DECEMBER 2023

BE SAFE | BE INFORMED | BE AWARE

FIGHTING FRAUD with ENOA

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

8 Scams That Senior Medicare Patrols Are Seeing Now

Old deceptions are recycled to take advantage of what you know from news reports.

By Kimberly Lankford, AARP

Senior Medicare Patrol volunteers are often the first to identify new Medicare scams because they meet one-on-one with Medicare beneficiaries. Here are some of the top scams they're seeing and what you can do to protect yourself:

1. A new round of COVID fraud

During the height of COVID-19, criminals offered free coronavirus tests as a way to gather people's Medicare numbers and other personal information and file fake claims in their name.

"Somebody calls unsolicited, offering to send a COVID test," says Tiffany Erhard, New York state Senior Medicare Patrol director. "They aren't sending real tests, but they're billing as if they are, and they're taking the person's information to use it unscrupulously or sell it."

After a major investigation, the Department of Health and Human Services Office of Inspector General charged 18 defendants in nine federal districts across the U.S. for making more than $490 million in COVID-related false billings.

The scam died down but resurfaced near the end of the public health emergency, which officially expired May 11, 2023. Senior Medicare Patrols reported seven COVID complaints in January 2023, then suddenly had 72 in April.

"They're using the end of the public health emergency to try to get personal information and Medicare numbers," says Director Rebecca Kinney of the Administration for Community Living's office of health care information and counseling. Her division of the U.S. Department of Health and Human Services (HHS) finances the Senior Medicare Patrol program.

Note: You can get four free COVID tests in the mail by requesting them at covid.gov/tests.

2. Bills for diabetes supplies

Volunteers in the Lone Star State report an increase in diabetes supply scams, says Diane Nguyen, program director for the Texas Senior Medicare Patrol.

Claims for continuous glucose monitoring devices are showing up on Medicare summary notices for people who don't have diabetes and didn't receive the device, she says. The scammers charge Medicare.

"The only reason we are seeing these cases is that people are checking their Medicare summary notices," Nguyen says.

3. Flimsy medical equipment

This is a long-standing Medicare problem.

Con artists offer you a knee brace or other medical equipment if you give them your Medicare number. You'll get a cheap brace in the mail that you could have purchased at a drugstore, or you might receive no brace at all.

The criminals charge Medicare for an expensive brace and make other unauthorized charges with your number. In 2019, Senior Medicare Patrol volunteers helped uncover an international fraud ring that had charged Medicare $1.2 billion in false durable medical equipment claims.

4. Bogus genetic testing

Even though the Senior Medicare Patrol helped uncover a $2.1 billion genetic testing scam, phony pitches are still an issue.

Someone at a health fair might offer to swab your cheek and test the sample to determine whether you have a genetic propensity for cancer. You need to give your Medicare number to cover the test, the con artist says.

Continued on next page

In reality, Medicare rarely covers genetic testing. Scammers use the ploy to get your Medicare number and make all sorts of fraudulent charges in your name.

"Many times, they would not get the test [results] at all," Maria Alvarez, executive director of New York Statewide Senior Action Council, says of Medicare beneficiaries. The nonprofit runs New York's Senior Medicare Patrol program. "They [the scammers] would just discard the swabs and use the Medicare number."

5. Hospice fraud

Much like a 2021 California case, scammers enroll people who aren't terminally ill in hospice without their knowledge. The Medicare beneficiaries instead may believe they are signing up for extra benefits programs, such as home cleaning, in-home nurse visits or a shower chair.

"They have a doctor that works with them and is 'diagnosing people' and sending paperwork to Medicare and claiming thousands of dollars that Medicare pays for in hospice," says Carolina Oehler, the Senior Medicare Patrol liaison for the Kern County Aging & Adult Services Department in California.

The criminals receive payment from Medicare for hospice services never delivered. The Medicare beneficiary has legitimate nonhospice claims denied.

6. Medicaid 'unwinding'

During the COVID public health emergency, beneficiaries of Medicaid, the federal-state health insurance for low-income Americans, didn't need to recertify eligibility based on their income. When the emergency ended in May, states began to ask Medicaid recipients for recertification.

"Scammers are using that as a way to get to people," Kinney says. "We've heard cases of scammers calling Medicaid beneficiaries and telling them they need to pay them, so they don't lose Medicaid. Or they're using it to get [beneficiaries'] personal information."

7. Next generation Medicare cards

Medicare saw a big increase in card scams in 2018 when the government sent every beneficiary new cards that didn't include Social Security numbers. Senior Medicare Patrol volunteers are seeing some card scams resurfacing.

"We had an influx of people reporting to the SMP volunteers that they were receiving unsolicited calls from people who were falsely claiming to be a Medicare representative and offering a new card, maybe a plastic card with a chip," Erhard says.

The scammers ask for money for the new card or ask for your Medicare number. Medicare won't call you to offer a new card, its cards are paper stock and you can print an official card from your online Medicare account anytime.

What's more, Medicare won't ever call you without scheduling an appointment ahead of time.

8. Telemedicine sessions

"You may get a call from somebody who is trying to sell you something, and then you'll get billed for a telehealth consult," says Jean Stone, a 40-year Centers for Medicare & Medicaid Services employee who in retirement is a New York Senior Medicare Patrol volunteer.

Sometimes the fraud is tied to fake genetic testing or flimsy medical equipment, and the criminals will add a telemedicine appointment to the Medicare bill.

Kimberly Lankford is a contributing writer who covers Medicare and personal finance. She wrote about insurance, Medicare, retirement and taxes for more than 20 years at Kiplinger's Personal Finance and has written for The Washington Post and Boston Globe. She received the personal finance Best in Business award from the Society of American Business Editors and Writers and the New York State Society of CPAs' excellence in financial journalism award for her guide to Medicare.

All Covered Security Tips - IRS and Tax Scams

Every year, the bad guys take advantage of innocent taxpayers, like you, who are patiently waiting on their tax return.

Last year, the IRS noticed a significant increase in phishing attempts to steal money or tax data, therefore you must be on high alert.

How it Happens: Tax Scams and Malicious Activity

The bad guys have a number of tax-related tricks up their sleeves when it comes to stealing your money and/or sensitive information. Here are a few examples of sophisticated tax scams that have been found in the wild:

- Scammers send emails posing as tax service companies by spoofing emails and using stolen logos. Once you respond to the email with personal data or tax information, they can pocket your hard-earned money.
- Similar to the scam above, the bad guys send look-alike emails containing hyperlinks that lead you to malicious websites or fake PDF attachments that download malware or viruses to your computer.
- Tax scams aren't limited to emails! Be on the look out for callers posing as IRS representatives claiming you owe money that must be paid immediately. The callers typically threaten arrests, deportation, or suspension of business or driver's license.

Keep in mind, these are only a few examples and these scam artists are constantly coming up with new ways to fool you.

Continued on next page

How Do I Know it's a Scam?

Always remember the following during tax season, and all year long:

- The IRS will always mail a bill before calling you about taxes owed.
- The IRS will never ask for credit or debit card numbers over the phone.
- The IRS will never immediately threaten to arrest you for not paying taxes owed.
- The IRS will always offer the opportunity to question or appeal the amount owed before demanding your payment.
- The IRS does not use emails or text messages to discuss personal tax matters, such as taxes owed or tax refunds.

Only share sensitive data over email when there is no other alternative and you're certain the recipient is valid.

Stop Look Think - Don't be fooled

The All Covered Security Team

Legal Aid OF NEBRASKA

ARE YOU 60 YEARS OF AGE OR OLDER?

Legal Aid of Nebraska provides legal advice and assistance to Nebraska residents 60 years of age and older through our ElderAccessline®.

Phone calls to the ElderAccessline® are answered by an experienced attorney or paralegal who will ask you questions about your situation.

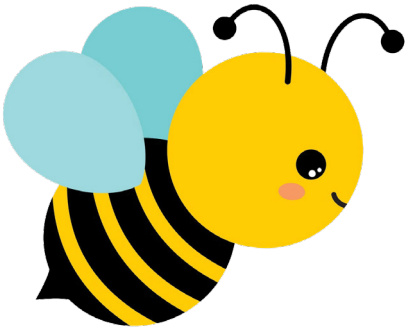
ELDERACCESSLINE®
Toll-free: 1-800-527-7249
In Omaha: 402-827-5656
HOURS OF OPERATION:
Monday - Thursday
9 a.m. to Noon CST
1 p.m. to 3 p.m. CST
Friday
9 a.m. to Noon CST

WE CAN HELP YOU WITH ...

Collections | Medicare/Medicaid | Consumer Protection
Advanced Directives/Living Wills | Simple Wills
Power of Attorney | Homestead Exemption
Tenant Issues | And other legal concerns

Serving Nebraska's seniors in all 93 countries

VISIT US AT LEGALAIDOFNEBRASKA.ORG



BE THE DIFFERENCE

Honey, it's worth it!

Report Abuse and Neglect of the Elderly or Vulnerable Adults

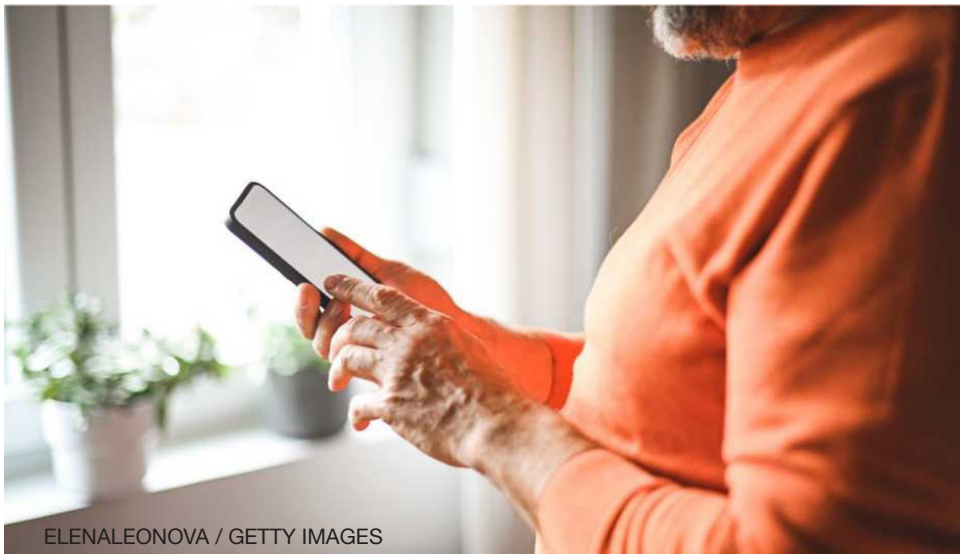
Call **1-800-652-1999**

Nebraska Adult Protective Services

Bank Impersonation Is the Most Common Text Scam: What You Need to Know

It can be hard to tell whether you're being contacted by your bank or a criminal | Patrick J. Kiger, AARP

Last year, Pittsburgh resident Molly Sinclair, 54, suddenly received ominous-sounding messages from two local banks where she's a customer. One warned her that her account had been locked because of unusual activity, and instructed her to click a link in order to verify the transaction. The other simply said that her account was locked, and gave her a phone number to call.



ELENALEONOVA / GETTY IMAGES

Skeptical but alarmed, Sinclair got on her laptop, and went to the website for one of her banks, just to reassure herself that her money was still there. "The first thing that popped up on its homepage was a scam alert," she recalls. It warned about fake text notifications of the sort she had received. She's glad she didn't click on that link or make that call.

You've probably received these messages, too: The Federal Trade Commission (FTC) recently reported that text messages pretending to be from banks are up nearly twentyfold since 2019. They're now the most common type of text-based fraud, costing victims a median loss of $3,000 each. (These crimes are notoriously underreported, however, so the number of people affected and the amount lost are probably far higher.)

If you have signed up for text notifications from your bank, it's easy to mistake the scam texts for legitimate bank alerts. After all — as we all know — fraud is rampant.

"People are accustomed to getting texts from banks to prevent fraud," notes Emma Fletcher, a senior data researcher in the Division of Consumer Response and Operations for the FTC. "There's a certain irony that scammers are now using this to perpetrate fraud."

How bank impersonation scams work

Bank-impersonation scammers pretend to be security departments at banks, and send out text messages, emails and robocalls that supposedly warn people of unusual, possibly fraudulent activity that requires immediate action. In reality, they're trying to get people to provide account numbers and login information, or to transfer their funds for safekeeping into accounts controlled by the criminals. In the process, they also may steal targets' personal information, which can be used to commit identity fraud.

Some fake bank notification texts warn that an account has been locked, while others ask the target to verify a large purchase that supposedly has been made at a store. "If they reply 'no,' which many people might do reflexively, they'll get a call from someone claiming to be the bank," Fletcher says.

Fake bank messages try to create a sense of urgency

Typically, a scammer on the phone will try to alarm the people being targeted, saying that they must take immediate action to protect their accounts from being emptied.

"They will be walked through a series of steps that they've been led to believe will cause the fraudulent purchase or transfer to be reversed," Fletcher says. But the money is actually being transferred into the criminal's account.

Sometimes, the scammers will guide targets to sophisticated replicas of actual bank websites.

Continued on next page

"Other than a different web address, you really can't tell that they're fake," explains Aaron Foss, founder of Nomorobo, a security company that specializes in blocking robocalls and spam text messages for its clients. "They use fear to get people to quickly tap on the link and not look at the URL too closely."

The object in such cases is to steal victims' login credentials and other personal data.

Bank impersonation robocalls, meanwhile, aim to connect victims to a live scammer, who then carries out the scams noted above. Or sometimes, the criminal on the phone will tell victims to download remote-access software, which people don't realize will actually give the scammers access to their computers, Foss says.

How to protect yourself against bank text scams

Some tips from the American Bankers Association and other sources include:

- **Never click on links on texts or emails in a text or email notification.** Instead, go to the bank's website (even if you've signed up for text alerts). Use the URL listed on your statements or that you've previously bookmarked, and check for any alerts on your account.
- **If you get a robocall or call from someone claiming to be from your bank, hang up.** Then contact your bank in a way you know to be legitimate, either online or by calling the phone number on your statement or debit card.
- **Never provide account data or personal info.** As ABA's Banksneveraskthat.com website explains, "our bank will never ask for your PIN, password, or one-time login code in a text message. If you receive a text message asking for personal information, it's a scam."
- **Don't rely on caller ID.** Scammers can use technological tricks to display actual bank phone numbers or even the name of the bank.
- **Be wary of a message or caller insisting that you take immediate action.** Scammers try to put you under pressure to act quickly, to make it more difficult for you to think clearly.
- **When in doubt, seek assistance.** If you're unsure what to do in response to what appears to be an alert from your bank, stop and ask a trusted person — a friend, family member or coworker — to help you.

Reporting bank impersonation scams

If you experience a bank impersonation attempt, **notify your financial institution of the occurrence.** Include a screenshot of the text. If you lose money to this scam, contact your bank immediately — they may be able to halt the transaction.

File a police report. The documentation may be of value if there is some means of recouping your loss; for example, some home insurance providers offer fraud loss protection.

File reports with the federal government. The Federal Trade Commission (FTC) and the Federal Bureau of Investigation's Internet Crime Complaint Center use fraud reports to target their investigations; the more information they have, the better they can identify patterns, link cases and ultimately catch the criminals. Contact the FTC at reportfraud.ftc.gov and the FBI at IC3.gov.

Patrick J. Kiger is a contributing writer for AARP. He has written for a wide variety of publications, including the Los Angeles Times Magazine, GQ and Mother Jones, as well as the websites of the Discovery Channel and National Geographic.

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

So you think you may have been scammed?

Recognize the Signs and TAKE ACTION!

- Remember: if it sounds too good to be true, it probably is.
- Be direct. Don't be afraid to hang up the phone or shut the door on unwanted solicitations. Everyone, regardless of age, sex, education level, financial situation or where they live, is a potential victim. Seniors may be targeted more because they are perceived by scam artists to have more free time or may be more trusting.
- Never pay money up front to collect a prize.
- Be aware that wiring money is just like sending cash. Same with buying gift cards and providing them with the numbers off the back of the card. Once you send it, or provide the numbers, code or PIN - it is gone for good.
- Review financial statements regularly.
- Don't carry your social security card, birth certificate or passport in your purse or wallet, except when absolutely necessary.
- Ask a neighbor, family member, friend, banker, or trusted advisor if you have doubts about an offer or business BEFORE you agree to anything.
- Call law enforcement immediately if you think you have been victimized. Never accept the help of someone who calls you and offers to help recover the losses in a scam "for a small fee." Odds are it is the same scam artist coming back for more.
- Order a credit report once a year from each of the three major credit bureaus through www.annualcreditreport.com.
- Scammers may also target seniors for identity theft. To help ward off identity theft, be sure to protect your personal information by shredding the following:
    - **Receipts,**
    - **Credit cards and other offers of credit,**
    - **Credit card statements,**
    - **Mailing labels from magazines,**
    - **Copies of credit applications,**
    - **Insurance forms,**
    - **Bank checks and statements and expired charge cards, and**
    - **Any other item that might have account numbers, physicians' statements, customer numbers or membership numbers.**