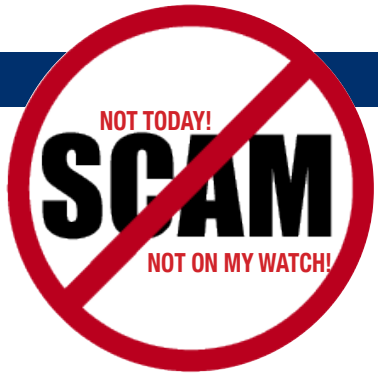
NOVEMBER 2025



BE SAFE | BE INFORMED | BE AWARE

FIGHTING FRAUD with ENOA

Eastern Nebraska Office on Aging
(402) 444-6536 | Blair (402) 426-9614
enoa.org

This Medicare Open Enrollment season, learn how to protect yourself from scams

By BCP Staff

Every year, scammers get more active around Medicare Open Enrollment Period, trying to get your money, information, or both. As you consider your health coverage and prescription options during this period **(October 15-December 7)**, learn to spot the scams.

First, know that scammers often impersonate Medicare and contact you unexpectedly. They might sound professional and even have some of your personal information. They'll say you need a "new" or "updated" Medicare card and ask for your Medicare, bank account, or credit card number. But real Medicare cards are free and mailed to you automatically. And true Medicare representatives won't call, text, or email you out of the blue to ask for your numbers or a payment.

Here are some ways to protect yourself from Medicare scams during Open Enrollment — and year-round:

- **Ignore unexpected calls from anyone who demands you share Medicare, personal, or financial information**. Medicare will only ask you to verify information if you contact them first, and they won't try to sell you anything or tell you to pay for your Medicare card. Only scammers do that.
- **Don't rely on your caller ID**. It might show Medicare's name or phone number, but caller ID can be faked. To check it out, hang up and call 1-800-MEDICARE (1-800-633-4227).
- **Get help to compare costs, coverage, and plans**. Contact your State Health Insurance Assistance Program (SHIP) for assistance. And find information about your coverage options at Medicare.gov — the official U.S. government site for Medicare — or by calling 1-800-MEDICARE.

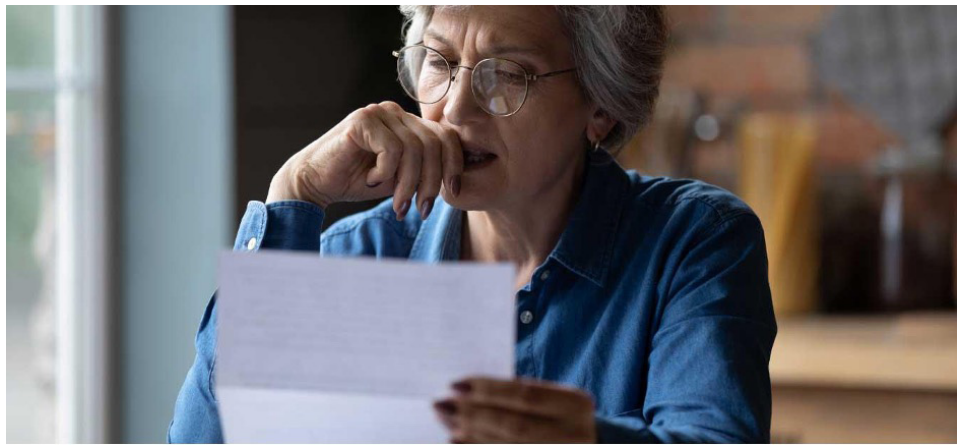
Report Medicare impersonators and other Medicare scams at 1-800-MEDICARE. Then tell the FTC at ReportFraud.ftc.gov.

For additional help to prevent, detect, and report potential Medicare fraud, errors, and abuse, contact your local Senior Medicare Patrol.

Misleading Medicare Marketing: Don't Be Misled During Medicare Open Enrollment

KEY TAKEAWAYS

- During Medicare Open Enrollment (Oct. 15-Dec. 7), ads may mislead you into thinking one plan is better for you than another.
- It's important to understand what brokers and agents from private insurance carriers are and aren't allowed to do.
- Find out what to do if you suspect Medicare fraud or abuse.



During Medicare's Annual Election Period, commonly known as the Medicare Open Enrollment Period (OEP) (Oct. 15 through Dec. 7),you can make changes to you Medicare coverage. If you have original Medicare, you can compare and change prescription drug plans (Part D) and Medigap plans.

You can also decide if, instead of original Medicare, you want to sign up for a Medicare Advantage (MA) plan (Part C).

Unlike original Medicare, Medicare Advantage and Part D plans are administered, marketed, and sold by private insurance companies. During OEP, these companies are actively promoting their plans through television ads, social media ads, radio ads, text messages, phone calls, and mailings. In an attempt to get your interest, the ads may intentionally or unintentionally mislead you into thinking one plan is better for you than another.

It's important to understand what brokers and agents from these private insurance companies are and aren't allowed to do so you aren't misled, and you'll be prepared if an insurance agent or broker tries to enroll you in a Medicare plan that isn't right for you.

Nicole Liebau, SMP Resource Center Strategic Partnership and Engagement Director Older adults (and caregivers) watch out for agents who:

- Start a discussion about other insurance products, like life insurance annuities, if your meeting was scheduled to discuss Medicare Part C or Part D.
- Set their own time limits for you to sign up for a plan. You have until Dec. 7 to enroll, and there are no extra benefits for signing up early.
- Pressure you or even threaten to take away your benefits if you do not sign up for their plan.
- Offer you gifts if you do agree to sign up for their plan.
- Approach you in public and try to sell you a plan.
- Suggest that Medicare endorses or prefers their plan.
- Discuss Medicare products you did not ask to talk about when you filled out a scope of appointment form.
- Ask for your personal information or try to sell you a plan at an educational exhibit.

How to avoid unwanted enrollment in a Medicare plan

According to the Senior Medicare Patrol Center (SMP), you can protect yourself by:

- Keeping your Medicare information private. Only share it with your trusted doctors or other health care providers.

Continued on next page

- Double-checking what you're told. Before signing up for a Medicare plan, confirm all details an insurance agent shares with you.
- Getting it in writing. Always ask for written information so you have proof and can review it carefully.
- Checking with your doctors. Call your preferred providers to be sure they're part of a plan's network before you enroll.

Should I report Medicare fraud?

Yes—you should report potential Medicare marketing violations and/or misleading marketing concerns if you see these red flags:

- You received unsolicited phone calls or text messages. Plans must provide you with the option to opt out of communications. It must be done annually and in writing.
- A company represents itself as coming from or sent by Medicare, Social Security, or Medicaid.
- You received information such as leaflets, flyers, door hangers, etc., on your car or at your residence from a company you did not have an appointment with.
- An agent returns uninvited to your residence after missing an appointment with you earlier.
- You signed up for a plan after being told that certain prescriptions or services were covered. But after reviewing your Explanation of Benefits (EOB), you found they were not covered by the plan and you will have to pay out of pocket.
- You were told you could keep your Medigap (or supplemental) plan when you signed up for a Medicare Advantage plan. In reality, you cannot have both a Medigap plan and a Medicare Advantage plan.

For more information on potential Medicare marketing violations and misleading marketing, visit the Senior Medicare Patrol website. If you suspect Medicare fraud, errors, or abuse, follow these steps outlined by SMP.

"Medicare Open Enrollment brings a surge of aggressive marketing, and some of it crosses the line into misleading or fraudulent tactics," explains Ryan Ramsey, NCOA Associate Director of Health Coverage and Benefits. "Be cautious of anyone who pressures you for immediate decisions, asks for your personal information unsolicited, or makes promises about benefits that seem too good to be true."

Who can help me choose the right Medicare plan?

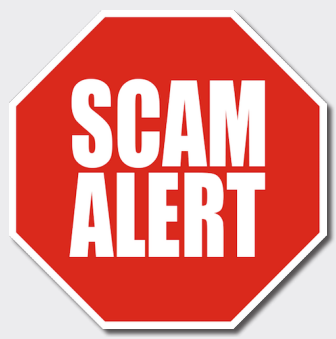
Comparing plans and knowing what is best for you can be overwhelming. And since Medicare fraud and abuse is a reality, it can be hard to know who really has your best interests in mind. That's why NCOA is here to point you in the right direction with resources for free, unbiased Medicare advice.

One way to get reliable help comparing Medicare plans is to call Medicare directly at 1-800-MEDICARE (1-800-633-4227) or start a live chat with a Medicare representative.

You can also contact your State Health Insurance Assistance Program (SHIP). These programs are located in all U.S. states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. Find your local SHIP.

Sources

1. Senior Medicare Patrol Center. Misleading Marketing & Marketing Violations Tip Sheet.



If you spot a scam, report it to the ***FTC*** @ ReportFraud.ftc.gov.

CREDIT FREEZES AND FRAUD ALERTS

Credit freezes and fraud alerts can help protect you from identity theft by making it harder for scammers to open new credit accounts in your name. They can also help stop someone who already stole your identity from misusing it again. Here's what to know about what credit freezes and fraud alerts do and how to use them.

- What To Know About Credit Freezes
- What To Know About Fraud Alerts
- Freezing Your Child's Credit
- Get Your Free Credit Reports

What To Know About Credit Freezes

Freezing your credit can help stop identity theft. When a credit freeze is in place, nobody can open a new credit account in your name. There's no cost to place or lift a credit freeze, and it doesn't affect your credit score.

You don't have to wait for your Social Security number or other information to be exposed in a data breach or misused by an identity thief to get a credit freeze. Anyone can do it, any time.

Credit Freeze

What it does: While a credit freeze is in place, nobody can open a new credit account in your name, including you. If you need to do things like apply for new credit or a job, rent an apartment, or buy insurance, you can temporarily lift the freeze and put it back when you're done.

A credit freeze is always a good idea, but it's even more important if your Social Security number or other information is exposed in a data breach or if an identity thief has misused your information.

Who can place one: Anyone can freeze their credit report, for any reason, even if their identity hasn't been stolen.

How long it lasts: A credit freeze lasts until you lift it.

Cost: Free

How to place one: Contact all three of the credit bureaus — Equifax, Experian, and TransUnion.

When to lift one: Contact the bureau(s) to request it be lifted when you need lenders to access your credit. It is a good idea to identify which bureau a lender will use to check your credit and just lift the freeze at that one bureau, and then put the freeze back in place once the need for a credit check passes.

What To Know About Fraud Alerts

Even if you already have a credit freeze in place, you can also place a fraud alert. Fraud alerts make lenders verify your identity before they grant new credit in your name. There are three types of alerts, and which is best depends on your situation and needs.

Initial fraud alert

What it does: An initial fraud alert tells businesses to check with you before opening a new credit account in your name. Usually, that means contacting you first to make sure the person trying to open a new account is really you. Unlike a credit freeze, a fraud alert doesn't prevent businesses from seeing your credit report.

Who can place one: Anyone who is or suspects they may be affected by identity theft. When you place an initial fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus.

How long it lasts: An initial fraud alert lasts one year, but you can renew it.

Cost: Free

How to place one: Contact one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an initial fraud alert on your credit report.

Extended fraud alert

What it does: Like an initial fraud alert, an extended fraud alert tells businesses to check with you before opening a new credit account in your name, and doesn't prevent businesses from seeing your credit report.

An extended fraud alert also requires the credit bureaus to take you off their marketing lists for unsolicited credit and insurance offers for five years, unless you ask them not to.

Continued on next page

Who can place one: People who have experienced identity theft and have completed an FTC identity theft report at IdentityTheft.gov or filed a police report.

How long it lasts: An extended fraud alert lasts seven years. You'll have the choice to renew it, but you'll have to resubmit your FTC identity theft report or police report.

Cost: Free

How to place one: Contact one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an extended fraud alert on your credit report.

Active duty alert

What it does: As an active duty servicemember, placing an active duty fraud alert tells businesses to check with you before opening a new credit account in your name. Usually, that means contacting you first to make sure the person trying to open a new account is really you.

An active duty fraud alert also requires the credit bureaus to take you off their marketing lists for unsolicited credit and insurance offers for two years, unless you ask them not to.

Who can place one: Active duty servicemembers.

How long it lasts: An active duty fraud alert lasts one year. After a year, you'll have the choice to renew it for the length of your deployment.

Cost: Free

How to place one: Contact one of the three credit bureaus — Equifax, Experian, or TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an active duty fraud alert on your credit report.

Free credit monitoring for active duty servicemembers and National Guard members

Active duty servicemembers and National Guard members can also get free electronic credit monitoring to help detect problems that might be the result of identity theft. To sign up, contact each of the three credit bureaus — Equifax, Experian, and TransUnion.

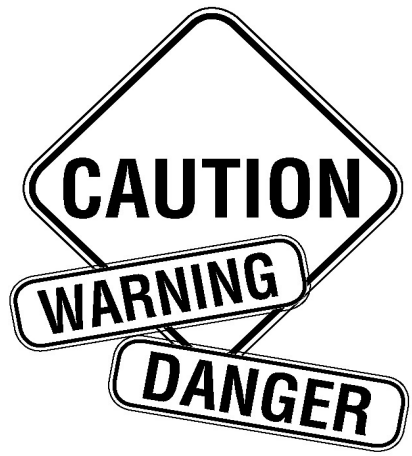
Freezing Your Child's Credit

If your child is under 16, request a free credit freeze to make it harder for someone to open new accounts in your child's name. The freeze stays in place until you tell the credit bureaus to remove it. The process for getting a freeze for a minor is different than getting one for an adult. The credit bureaus give specific instructions at these three sites:

- Experian
- Equifax
- TransUnion

Get Your Free Credit Reports

It's also a good idea to regularly check what's in your credit report. Accounts in your name that you don't recognize could be a sign of identity theft. Here's how to get your free credit reports.



If you see the signs
Take the time….

TO STOP
ELDER ABUSE

Report Abuse and
Neglect of the Elderly
or
Vulnerable Adults

Call **1-800-652-1999**

Nebraska Adult
Protective Services

ENOA

*Calls can be made anonymously

How Scammers Try To Steal Your Life Savings

People are losing big money to scammers running complicated scams.

Here's how the scam works:

A scammer pretending to be from a company you know contacts you, saying they supposedly spotted fraud on one of your accounts and your money isn't safe.

They connect you with someone else to supposedly help you move your money to "protect" it.

The "helper"— who often claims to work for the government — is really a scammer trying to steal your money.

If someone tells you to do any of these things, it's a scam.

- "Put your money in a secure account to protect it." **That's a scam.**
- "Transfer your money to a cryptocurrency account to protect it." **That's a scam.**
- "Get cash and I'll send a driver to pick it up." **That's a scam.**
- "Deposit cash at a Bitcoin ATM to protect your money." **That's a scam.**
- "Buy gold and a driver will come get it." **That's a scam.**

No one from the government will tell you to do these things. **Only a scammer will.**

Never transfer or send money, cryptocurrency, cash, or gold to someone you don't know in response to an unexpected call or message.

FEDERAL TRADE COMMISSION

More at ftc.gov/imposters

Report scams to the Federal Trade Commission at ReportFraud.ftc.gov

November 2024