OCTOBER 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

Stay away from scams this Medicare Open Enrollment Period

Gema de las Heras
Consumer Education Specialist

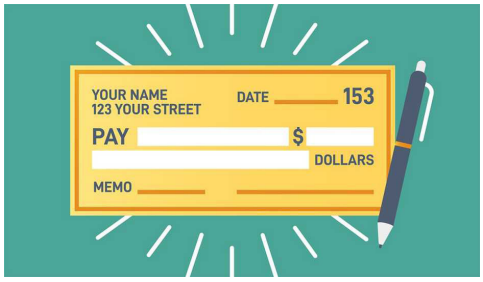
If you or one of your loved ones are on Medicare, you're probably aware that open enrollment ends on December 7. And you're probably reviewing and comparing different options to select a plan that's right for you. But as you shop around, know that scammers might take advantage of this period to impersonate Medicare agents.

Scammers may sound professional, say they're from Medicare, and have your personal details. But in reality, they're trying to steal your money, Medicare information, or your identity. Here's how to spot potential scams and what to do:

- Don't trust the name displayed on your phone. Scammers can fake a caller ID.
- Hang up if anyone calls and asks for your Medicare, Social Security, or bank or credit card information. Legitimate Medicare employees have your Medicare number on file.
- Don't be rushed into making a decision. You have until December 7 to enroll, and Medicare doesn't offer extra benefits for signing up early.
- Ignore threats to take away your benefits. If you qualify, your benefits can't be taken away for not signing up for a plan.
- Don't talk to anyone that suggests their plan is preferred by Medicare. The truth is that Medicare doesn't endorse a specific plan.
- Get help to deal with Medicare fraud and abuse at smpresource.org.
- Visit the Eldercare Locator or call toll-free 1-800-677-1116 to find local resources that can give you more information about the different Medicare plans available.

To report someone pretending to be affiliated with Medicare and other Medicare scams, call **1-800-MEDICARE (800-633-4227) and tell the FTC at ReportFraud.ftc.gov.**

Should You Stop Using Paper Checks?



Other forms of payment may be safer as mail theft and check-washing cases surge

By Christina Ianzito, AARP

Last month, two men were arrested in Fayetteville, Georgia, after authorities reportedly found 211 pieces of stolen mail in their possession, including 151 personal checks worth almost $50,000. They'd swiped the stash from a large blue mailbox in front of the Fayetteville post office, according to the Fayette County Sheriff's Office.

The good news is that the bad guys were caught. The bad news is that this kind of crime is rampant — so much so, it may be time to think twice before using paper checks and opt for alternative ways to send money.

The thefts, and subsequent check fraud, have become a huge problem: Last year, financial institutions received more than 680,000 suspicious activity reports (SARs) related to check fraud, nearly double the previous year's 350,000 SARs, according to the Federal Reserve. And that's while the number of paper checks in circulation has been dropping dramatically. Almost 3.4 billion checks were processed in 2022, down by nearly half, from 6.4 billion 10 years earlier.

"Checks have reached a point where they're almost more of a problem than a solution," says Frank McKenna, chief fraud specialist for the fraud detection company Point Predictive. "I think limiting [the use of paper checks] as much as you can, and using alternatives right now, is a good idea."

Mail theft on the rise

The growing check fraud problem is fueled by a surge in mail theft — from mailboxes and trucks — as well as robberies of carriers. In all of 2022, 412 U.S. Postal Service letter carriers were robbed on the job; in the first half of 2023, there were already 305 incidents, according to the United States Postal Inspection Service (USPIS). And after receiving 38,500 reports of mail theft last year, the service has seen 25,000 from just January to mid-May of 2023.

The thieves who steal from mail collection boxes (including personal mailboxes) want the checks, which they alter or "wash" to direct the money — often increasing the original dollar amount — to themselves or someone in their criminal network. Many stolen checks are put up for sale on the dark web for other criminals to purchase.

Those who target mail carriers seek what are known as arrow keys, extremely valuable among criminals because they're designed to open multiple mailboxes within a certain area.

In response, the USPS and USPIS say they are installing more-secure mail collection boxes that prevent thieves from fishing for mail through the slot, as well as electronic locks to replace arrow-key locks in high-risk areas.

"We are hardening targets — both physical and digital — to make them less desirable to thieves, and working with our law enforcement partners to bring perpetrators to justice," Chief Postal Inspector Gary Barksdale said in a May press statement.

Though there have been reports of USPS employees stealing mail, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) said in a February alert about check fraud to financial institutions that mail thefts are increasingly committed by non-USPS workers, "ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules."

Paper checks and identity theft

There are other reasons to be concerned about using checks: Each one is loaded with your personal information. Most of us have our names, addresses and phone numbers printed on our checks, not to mention our bank account and routing numbers. McKenna notes that

Continued on next page

identity thieves can use that data to find out even more, such as your Social Security number and email address, using online tools popular with criminals.

"We have to think about who we're handing a check to even physically because of the way that that information can be used digitally," says Mary Ann Miller, fraud and cybercrime executive adviser and vice president of client experience at the consumer identity company Prove. Miller notes that the bad actors can get enough information to open another bank account in your name and, using that routing and account number, "conduct ACH transactions out of your bank account." (ACH transactions are electronic fund transfers between banks.)

"That paper check is riskier than we think," Miller says.

Alternatives to paper checks

Before writing a check, see if there's another way to pay, says Roxann Cooke, managing director for consumer banking at Chase, who points to alternatives that include cash transfer apps such as Zelle, your bank's online bill payment feature, and particularly credit cards, which have substantial consumer protections.

When using apps, it's important to confirm the payment details before hitting that send button. It can be hard to get your money back if you make an error, which is why some experts, such as Cooke, suggest only using this method when transferring money between friends and family or others you trust. Even then, she adds, "triple check the user name and phone number" before sending the money.

Miller suggests using a credit card for online bill payment when you can, because "it's easier and more convenient to dispute a transaction with your credit card" than it is with other payment methods.

How to lower your risk of fraud when you do use checks

When making out a check, write out the amount — "Two hundred and fifty dollars and sixty-one cents," for example — so the words fill out the line. This makes it more difficult for someone to alter it without washing off the ink. Also make sure the numeric amount fills the box on the far-right side of the check.

Use permanent ink to prevent the check from being washed.

"Never, never write checks out to cash," Cooke says, "unless you intend for it to be used by anyone who comes in possession of that check."

Sign your checks the same way every time so that your signature is more easily recognized by the bank when signatures are compared, Cooke suggests.

Keep your checks in a secure, private place in your home (never keep blank checks in your wallet).

Deposit mail in collection boxes as close to the indicated pickup time as possible — or, better yet, take it inside the post office for mailing.

Get online regularly to scan your transactions for suspicious activity. "If you get paper statements, you may not know [there's a problem] for 30 days," McKenna says. And make sure the amount that the check was cashed for matches the amount you wrote on it. Some banks' apps allow you to pull up images of the cashed check.

Sign up for transaction alerts with your bank. Unfortunately, however, you need to be aware of bank impersonation scams, in which bad actors pretend to warn you about fraud to get your personal information or money.

Report suspicious activity as soon as possible.

What to do if you think your check has been stolen

1. **Notify your bank**. "The faster the better," Cooke says.
2. **Report suspected mail losses to the USPIS**, which uses such reports to identify problem areas and where to focus crime investigations, at uspis.gov/report or by calling 877-876-2455.
3. **Report the theft to local law enforcement**, so you'll have a police report documenting the crime.

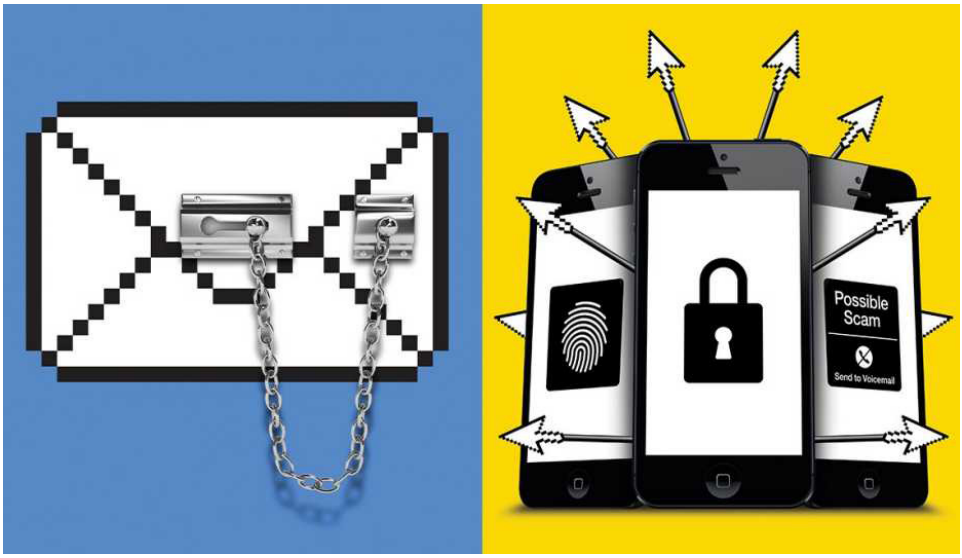
---

13 Ways to Protect Yourself From Fraud

Learn how to lower your risk and keep criminals at bay

By Amy Nofziger and Mark Fetterhoff, AARP

Scams are rampant these days, with criminals stealing a reported $8.8 billion from Americans last year, according to the Federal Trade Commission. But there are ways to protect yourself, including staying up on the latest schemes and following the advice listed below.



1. Stop at the mailbox

Informed Delivery is a free service from the U.S. Postal Service. The agency emails photos of letter-size mail expected to be delivered to you that day or shortly after. This is a great way to be sure that nothing is stolen from your mailbox by ID thieves. Sign up at InformedDelivery.usps.com.

Pick up mail as quickly as possible after it's delivered, and always take your outgoing mail directly to the post office. A hot fraud now is scammers stealing checks from mailboxes, erasing the ink and using them to steal from bank accounts.

2. Halt scammers at your front door

Consider installing a video camera; they are increasingly less expensive, and they're easy to install. If you don't recognize a visitor, don't answer.

If you find yourself being pressured to buy or donate, have a refusal script ready (consider taping it near the door) that says, "I do not do business at my door. Please leave me something to review. If I'm interested, I'll call you."

Be wary of people posing as utility workers who show up unannounced. Don't allow anyone into your house without an appointment.

3. Prevent garbage theft

Shred any papers that contain private information (financial statements, bills, shipping receipts) before putting them out for pickup to avoid identity theft. Don't want to invest in a good cross-cut shredder? Many communities have shredding events or permanent drop-off sites. Get in the habit of dropping off your accumulated documents once every few months.

4. Watch for credit card skimming

Card skimming, in which the criminal affixes a credit card reader on top of a legitimate card reader at a store or gas station, is estimated to cause up to $1 billion in losses annually. When you are paying at a gas station or other point-of-sale location, inspect the device for loose/broken/scratched machinery to make sure someone hasn't tampered with it. If you are unsure, notify the cashier and pay using an alternative method.

5. Monitor your credit report

Routinely check yours (many credit card companies provide it for free; if not, go to AnnualCreditReport.com or call 1-877-322-8228). Watch for unusual activity; if you see any, report it immediately to the appropriate financial institution.

Then freeze your credit report. This prevents scammers from opening new credit cards or making big purchases in your name. You can "unfreeze" it as needed for legitimate transactions. Visit IdentityTheft.gov for more information.

6. Safeguard your wallet

Continued on next page

Remove cards and information you don't need to carry (such as your Social Security or Medicare card). Make copies of the remaining cards (front and back) and store in a safe place.

Audit your wallet and purse frequently. Take out any unnecessary items that collect and could compromise your personal information if lost or that would be a hassle to replace.

7. Protect your financial accounts

Create online accounts with each of your financial institutions. Come up with a unique password for each.

Then get in the habit of reviewing the transaction lists on a weekly or biweekly basis. Be sure you can account for every listed transaction. Spot something odd or incorrect? Immediately report it.

8. Safeguard your smartphone

If you have a newer model, turn on biometric identification (fingerprint or facial recognition); this will help prevent a thief from logging in to your phone.

Send calls from unknown numbers to voicemail (you can enable this in the phone's settings). Make sure your voicemail is set up and not full, so you can receive legitimate messages.

Scammers are sending far more bogus texts, often posing as companies you routinely deal with. Never respond to an unsolicited business text; if you think it might be valid, call the organization or go online.

9. Secure your computer

Turn on two-factor authentication for all secure websites you frequent, such as financial institutions or utility companies (find out how via each site's online security center). Then only someone logged in to your phone can receive the code to access those accounts.

Consider subscribing to an antivirus software service. Some security experts say browsers and device manufacturers have more built-in malware protection than years ago, such as Microsoft Defender, which comes installed on Windows 10 and 11 machines. Some paid subscriptions also include ad tracker blocking, cloud backups of your machines and identity theft monitoring.

10. Protect your email accounts

Actively designate unsolicited and unwanted email that shows up in your inbox as spam, so future emails from that site get blocked.

Do not open file attachments in emails from businesses or people you don't trust completely. Malware is often planted via email attachments.

11. Set limits on social media

Set your profile so that only your friends can see your Facebook page. To do that, click the downward arrow button in the upper-right corner of your Facebook page, then click on Settings & Privacy and Privacy Checkup. This easy-to-use wizard will guide you through the settings. And never accept friend requests from people you don't know or respond to random messages from strangers. But also note that imposter scams, where someone pretends to be your friend, are rampant on social media.

12. Verify online stores

To avoid shopping scams, when typing in a URL, double- and triple-check the spelling to ensure you are on the correct page. Scammers often create a URL with one letter off from the authentic one in hopes you won't catch it.

Remove your credit card number and information from restaurant delivery and retail store sites. Pay using an e-payment service that keeps credit card info on a highly secure site.

13. Change the way you think

Learn how to not engage. You are under no obligation in these modern times to respond to calls, emails or texts from strangers — especially given that so many of them are fraudulent.

Learn to say no. Sometimes a caller will get through. Get tough: Say, "I do not do business over the phone. Goodbye." Then hang up without remorse.

Trust your instincts. If something doesn't sound right, run it by someone you trust and take extra time to think about it.

Medicare Annual Open Enrollment: Oct 15-Dec7

Volunteers Assisting Seniors will be helping seniors during Medicare Open Enrollment. During Open Enrollment, you can (and should) review your part D prescription drug plan to make sure it will still meet your needs and budget for the coming year, and change plans if necessary. This is also the time that you can review and change Medicare Advantage Plans.

Book your Open Enrollment appointment, starting September 5,
by calling VAS at 402-444-6617 .
Appointments fill up fast, so please call before October 15 for best availability.
Appointments available from October 15-December 7

VOLUNTEERS ASSISTING SENIORS

Volunteers Assisting Seniors is the Eastern Nebraska SHIP office, our purpose is to provide free, unbiased information to help seniors make informed decisions about their Medicare benefits.
www.vas-nebraska.org

NEBRASKA SHIP
Local help for Nebraskans with Medicare