

# PROTECT YOURSELF FROM COMMON CONSUMER SCAMS



*Connecticut's Senior Medicare Patrol (SMP) Program helps Medicare and Medicaid beneficiaries prevent, detect and report suspected health care fraud and abuse.*

*The Consumer Law Project for Elders is a project of Connecticut Legal Services, Inc.*

## THIS BOOKLET TELLS YOU:

- What a scam is.....2
- Why seniors are frequent targets of scams.....2
- Who the scammers are.....2
- What the most common scams are.....3-8
- What you can do to prevent becoming a victim  
of a scam.....9
- Who to contact if you are a victim of a scam.....10

## COMMON SCAMS

### ►►►► Medicare Scams:

- You receive a Medicare Summary Notice and don't recognize the doctor or service.
  - Some unscrupulous medical providers bill Medicare for services or equipment you never received.

***ALWAYS CHECK YOUR MEDICARE SUMMARY NOTICE AND REPORT ANY ITEM YOU THINK IS INCORRECT.***

Call: Medicare 1-800-633-4227

or The Senior Medicare Patrol (SMP) program 1-800-994-9422.

- You receive a call from someone claiming to be a Medicare employee or insurance representative who asks for personal information including Social Security and/or bank account numbers.
  - No one from Medicare or other insurance companies will call you and ask for that information.

***NEVER GIVE OUT YOUR MEDICARE NUMBER OR OTHER PERSONAL INFORMATION IF YOU GET A CALL LIKE THIS.***

### ►►►► Medical Identity Theft Scam:

- Medical identity theft occurs when a scammer gets your Medicare and other insurance information and uses it to receive health care. If any of the situations listed below happens to you, you could be a victim of medical identity theft.
- You receive a bill for medical services you didn't receive.
- A debt collector contacts you about medical debt you don't owe.
- You try to make a legitimate insurance claim and Medicare says you have reached your limit on benefits when you know you haven't.
- You are denied coverage because your medical records show a condition you do not have.

***PROTECT YOUR MEDICARE AND OTHER HEALTH INSURANCE CARDS. KEEP THEM IN A SAFE PLACE.***

### ▶▶▶▶ *Grandparent Scam: (phone)*

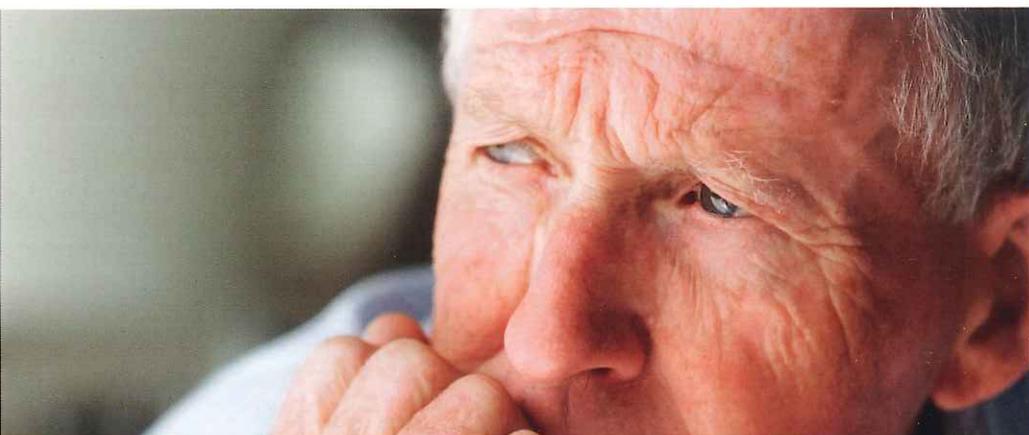
You receive a phone call from someone who says he is a loved one (e.g., your grandchild) and is in trouble with the police, in the hospital, or stuck in another country, and needs money. He tells you not to tell his parents and to wire the money to a specific location. You send the money, but then you find out it was not your grandchild calling and the scammer now has your money.

***NEVER SEND ANY MONEY WITHOUT CHECKING WITH OTHERS TO BE SURE THIS CALL IS REAL.***

### ▶▶▶▶ *Counterfeit Check Scam: (mail)*

You receive a letter in the mail stating you have won money (e.g., a million dollars). Enclosed is a large check. You are told to cash the check, keep a small amount of the money for yourself but send most of it back to the sender to cover taxes or processing fees. Because you are told you can keep some of the money, you trust the sender and do as you are told. Soon you learn that the check has bounced because this was a scam. Your bank then comes after you to pay back the money it paid out to you.

***NEVER SEND MONEY TO ANYONE IN ORDER TO RECEIVE MONEY YOU HAVE "WON."***



***No one from Medicare or other insurance companies will call you and ask for personal information.***

▶▶▶▶ *Prize Offers and Sweepstakes Scam:*  
(telephone, mail, internet)

You are contacted by someone who offers you a "free" prize or says you have won something. The person then requests a fee to process your "winning entry," or you are told you have to do something to obtain the prize - attend a sales presentation, buy something, or give out a credit card number. The scammer is trying to rope you in with these offers, hoping to get money or personal information from you.

*NEVER GIVE MONEY TO ANYONE IN ORDER TO RECEIVE A PRIZE.*

▶▶▶▶ *Nigerian Scam: (telephone, mail, internet)*

You receive a call or email from someone who claims to be a foreign official, business person or the spouse of a former government official. He tells you that he needs to move millions of dollars out of the country. He says he needs your help and offers you a huge reward for your help. He then requests your bank account numbers, blank checks, or cash to help cover the transaction. Once the scammer has your money, he disappears.

*NEVER GIVE OUT PERSONAL INFORMATION TO SOMEONE YOU DO NOT KNOW.*

▶▶▶▶ *Spoofing Scam: (telephone, internet)*

You receive a call from someone claiming to be a police officer investigating a fraud ring preying on elderly homeowners in your local area. Your caller ID shows the call comes from your local police department. The caller asks you to verify your name, Social Security number, bank account and credit card numbers and other personal information. The caller has "spoofed" you by using technology to cause a false identifier to appear on your caller ID. The spoofer now has your personal information and can obtain credit, loans or take money from your bank account.

*NEVER GIVE OUT PERSONAL INFORMATION TO SOMEONE YOU DO NOT KNOW.*

➤➤➤ *Phishing Scam: (internet)*

You are emailed a document on letterhead of a legitimate company such as your bank, a government agency or a credit card company. The email tells you that the company is updating records, or that there has been a security breach and it needs to verify your information. You are asked to provide personal information, such as your Social Security number, bank account or credit card numbers. This is called "phishing" as the scammer is using fake letterhead to "fish" for personal information from people. The phisher then uses the personal information you provide to commit fraud.

***NEVER GIVE OUT PERSONAL INFORMATION BY EMAIL OR THE INTERNET TO SOMEONE YOU DO NOT KNOW.***



*Never give out personal information to someone you do not know.*

### ►►►► *Fake Charities Scam: (telephone, internet)*

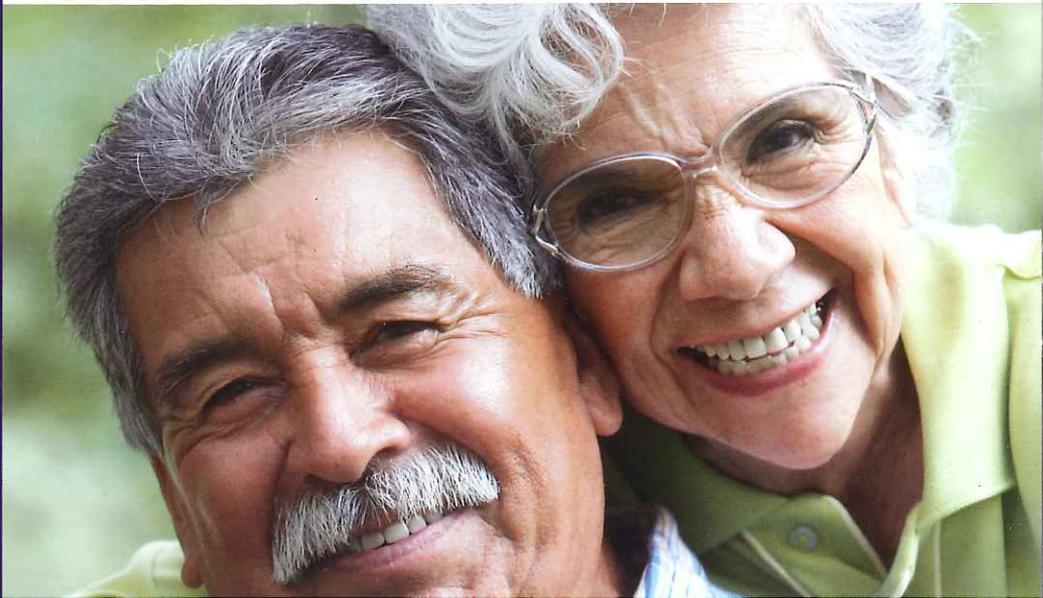
You receive a call or e-mail from someone who claims to be contacting you on behalf of a charity whose name may sound familiar to you but is really a phony charity. The caller asks for a donation by credit card or electronic bank withdrawal. If you ask to be sent something in writing, the caller refuses to send anything to you. If you provide the requested information, the scammer will use your credit card or take money from your bank account.

***NEVER GIVE OUT PERSONAL INFORMATION BY TELEPHONE OR EMAIL UNLESS YOU MADE THE CONTACT YOURSELF.***

### ►►►► *Home Repair Scam: (in person)*

Your door bell rings and at the door is someone who says he is a home repair contractor doing work in the neighborhood. He offers to look over your house to see if you need any work done. He then may offer to do a small job for a low fee as long as you let him do the work immediately. Once the work is done, he asks for a much higher fee. Or, he may tell you that you need more costly work done, such as a new roof or new windows that he will be happy to do, but he needs the full cost of the job upfront. Once paid, the scammer does a poor quality job or never shows up to do the job. In addition, if the repair allows the scammer to be inside your house, your valuables could be at risk.

***ALWAYS CHECK THE LICENSE AND REPUTATION OF HOME REPAIR CONTRACTORS BEFORE HIRING THEM.***



### ➤➤➤➤ *Home Rescue Scam:*

*(telephone, mail, internet, in person)*

You are contacted by a company claiming it has learned you are in financial difficulty and facing foreclosure. The company tells you that it can save you from foreclosure with a loan. You agree to the loan and sign a stack of papers without reading them. Without knowing, you sign the title of your home over to the scammer. You find out much later, when the scammer tries to evict you, that you no longer own the home and the money you have been paying each month on this so-called loan is rent.

***NEVER GIVE OUT PERSONAL INFORMATION FOR A LOAN UNLESS YOU MADE THE CONTACT YOURSELF.***

### ➤➤➤➤ *Recovery Scams:*

*(telephone, mail, internet, in person)*

Beware! If you are a victim of any scam, you will likely to be contacted again by someone promising to get back any money you have lost to a scammer. This is another scam. Scammer's sell victims lists to other scammers who contact those already scammed and offer to recover their money for a fee. Be careful not to lose more money in this common practice.

***Never give out personal information for a loan unless you made the contact yourself.***



## *How can you avoid being scammed?*

The goal in all of these scams is the same, to get your personal information allowing access to your credit cards, bank or investment accounts, and/or health insurance. While anyone can become a victim of a scam, here are some tips to help avoid being victimized by a scam artist:

- Never give personal information over the phone or by email or the internet unless you are familiar with the company/person or you made the contact yourself. **Remember, Medicare, your bank and other legitimate companies will never ask for personal information over the phone, by email or the internet.**
- Never wire any money to someone unless you are sure it is someone you know.
- Don't cash checks you receive in the mail unless you are certain you trust who the check is from.
- Don't fall for "get rich quick" schemes. If something sounds too good to be true, it is probably a scam.
- Verify any phone, email or internet requests for money or personal information by contacting the person or company directly using a telephone number or email/web address you have looked up yourself and know to be genuine.
- Don't respond to emails from financial institutions or companies asking for verification of personal information.
- Don't click on links in any unsolicited email from someone you don't know.
- Don't make charitable donations over the phone. Have the caller send you a paper contribution form.
- Beware of any salesperson or contractor who insists you give or send money to them immediately.
- Check out a company or individual with the CT Department of Consumer Protection 1-800-842-2649, Better Business Bureau 203-269-2700, or law enforcement agencies before you do business with them.
- Never pay in full upfront for any work that is to be done on your house.
- Be certain you are on a secure internet site before entering any personal information to purchase goods. Look for the little padlock sign in the address block that shows the site is secure.
- Consider first discussing any plan to sign a contract or purchase an expensive product with a trusted family member, friend or lawyer.

## *Who can I contact if I think I may be a victim of a scam?*

### **To report Medicare and other health care related scams:**

CT's Senior Medicare Patrol (SMP) program: 1-800-994-9422  
(operated by the CHOICES program at your local Area Agency on Aging)

Centers for Medicare & Medicaid Services

Call: 1-800-633-4227

TTY: 1-877-486-2048

Mail: Medicare Beneficiary Contact Center

P.O. Box 39

Lawrence, KS 66044

HHS Office of Inspector General

Call: 1-800-477-8477

TTY: 1-800-377-4950

Online: [Report Fraud Online](#)

Mail: HHS Tips Hotline

P.O. Box 23489

Washington, DC 20026-3489

U.S. Senate Special Committee on Aging - Fraud Hotline (toll-free)

Call: 1-855-303-9470

Online: <http://www.aging.senate.gov/fraud-hotline>

Connecticut Attorney General's Office

Call: 1-860-808-5354

Fax: 1-860-808-5033

Email: [ag.fraud@ct.gov](mailto:ag.fraud@ct.gov)

Mail: Office of the Attorney General

State of Connecticut

Antitrust and Government Program Fraud Department

Fraud Complaint

P.O. Box 120

Hartford, CT 06141-0120

### **All other scams:**

Your local police department

The Consumer Law Project for Elders: 1-800-296-1467

(free legal assistance with consumer problems for CT residents ages 60 and over)

Connecticut Department of Consumer Protection: 1-800-842-2649

Better Business Bureau: 203-269-2700

Federal Trade Commission: 1-877-FTC-HELP (1-877-382-4357)

## *WHAT IS A SCAM?*

Fraud, commonly known as a scam, is a crime that involves deceit, dishonesty, and/or swindling. People who commit scams are known as scammers or scam artists. Scammers try to get money or personal information from you, such as your Social Security, Medicare, bank account or credit card numbers. Scammers then use that personal information to obtain goods and services in your name or to take money from your accounts.

## *WHY ARE SENIORS POPULAR TARGETS OF SCAMMERS?*

Several reasons have been given by experts.

Seniors often:

- Have money (pension, Social Security, savings) or assets (a home, stocks and bonds);
- Are home during the day and easy to contact;
- Tend to trust people, especially those who are polite;
- Are isolated and more willing to talk to strangers;
- Are more easily intimidated and less likely to take action or complain.

## *WHO ARE THE SCAMMERS?*

**Strangers.** We all know to beware of strangers but people can still easily fall victim to them. Be very wary of any new person in your life, even a new romantic interest, who wants to help with your finances or who asks for money or personal information.

**Family, friends and neighbors.** Sad as it is, people are often taken advantage of by their loved ones. Use good judgment when sharing your personal information with anyone, even your children.

You Have  
**CHOICES**



**1-800-994-9422**

This publication was developed by Connecticut Legal Services, Inc. Consumer Law Project for Elders. It was supported in part by a grant (No. 90MP0185-02) from the administration on Aging (AoA), Administration for Community Living (ACL), U.S. Department of Health and Human Services (DHHS). Grantees carrying out projects under government sponsorship are encouraged to express freely their findings and conclusions. Therefore, points of view or opinions do not necessarily represent official AoA, ACL or DHHS policy.

**The Consumer Law Project for Elders** provides free legal assistance to Connecticut residents 60 and over who have consumer problems. Call **1-800-296-1467**.

**Connecticut's Senior Medicare Patrol (SMP)** program helps Medicare and Medicaid beneficiaries prevent, detect and report suspected health care fraud and abuse. Call **1-800-994-9422**.