Spot the Scam

Combatting Elder Fraud Through Education & Advocacy

Welcome to **Spot The Scam**, your essential resource for Medicare-eligible seniors and their caregivers to identify and avoid all forms of elder fraud.

Combatting
ELDER FRAUD
Through Education & Local Advocacy

You earned your retirement, no one deserves to enjoy it but you. Learn a few simple ways to better defend yourself against fraud and advocate for your future

Our 3-step method—Spot the Scam, Take Action, Take Back Control—empowers you to identify common threats like identity theft, Medicare telemarketing scams, and financial fraud. With clear guidance and practical tools, Spot The Scam helps you stay vigilant, respond effectively, and regain control of your financial security.

Stay safe with Spot The Scam and safeguard your future.

Examples

iKan “unpaid” Tolls Scam

An important message from iKan, KDOT, and the Kansas DMV

Dear iKan subscriber:

We want to inform you of nationwide text message scams in which fraudsters impersonate state agencies, including the Kansas Division of Motor Vehicles (DMV) and the Kansas Department of Transportation (KDOT). These text messages falsely claim recipients owe unpaid tolls and are sent at random to individuals in an attempt to steal personal and financial information. **Please note that Kansas tolls are never collected through unsolicited texts, instant messages, or emails.**

DriveKS is Kansas' official toll payment system, operated by the Kansas Turnpike Authority. Official communication regarding unpaid tolls or account status will direct you to log into your secure DriveKS account or contact customer service directly. You receive this communication if you've established a DriveKS account and opted in to notifications, either through self-service channels or when contacting DriveKS customer service. You control your communication preferences and can opt out at any time.

What to do if you receive a scam message:

- **Do NOT click on any links** in the text message.
- **Do NOT provide any personal or payment information.**
- **Delete the message** immediately.

Text message scams such as these are successful because they attempt to scare people into acting quickly, often using language like 'final notice' or referencing threatening penalties.

If you receive a text message claiming to be about unpaid tolls that you suspect is a scam, please report it to the Federal Trade Commission (FTC) and the Internet Crime Complaint Center (IC3).

Protecting your information is important. Fraudsters constantly change tactics to exploit unsuspecting individuals through deceptive text messages. Stay informed and stay vigilant against these fraudulent attempts.

3 STEPS TO KNOW

You earned your retirement, no one deserves to enjoy it but you. Learn a few simple ways to better defend yourself against fraud and advocate for your future

STEP 1 - SPOT THE SCAM

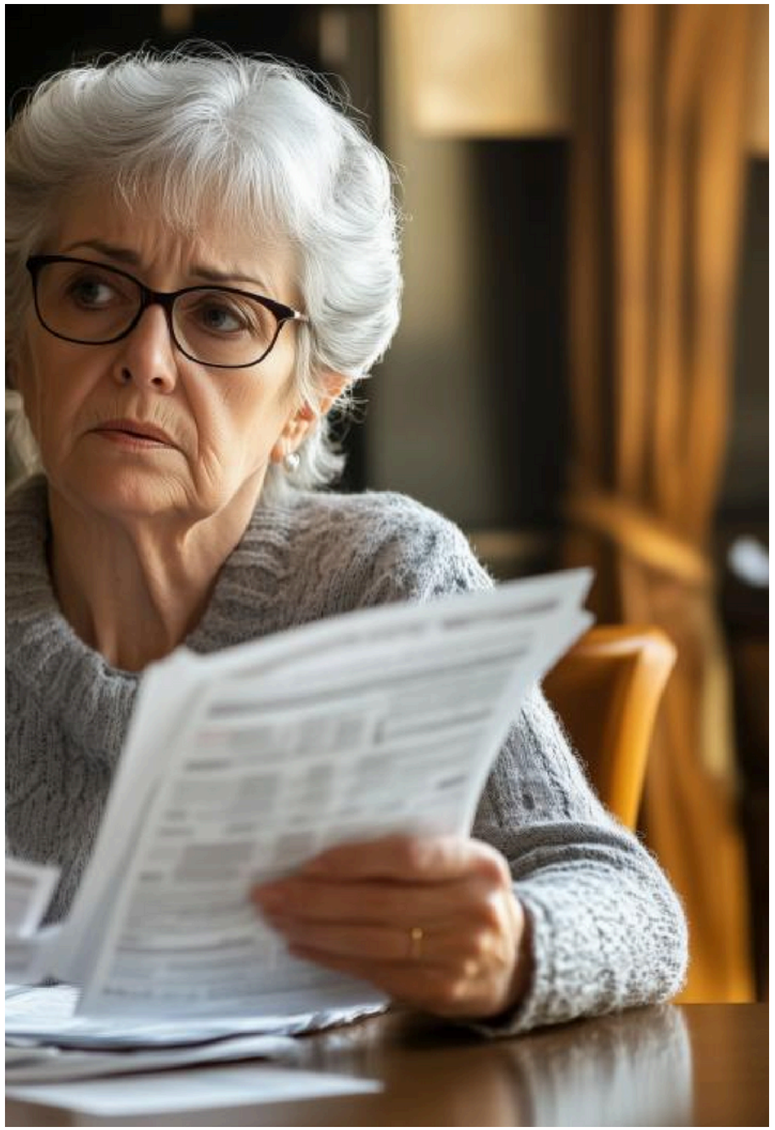
You earned your retirement, no one deserves to enjoy it but you. Learn a few simple ways to better defend yourself against fraud.

STEP 2 - TAKE ACTION

Concerned you may have already been targeted? It’s not your fault, scammers can be extremely convincing. Now is the time to act quickly to minimize the damage they can do.

STEP 3 - TAKE BACK CONTROL

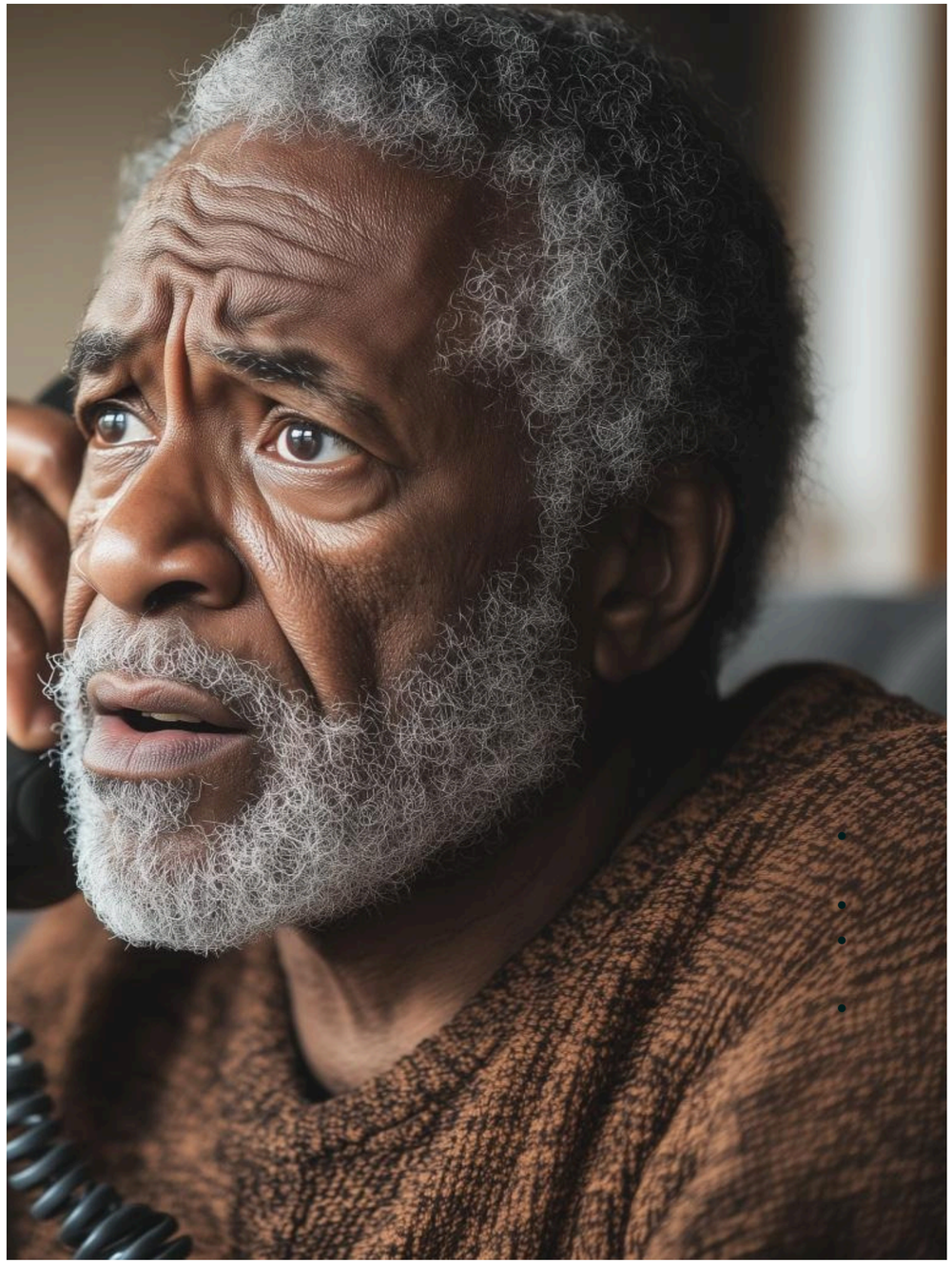
Scammers target everyone, no matter their age or circumstance, if you have been a target of fraud, it's not your fault, scams targeting Medicare individuals are, unfortunately, very common. Here are a few simple ways to take back control and better advocate for your future.



STEP #1 'SPOT'

The first step is to learn how to 'Spot the Scam'. Here are some easy ways to identify the top 3 most common scam types. [2021 Elder Fraud Report]

DID YOU KNOW: 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. [www.ncoa.org]



Medicare Telemarketing Scams

Beware of fraudulent callers pretending to represent Medicare! [www.ncoa.org]

Be wary of anyone claiming to represent Medicare calling you uninvited and asking you for personal or private information.

Medicare will **NEVER** call you unsolicited!

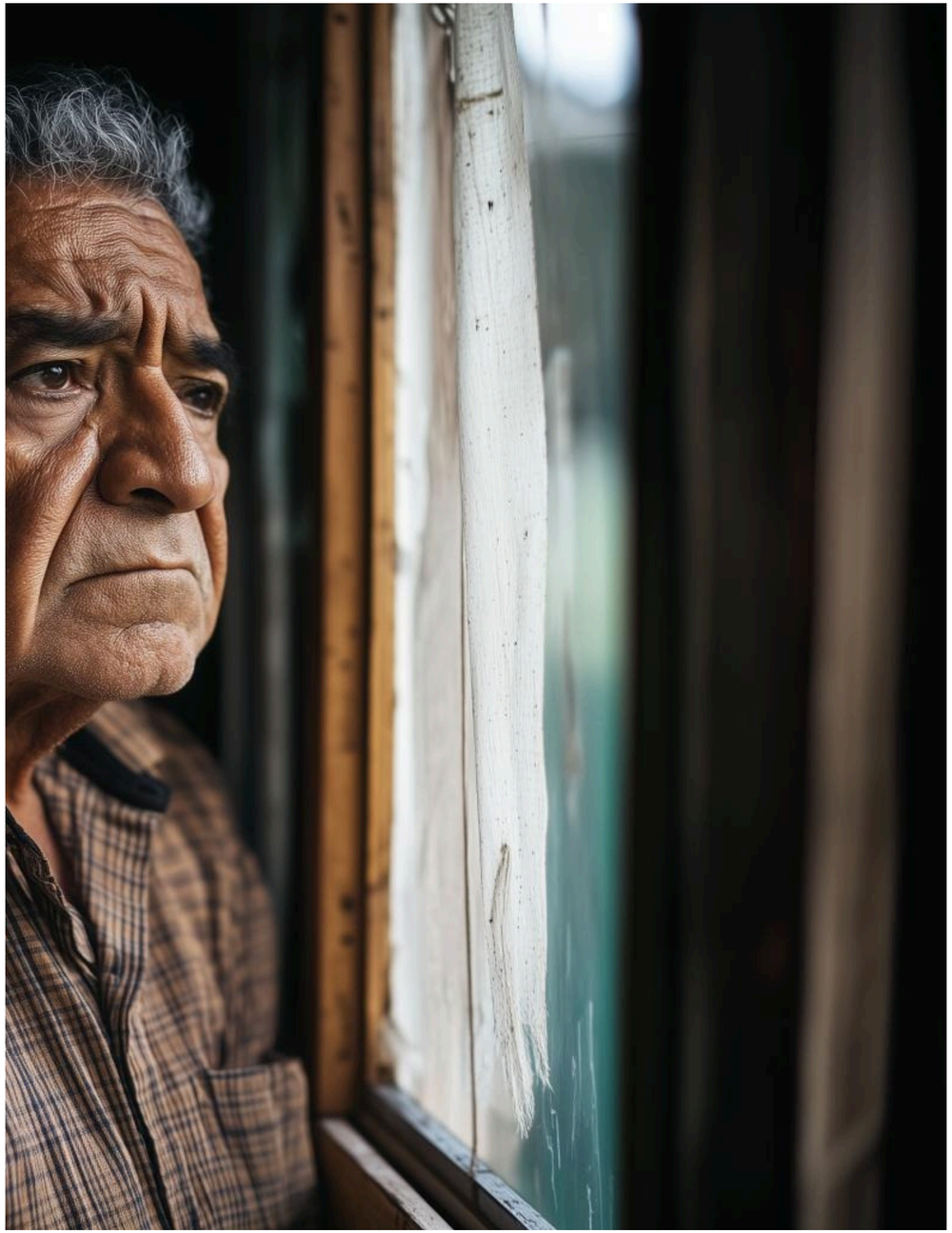
Don’t participate in any calls requesting health insurance information you didn’t initiate.

Beware of being asked to provide your Medicare card or Social Security Information on the phone.

Financial Fraud Scams

$2.9 billion is lost annually due to senior-specific financial fraud alone! [Met-Life]

- You receive calls from unknown numbers claiming to be representatives of a bank or a government agency like Medicare.
- You find medical or supply charges on your account statements that you do not recognize.
- You receive bills for medical treatments you never had or you suddenly stop receiving bank or medical statements.
- A caregiver is contacted by a ‘collection agency’ seeking to collect on debts created in your name, without your permission.



Identity Theft Scams

In 2022 there were 4,825 senior victims of identity theft!

[FBI Elder Fraud Report]

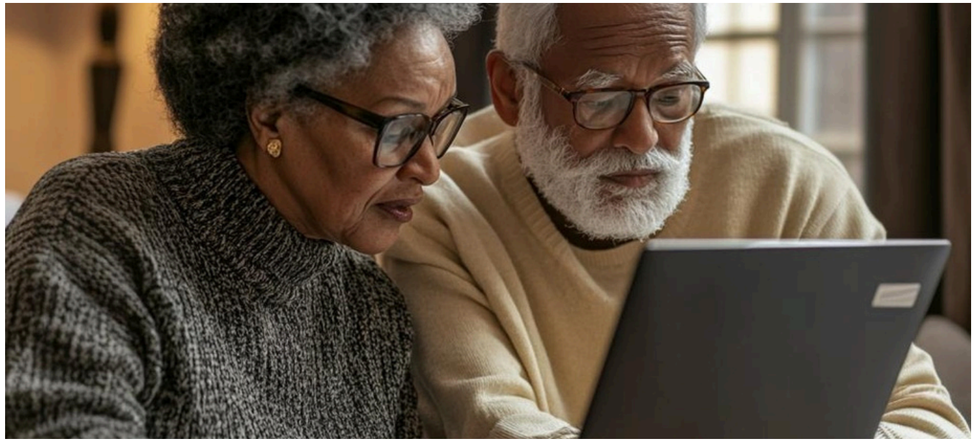
- Be alert if you find charges on your account statements that you do not recognize. Be alert if you receive bills for medical treatments you never had.
- Be careful if your mail is missing. For example, you suddenly stop receiving your bank or medical statements.
- Beware if you are a caregiver and receive phone calls or mail from collection agencies seeking to collect on debts created in the senior person’s name, without their permission.

STAYING INFORMED

Once you've successfully **Spotted the Scam**, the next crucial step is to understand the seriousness of the threat and prepare to take immediate action. Scammers often rely on confusion and hesitation, so recognizing the signs early gives you the upper hand. Whether it's a suspicious phone call, email, or unexpected request for personal information, acknowledging the red flags is your first line of defense. By staying informed and vigilant, you're now equipped to move confidently into the **Take Action** phase, where swift and decisive responses can prevent further harm and protect your assets.

Here are eight tips from the National Council on Aging for how seniors can avoid scams:

1. Never give your credit card, banking, Social Security, Medicare, or other personal information over the phone unless you initiated the call
2. Be aware that you are at risk from strangers—and from those closest to you
3. Don't isolate yourself—stay involved!
4. Tell solicitors: "I never buy from (or give to) anyone who calls or visits me unannounced. Send me something in writing."
5. Shred all receipts with your credit card number
6. Sign up for the "Do Not Call" list and take yourself off multiple mailing lists
7. Use direct deposit for benefit checks to prevent checks from being stolen from the mailbox
8. Be skeptical of all unsolicited offers and thoroughly do your research



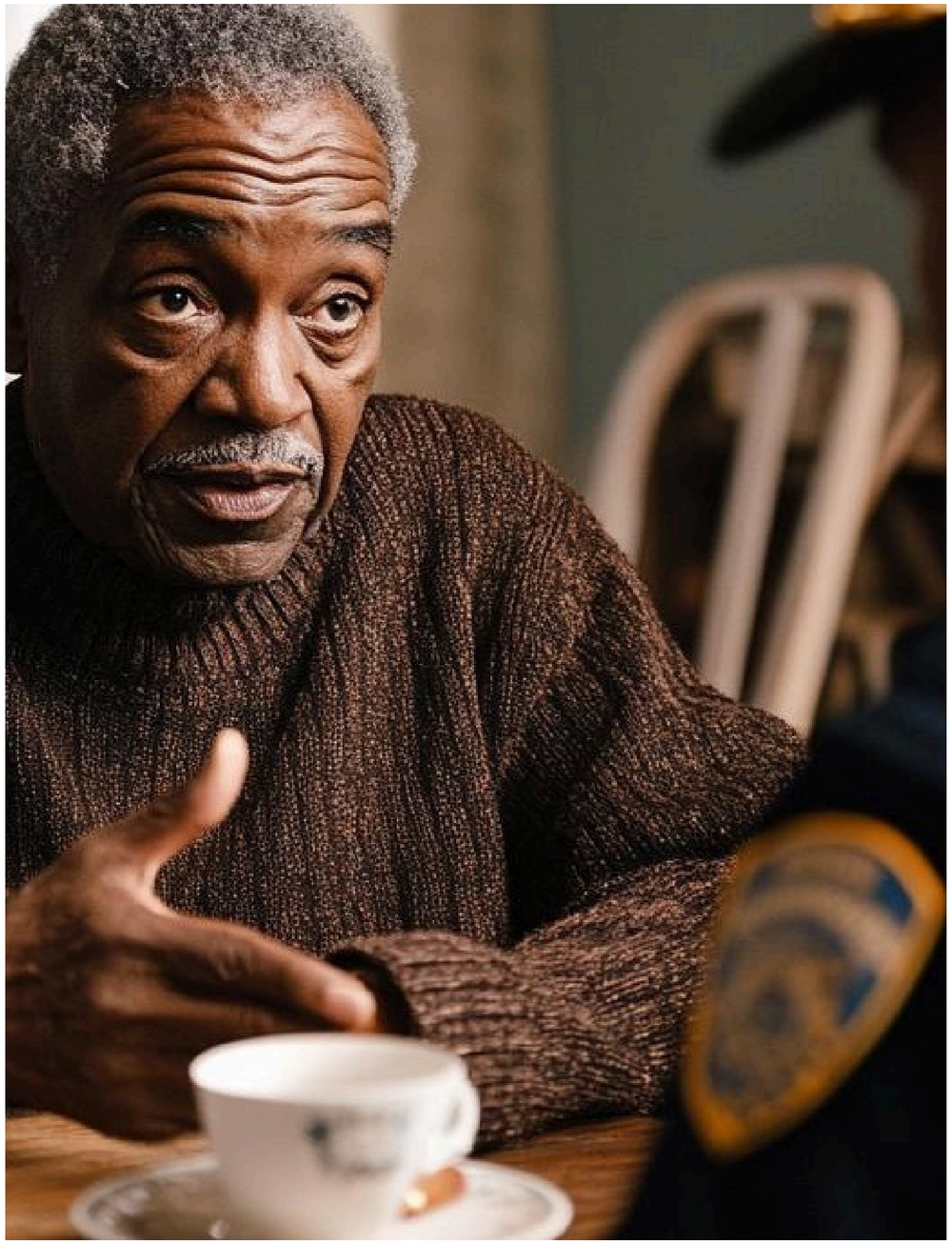
To avoid scams, discover the common ways seniors are targeted in these resources:

The Top 5 Financial Scams Targeting Older Adults (National Council on Aging) Top Scams Targeting Older Adults in 2021 (AARP) Senior Scams (Office of the Attorney General) Top 10 Scams Targeting Seniors (Experian) Defrauding The Elderly: 9 Scams Targeting Seniors (Senior Safety Advice)

STEP #2 'TAKE ACTION'

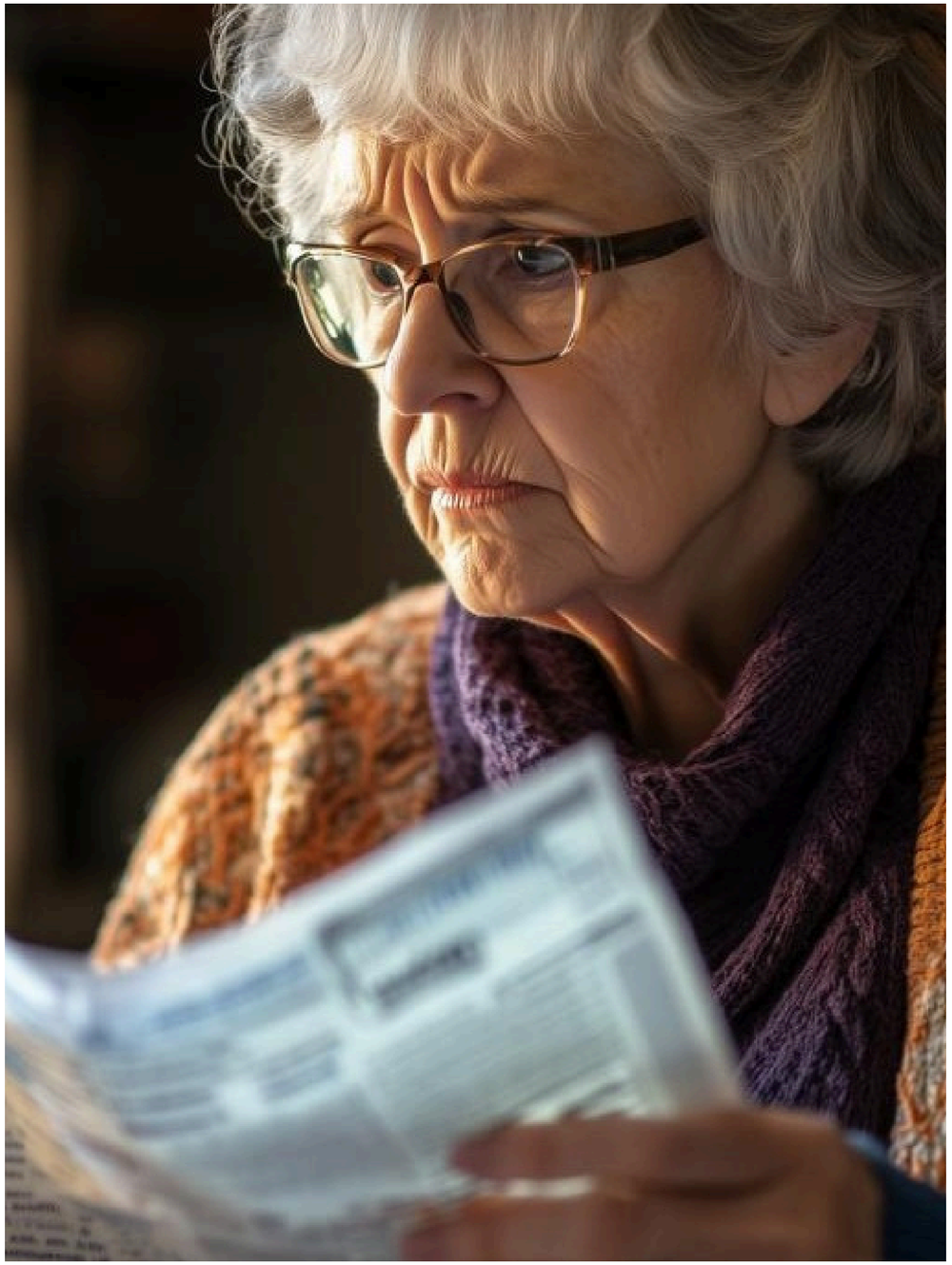
Concerned you may have already been targeted? It’s not your fault, scammers can be extremely convincing.

Now is the time to act quickly to minimize the damage they can do.



How to take action if you think you have been a victim of a Medicare Telemarketing Scam

- Call 1-800-MEDICARE (1-800-633-4227) to alert Medicare of potential fraudulent activity.
- Contact the FTC at IdentityTheft.gov and file an official identity theft report.
- Contact your local law enforcement and file a police report for identity theft.



How to take action if you think you have been a victim of a Financial Fraud Scam.

- Contact your credit card company, banking institution, or Medicare to report the fraud and secure your accounts.
- Call the National Elder Fraud Hotline at 833-372-8311, a free resource set up by the U.S. Department of Justice's Office for Victims of Crime to report fraud

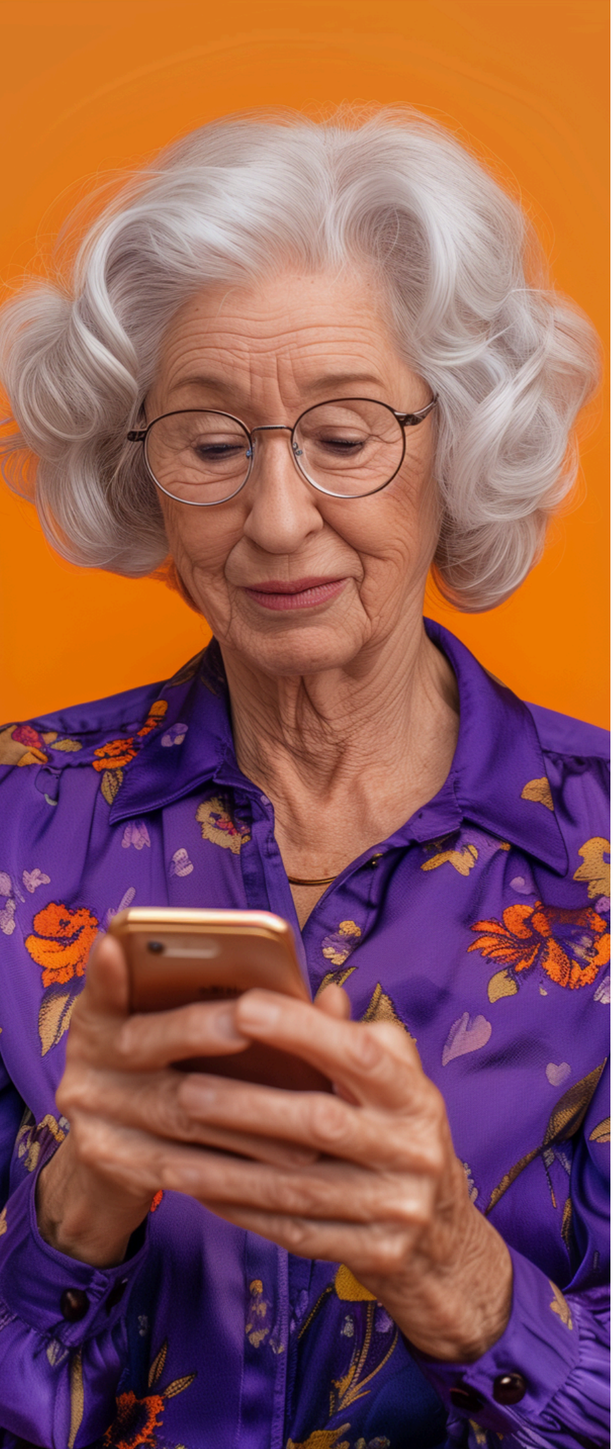
How to take action if you think you have been a victim of a Identity Theft Scam

- Contact your credit card company, banking institution, or Medicare to report the fraud and secure your accounts.
- Report it to the Federal Trade Commission online or by calling
- 877-FTC-HELP (877-382-4357)
- Call the Elder Helpline toll-free at 1-800-963-533

REPORTING FRAUD

If you or someone you know has been a victim of elder fraud, help is standing by at the National Elder Fraud Hotline.

833-FRAUD-11 or 833-372-8311



National Do Not Call Registry

Register your phone number to report stop or block unwanted, annoying,telemarketing, spam calls, robocalls to the FTC

https://www.donotcall.gov/

Report Fraud

Protect your community by reporting fraud, scams, and bad business practices

https://reportfraud.ftc.gov/assistant

IdentityTheft.gov

Recovering from identity theft is a process. Here's step- by-step advice that can help you limit the damage,…

https://www.identitytheft.gov/

National Elder Fraud Hotline

If you or someone you know is a victim of elder fraud, call this hotline at 833-FRAUD-11. A case manager wi…

https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope#what-to-expect-when-you-call

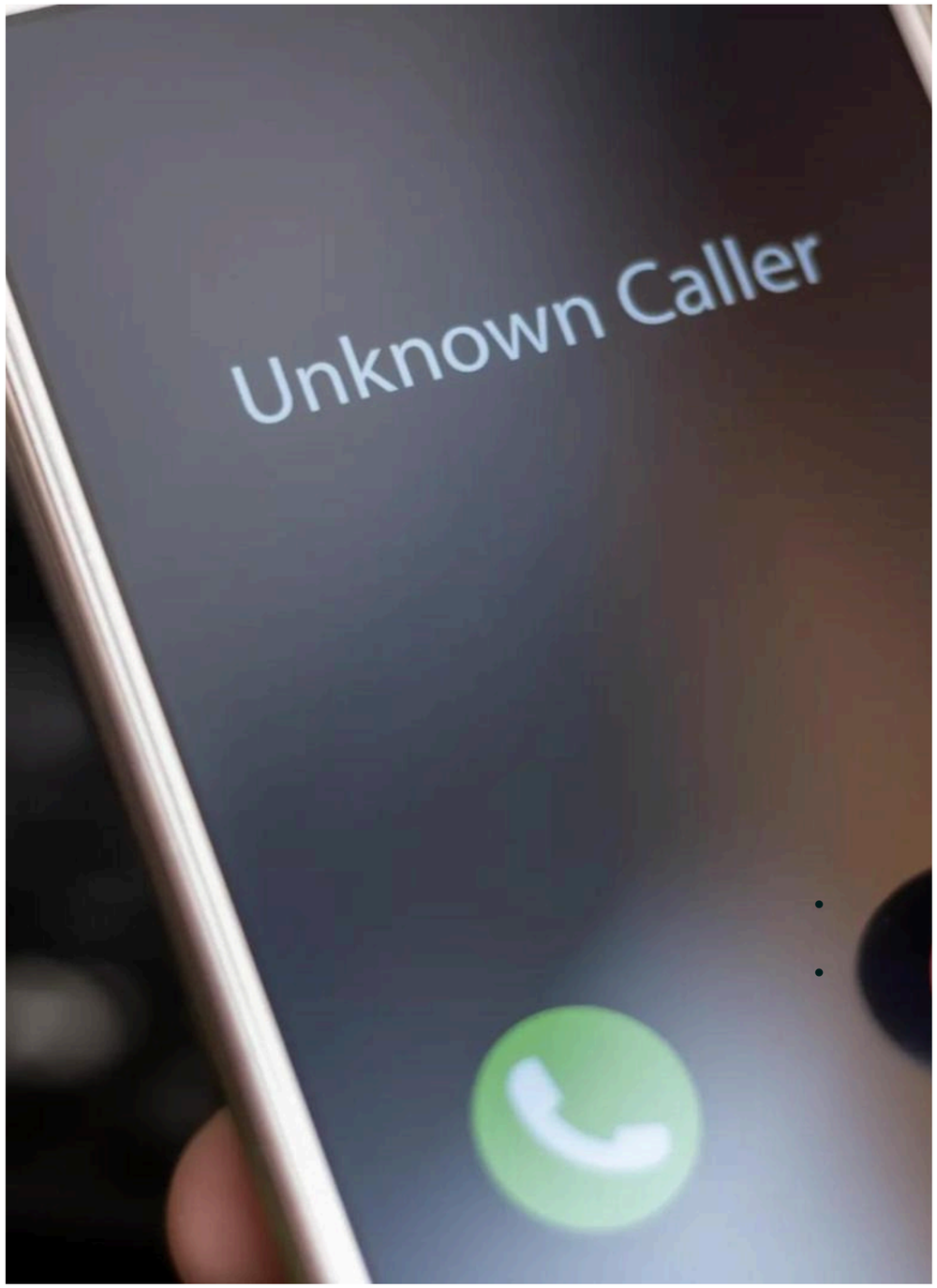
After you've taken action to address the immediate threat, it's time to **Take Back Control**. This step is all about reclaiming your security and ensuring long-term protection against future scams. Whether it involves updating your security settings, monitoring your financial accounts, or seeking professional advice, taking

proactive measures can help you restore confidence and peace of mind. Remember, every action you take strengthens your defenses and makes it harder for fraudsters to target you again. By staying vigilant and continuously safeguarding your personal information, you empower yourself to live with the assurance that your financial and personal well-being are secure.

STEP #3 'TAKE CONTROL'

Scammers target everyone, no matter their age or circumstance, if you have been a target of fraud, it's not your fault, scams targeting Medicare individuals are, unfortunately, very common.

Here are a few simple ways to take back control and better advocate for your future.

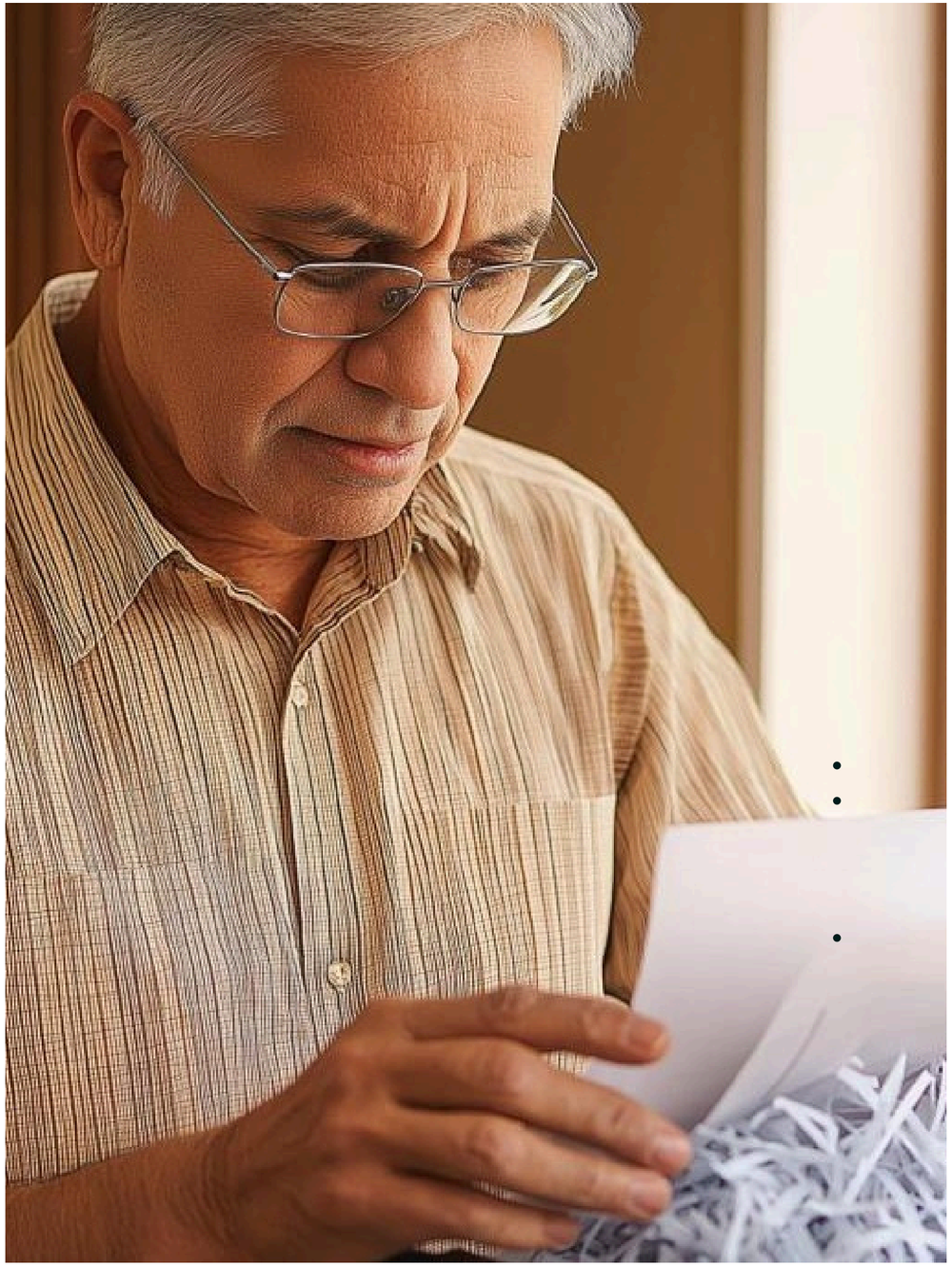


How to take back control after you have been a victim of a Medicare Telemarketing Scam

- Familiarize yourself with common scammer tactics, so you are less likely to fall prey to a scam in the future.
- Don’t answer calls from unknown numbers — Register your number on the FTC’s Do Not Call List.
- If a caller asks you to press a number on your keypad to stop their calls, don’t do it.
- Whenever someone calls you claiming to be from a company, hang up and call the company back using the official phone number on the company’s website.

How to take back control after you have been a victim of a Financial Fraud Scam.

- Safeguard your Social Security number and Medicare Card Don’t answer calls from unknown numbers — Register your number on the FTC’s Do Not Call List.
- Stolen mail is one of the easiest paths to a stolen identity. - Watch your mailbox!
- Check your credit reports regularly and monitor financial and medical statements

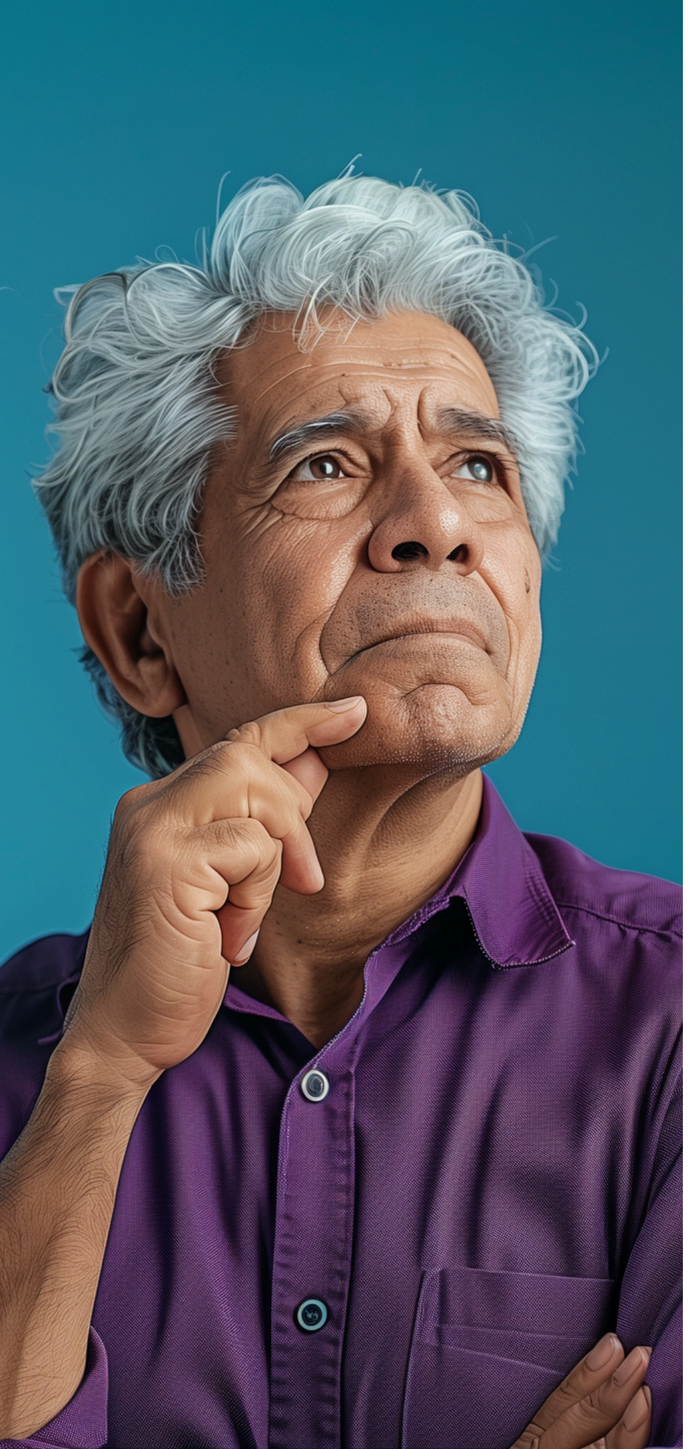


How to take back control after you have been a victim of a Identity Theft Scam

- Safeguard your Social Security number and Medicare Card Don’t answer calls from unknown numbers — Register your number on the FTC’s Do Not Call List.
- Switch to paperless billing and financial statements, so you get less sensitive information in the mail.
- Shred bank statements, tax forms, medical bills, and other documents containing personal or financial data.

As you Take Back Control, remember that this process is not just about reacting to a single scam, but about building a resilient defense against future threats. By reinforcing your security measures, staying informed about potential risks, and maintaining a proactive stance, you ensure that you are better prepared to handle any challenges that may arise.

Taking back control is about more than just regaining what was lost—it's about empowering yourself with the knowledge and tools to protect



RESOURCES FOR THE FUTURE

National Elder Fraud Hotline

If you or someone you know is a victim of elder fraud, we encourage you to call the Hotline at 833-FRAUD-11 (833-372- 8311). Professional case managers will assist you with reporting the crime and connect you with other resources as needed. The hotline is open Monday through Friday from 10:00 a.m. to 6:00 p.m., eastern time.

National Council on Aging: Savvy Saving Seniors

This site provides seniors with information on avoiding scams, which can help them stay secure and independent longer.

NIH.GOV Common Scam Report

There are many resources to help you avoid scams. Some resources also have reporting tools if you were the victim of a scam.
https://handls.nih.gov/news/2023-1.pdf

Victims of Crime Act (VOCA)-Funded Elder Abuse Programs

In August of 2016, a new VOCA Rule clarified and expanded states' allowable uses of VOCA victim assistance funding. The rule clarifies and expands how states may expend the funding, and states are looking to support all victims, including victims of elder abuse. This OVC page highlights examples of VOCA-funded elder abuse programs and the VOCA offices that funded them.

FBI Elder Fraud Resource Page

Each year, millions of elderly Americans fall victim to some type of financial fraud or confidence scheme, including romance, lottery, an…
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-sc ams/elder-fraud