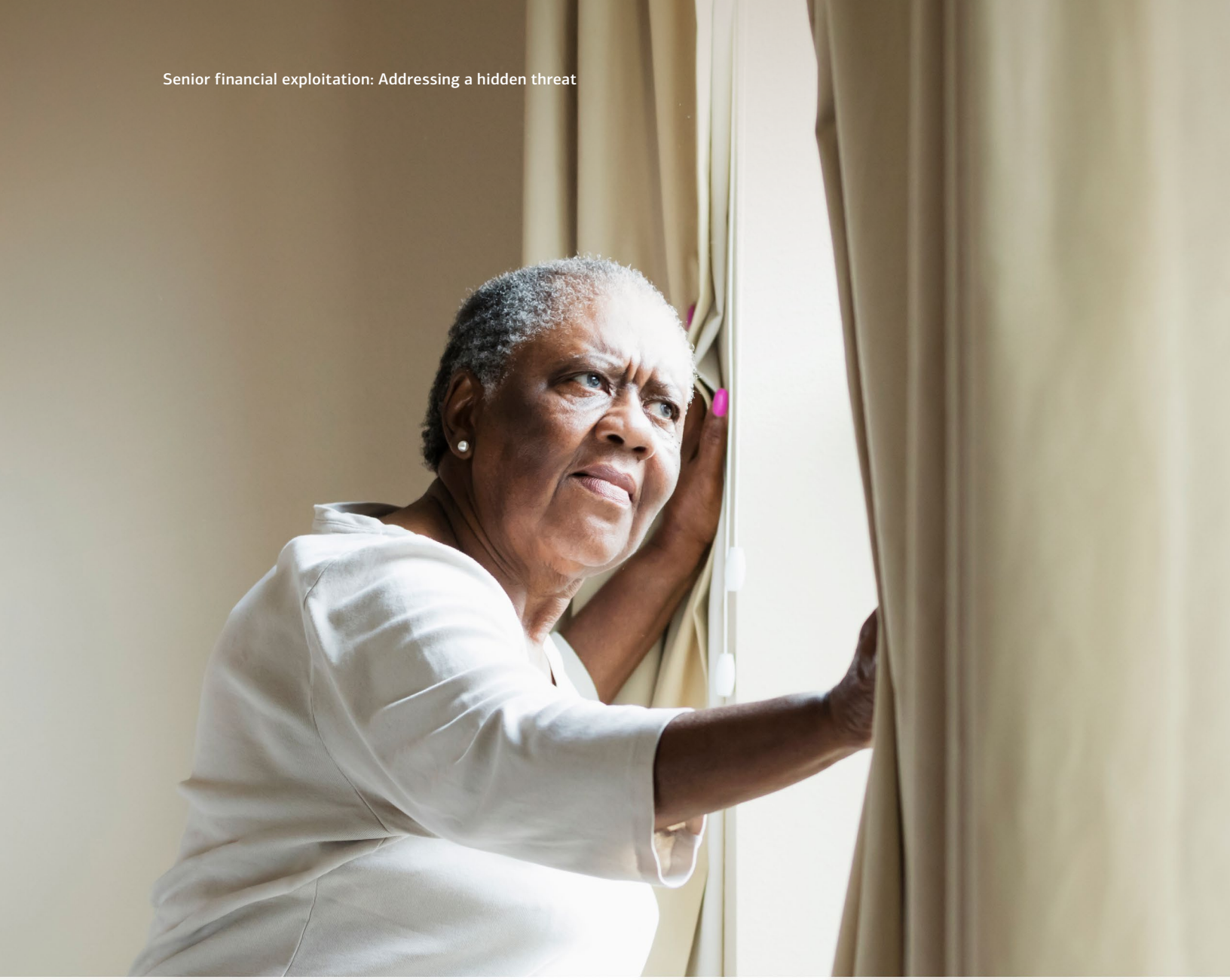
Abusing a power of attorney. Perpetrators attempt to steal the victim's money for their own personal use by using a power of attorney, granted by the victim.

Joint bank accounts. Perpetrators withdraw funds for their own personal use from a bank account held jointly with the victim.

ATM cards/ checks. Perpetrators use ATM cards or checks to withdraw money for their own personal use.

Threats. Perpetrators threaten to abandon or harm the victim unless they're given what they want.

Withholding medical care. Perpetrators refuse to obtain needed medical care or services in order to preserve the victim's money for their own use.



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.

Frauds and scams

There are many different frauds and scams designed to separate seniors from their money. These schemes evolve with the times; for example, many of them emerged as a result of the COVID-19 pandemic. These schemes included:[10]

- **Identity theft.** Scammers steal people's names, birthdates and other personal information when they post a picture of their vaccination card to social media.
- **Charity scams.** Scammers claim to be from genuine charities and solicit donations, or they create fake charities.
- **Checks from the government.** Scammers claim to be from the IRS or some other government agency and proceed to ask for personal information.
- **FDIC and banking.** Scammers claim to be from the FDIC or from the bank and scare seniors into giving them personal information by claiming that their bank-held assets are in danger.
- **COVID-19 funeral assistance.** Scammers claim to be from the FEMA COVID-19 Funeral Assistance Program and offer to register family members, thus collecting individuals' personal information.

Common frauds and scams

Medicare fraud

These types of scams usually involve perpetrators who pose as a Medicare representative to get seniors to reveal personal information. The scammers then use the information provided to bill Medicare and to pocket the money.

Because Medicare fraud is so prevalent, there's a network of volunteers across the country who are working to help seniors identify deceptive health care practices. Known as the Senior Medicare Patrol (SMP), these volunteers identify and report fraud and abuse in their communities.

Genetic testing fraud

Medicare strictly limits coverage for genetic screening tests. However, Medicare will cover many diagnostic genetic tests. Criminals will use these tests to scam seniors. The scams range from kickback arrangements to scammers who want to commit identity theft. The scope of these scams is broad, ranging from medically unnecessary services to billing for services that were never provided. Providers may not even be aware that they're part of a fraud scheme. There are also reports that criminals are using the names and logos of legitimate companies that offer genetic testing to convince patients that the offer of medical services and testing is not a scam.[11]

Scammers may claim to be from a genuine charity, the IRS, a bank, Medicare or a number of legitimate companies. All of these schemes attempt to get seniors to reveal personal information.

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 or identifying information and then use that information to make unauthorized purchases.[12]

Advanced fee scam

These telemarketing scams encourage victims to advance large sums of money in the hope they'll receive an unusually high rate of return on their funds. One example is the Nigerian letter scam. The perpetrators convince victims to disclose their credit card information to help a "Nigerian prince" travel to the U.S. to escape persecution. The scammers promise that a portion of the prince's fortune would be paid to victims in exchange for their help. Criminals then use the credit card information to make unauthorized purchases.[13]

Lottery and sweepstakes scams

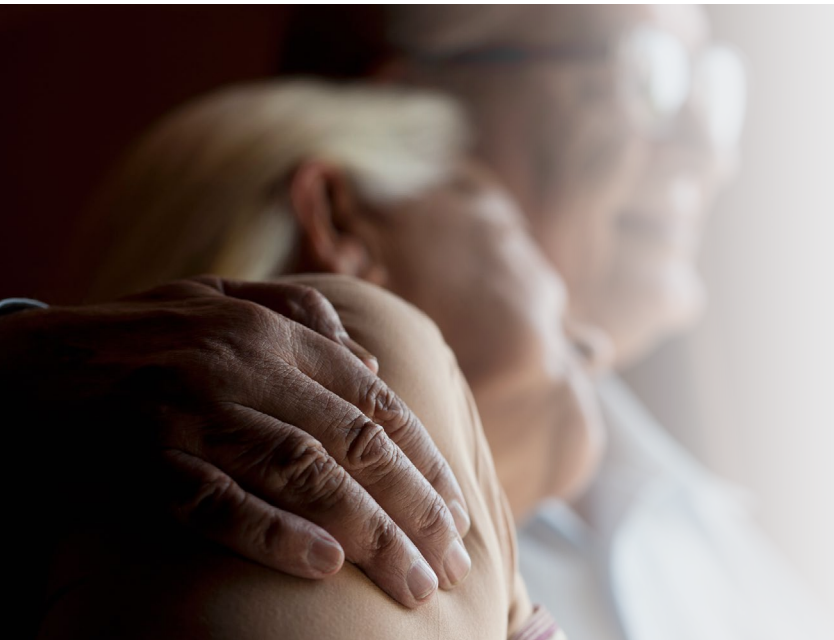
Perpetrators tell elders that they've won a monetary prize and mail them a check. The scammers ask seniors to send money in return to cover the prize's taxes or fees. When they collect this money, the original "prize" check bounces.

Grandparent scams

Scammers call elders and convince them that the person calling is one of their grandchildren. The scammer presents a problem that can be solved if the grandparent sends money. Problems can include getting out of jail, paying a hospital bill or getting home from a foreign country. Scammers appeal to victims' emotions and trick them into wiring money. They may also ask the victim 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 in this way.

Computer tech support scams

Older adults are nearly five times more likely than younger adults to report losing money due to a tech support scam.[14] Because seniors are less likely to be tech savvy, scammers view them as easy targets. The scammers try to gain a 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. Initial contact from scammers can occur in various ways, including unsolicited telephone calls, search engine advertising, pop-up messages and email. They convince the victim to turn over credit card information to pay for fixing the so-called virus.[15]



There are many different frauds and scams designed to separate seniors from their money. These schemes evolve with the times.

Romance/sweetheart scams

Online dating among seniors has risen in recent years. Some con artists appeal to their loneliness and vulnerability by conducting a cyber-romance. Often, perpetrators will create an elaborate online profile to lend credibility to their story. They may call and chat with a senior over the phone to prove that they're legitimate, as a means to gain the senior's trust. These conversations may take place over the course of several weeks or even months. In some cases, perpetrators will even propose marriage. After gaining the senior's trust, perpetrators will start to ask for money for various reasons, including medical emergencies, losses due to a temporary financial setback, or even travel expenses so that they can come to visit the victim. In addition to losing their money to these con artists, seniors may unwittingly get caught up in other nefarious activities, like money laundering or aiding in shipping stolen merchandise.[16]

Bereavement scams

Fraudsters read the obituary or attend the funeral of a stranger in order to take advantage of the bereaved surviving spouse. Con artists may use information gathered from the obituary or knowledge learned through funeral attendees to extract money or information from the survivors. They may claim that the deceased had an outstanding debt with them and try to get relatives to satisfy the fake debt. They may also use information gleaned from the obituary to start building a profile for identity theft.

Investment fraud

Older people may be viewed as more trusting and more likely to have investable assets after a lifetime of working. Callers may pressure seniors to send money to take advantage of a once-in-a-lifetime investment with virtually no risk and the opportunity for incredible gains. These investments may sound too good to be true because they usually are.

Reverse mortgage and home equity scams

Some of these homeowner scams include:

- **Reverse mortgage investments.** Scammers convince a senior to use the proceeds from a reverse mortgage for estate planning or for reinvestment into an insurance product or annuity promising high returns for the senior's estate.
- **House flipping.** Scammers persuade a senior to use the cash from a reverse mortgage to purchase another property to resell for a profit.
- **Home improvements.** Fraudster "handymen" perform a home inspection and reveal that the home needs major repairs. They then suggest the use of a reverse mortgage to pay for the repairs.
- **Fraud by relatives.** Relatives pressure an elderly family member to take out a reverse mortgage and then use the money for their own interests instead of in the best interest of the elderly family member.

Identity theft

There are three main types of identity theft: financial identity theft, medical identity theft and online identity theft. Identity theft occurs when someone steals personal information in order to commit fraud. This information may include a person's name and date of birth, Social Security number, driver's license number, Medicare account number, credit card numbers, bank account numbers, personal identification numbers (PINs), e-signatures, passwords or any other information that can be used to access a person's financial accounts and resources. Fraudsters may use this information to empty bank accounts, open credit cards and apply for loans, file taxes and commit tax fraud, get medical services, change the name on real property, and obtain goods and services.

The U.S. government identifies the following warning signs of identity theft:[17]

- Unexplained withdrawals from your bank account
- Bills or other mail that was never received
- Checks refused by merchants
- Debt collectors calling about debts you haven't incurred
- Unfamiliar accounts or charges appearing on your credit report
- Getting billed for medical services you didn't receive
- Health plans refusing to pay benefits for legitimate medical expenses, claiming that you've reached your benefit limit
- Notification from the IRS that more than one tax return was filed in your name or that you show income from an employer you don't work for
- Receiving a notice that your data has been compromised by a data breach at a company where you do business or have an account

What should you do if your identity is stolen?[18]

- If you have identity theft insurance, **file a claim immediately**. The theft insurance company should do most of the work for you.
- **Contact any company** where you know the identity thief used your identity. Close any accounts that may have been opened in your name and ask to have any charges removed from these accounts.
- **Contact all the major credit bureaus** and request copies of your credit reports. Set up fraud alerts for your reports by calling each bureau or visiting their website:
  - Experion: 888.397.3742
  - Equifax: 800.525.6285
  - TransUnion: 800.680.7289
- **Contact additional agencies**, including the IRS, Social Security Administration, health care providers, Department of Motor Vehicles, and telephone and utility companies.
  - IRS: 800.829.1040
  - Social Security Administration: 800.772.1213
- **Delete your personally identifiable information** from any and all websites and social media.

Are you being scammed?

The Federal Trade Commission and the U.S. Senate Special Committee on Aging offer the following as signs that you may be being scammed:[19]

- 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 from the government
- Being asked to provide personal information, such as 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 or prizes
- Getting a call from someone pretending to be from an organization that you know
- Being told to pay in a specific way, such as using cryptocurrency, wiring money or putting money on a gift card[20]
- Receiving a check and being asked to deposit it and send the person the money

Warning signs of elder 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 the person is being manipulated. Newly made changes to property titles, wills, powers of attorney or other documents 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.

Further protection

To help further protect yourself against financial fraud:

- Consult your financial advisor
- Visit your financial center
- Educate yourself using Better Money Habits®
- Access the Bank of America Security Center
- Obtain a Trusted Contact form for your accounts

Completing the Trusted Contact form provides your financial advisor with the name and contact information of someone you trust, who can be notified in the event your advisor notices uncharacteristic behavior on the part of the account owner. The form doesn't authorize the trusted contact person to transact business in your accounts and doesn't authorize your financial advisor to reveal any information about your accounts. It can, however, be an added level of protection to guard against financial fraud and abuse.

If you suspect an elder family member has been victimized, refer to the Department of Justice's Elder Justice website.

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 and your financial advisor about this topic soon. It might be one of the most important conversations you ever have.

Helpful resources

Following is a list of resources. Search for these organizations online to learn more:

- Consumer Financial Protection Bureau
- Elder Financial Protection Network
- Federal Bureau of Investigation Task Force on Senior Citizens
- Federal Trade Commission
- National Adult Protective Services Resource Center
- National Center for Victims of Crime, Financial Crime Resource Center
- National Center on Elder Abuse
- National Council on Aging
- National Do Not Call Registry
- National Resource Center on Women and Retirement Planning
- Senior Medicare Patrol
- U.S. Administration on Aging

Annual Credit Report.com allows you to check your credit reports. Visit online or call 877.322.8228.

Better Money Habits is part of Bank of America's commitment to fostering economic mobility and financial education.

Elder Care Locator is a public service of the U.S. Administration on Aging that can connect you to services for older adults and their families. Call 800.677.1116.

Money Smart for Older Adults is a free financial education program that raises awareness among older adults and their caregivers on how to prevent elder financial exploitation. It also encourages advance planning and informed financial decision-making. Call 877.ASKFDIC (877.275.3342).

BANK OF AMERICA

Endnotes

[1] Mark Mather, Linda A. Jacobsen, Beth Jarosz, Lillian Kilduff, Amanda Lee, Kelvin M. Pollard, Paola Scommegna and Alicia Vanorman, *America's Changing Population: What to Expect in the 2020 Census*, Population Reference Bureau, June 2019.

[2] See note 1, above.

[3] "Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims for Financial Gain," Federal Bureau of Investigation, Sept. 19, 2019.

[4] Mark Gill, "Senior scam statistics 2019 – 2021," Comparitech, Oct. 7, 2022.

[5] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission, February 2022.

[6] "What is financial exploitation?" National Adult Protective Services Association, Aug. 16, 2022.

[7] "Scams and safety: Elder fraud," Federal Bureau of Investigation, 2023.

[8] "Elder Financial Fraud & Abuse Information for Caregivers," Women's Institute for a Secure Retirement (WISER), March 27, 2022.

[9] See note 6, above.

[10] "Scams related to COVID-19," USAGov, Dec. 16, 2022.

[11] Jennifer Trussell, "Genetic Testing Fraud: A Concerning Trend for Seniors," National Council on Aging, Oct. 17, 2019.

[12] "Phone and telemarketing fraud," Cornell Law School, Legal Information Institute.

[13] See note 12, above.

[14] *Protecting Older Consumers 2021 – 2022: A Report of the Federal Trade Commission*, Federal Trade Commission, Oct. 18, 2022.

[15] *Fighting Fraud: Top Scams in 2021*, U.S. Senate Special Committee on Aging, 2022.

[16] See note 15, above.

[17] "Warning Signs of Identity Theft," IdentityTheft.gov, Federal Trade Commission.

[18] "What To Do If Your Identity Is Stolen," Security.org, Jan. 27, 2023.

[19] "Coronavirus Scams Targeting Older Americans," Federal Communications Commission, Feb. 2, 2021.

[20] *How to Avoid a Scam*, Federal Trade Commission, July 2022.