Beware of New Medicare and Social Security Scams

From the Office of Minnesota Attorney General Keith Ellison

Minnesota senior citizens report being targeted by a new scam: fraudulent operators who pretend to be calling about Medicare, Social Security, or supplemental insurance, but whose actual purpose is to trick seniors into disclosing their private financial information. Disclosure of such information can lead to identity theft or unauthorized withdrawals from a person's bank account. Consider the following to help prevent this scam from happening to you, or someone you care about.

How the Scam Works

Medicare and Social Security beneficiaries across the country report receiving calls from scam operators (frequently with foreign accents), who claim to represent Medicare, Social Security, or an insurance company. These callers claim that new Medicare, Social Security, or supplemental insurance benefits cards are being issued or that the beneficiary's file must be updated. The scam artist asks the citizen to verify or provide their personal banking information, which is then used to commit theft.

The caller may be extremely aggressive, calling over and over, and at all times of the day, in an attempt to wear down the potential victim. These criminals will say anything to try to gain a person's trust. In some cases, the criminals may have already obtained some limited personal information about the citizen, such as his or her name, address, or even Social Security number, which the criminal then uses to try to make the call seem legitimate. In other cases, the callers may claim that they can improve the benefits. Do not believe these claims, and do not carry on a conversation with the caller. Instead, if you receive a call asking you to disclose your bank account or other financial information, **hang up immediately**. These are criminals, and by speaking with the callers, even to ask them to stop calling, they may be encouraged to continue calling your telephone number.

If you are a Medicare or Social Security beneficiary, the Center for Medicare and Medicaid Services and the Social Security Administration will not call you to ask you to disclose financial information in order to get a new card. If you receive such a call, you should report it to these two agencies as follows:

Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244
(877) 267-2323
www.cms.gov

Social Security Administration
Office of Public Inquiries
1100 West High Rise
6401 Security Boulevard
Baltimore, MD 21235
(800) 772-1213
www.ssa.gov

The operators of this scam are engaged in criminal activity. Citizens who receive such calls are also encouraged to report them to the FBI as follows:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000
www.fbi.gov

Tips

These three tips should help you avoid falling victim to this scam:

1. Remember, the Center for Medicare and Medicaid Services and the Social Security Administration will not call you to update your information or give you a new card.

2. If someone who calls you asks for your personal information, do not provide it.

3. If calls persist, you may wish to speak to your phone company about calling features that would enable you to be selective in the calls that you accept or receive.

If you have already disclosed personal financial information to an unknown party, you may be at risk of identity theft. There are certain steps that you can take to further protect yourself including:

1. Call the three major credit bureaus and place a one-call fraud alert on your credit report:

- Equifax: Call (800) 525-6285, and write P.O. Box 105069, Atlanta, GA 30348-5069.
- Experian: Call (888) 397-3742, and write P.O. Box 9532, Allen, TX 75013.
- TransUnion: Call (800) 680-7289, and write Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790.

2. Consider placing a security freeze on your credit reports.

Under state law, Minnesota consumers can place a security freeze on their credit reports. In most instances, the freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. To place a security freeze on your credit report, you may send a written request to each of the three nationwide consumer reporting agencies by mail, or call or go online to request a freeze as follows:

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com/freeze

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 685-1111
www.freeze.equifax.com

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com/securityfreeze

3. Order a free copy of your credit report and look for unauthorized activity.

Many consumers first find out that they are victims of identity theft by discovering inaccuracies on their credit report. The Federal Fair Credit Reporting Act (FCRA) allows consumers to obtain a free copy of their credit report each year from the three major credit bureaus as follows:

a. Log on to *www.AnnualCreditReport.com*;

b. Call: (877) 322-8228; or

c. Write: Annual Credit Report Request Service, P.O. Box 105283, Atlanta GA 30348-5283

4. Monitor your financial accounts for suspicious activity.

Look carefully for unexplained activity on your bank and other financial statements. If you detect unexplained activity, you may want to contact the fraud department of your financial institution.

For additional information, contact the Office of Minnesota Attorney General Keith Ellison as follows:

Office of Minnesota Attorney General
Keith Ellison
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
www.ag.state.mn.us