

## **IDENTITY THEFT INFORMATION**

*From the Office of Blue Earth County Attorney Patrick R. McDermott*

### **IF YOUR KEYS WERE TAKEN:**

Change or re-key whichever locks need to be changed for protection.

### **IF YOURS CHECKS OR CREDIT CARDS WERE TAKEN:**

**Notify your bank if you have not already done so**, and then call the three credit reporting bureaus to report the loss and ask them to put a **FRAUD ALERT** on your account so **NO NEW CREDIT** will be issued without contacting you.

**Experian-** (888) 397-3742 [www.experian.com](http://www.experian.com)

**Transunion-** (800) 680-7289 [www.transunion.com](http://www.transunion.com)

**Equifax-** (800) 525-6285 [www.equifax.com](http://www.equifax.com)

### **IF YOUR SOCIAL SECURITY CARD WAS TAKEN:**

Call the Social Security Administration **FRAUD HOTLINE** to notify them of the loss and get information on how to get a duplicate card

**S.S.A. FRAUD HOTLINE-** (800) 269-0271 [www.ssa.gov](http://www.ssa.gov)

### **IF YOUR DRIVER'S LICENSE WAS TAKEN:**

Apply for a new license and "flag" your license as stolen (Identity Theft) at the DMV.

**MN DEPTMENT OF MOTOR VEHICLES-** (651) 296-2025

<https://dps.mn.gov/divisions/dvs>

### **IF NEW CHECKS OR CARDS HAVE BEEN MAILED TO A DIFFERENT ADDRESS:**

Call the U.S. Postal Inspectors about your mail being falsely forwarded:

**United States Postal Service/Inspection Service-** (877) 876-2455

**Local Postal Inspector-** (651) 293-3200

<https://postalinspectors.uspis.gov/>

### **IF YOUR STOLEN CHECKS OR CARDS HAVE BEEN USED:**

Contact the banks and/or business that accepted your checks and cards to notify them of the fraud and offer to sign any affidavits of forgery as needed. Encourage the banks and businesses to pursue charges against any suspects identified

### **IF SOMEONE HAS STOLEN YOUR IDENTITY TO GET NEW CREDIT:**

Call the police and/or sheriff's office and make an identity theft report. In Minnesota, identity theft becomes a crime only when a victim (person or business) suffer a monetary loss. Also, call the Federal Trade Commission Identity Theft Hotline to notify them and get advice on how to proceed

**FTC ID THEFT HOTLINE-** (877) 438-4338 [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

FTC FRAUD (Other than ID Theft)- (877) 382-4357

**OTHER INTERNET RESOURCES FOR ADVICE AND INFORMATION:**

<b>Federal Bureau of Investigations</b>	<a href="http://www.fbi.gov">www.fbi.gov</a>
<b>Privacy Rights Clearinghouse</b>	<a href="http://www.privacyrights.org">www.privacyrights.org</a>
<b>PRC- Identity Theft Resources</b>	<a href="http://www.privacyrights.org/identity.htm">www.privacyrights.org/identity.htm</a>
<b>Internet Fraud Complaint Center</b>	<a href="http://www.ic3.gov/">www.ic3.gov/</a>
<b>NWCCC Website</b>	<a href="http://www.nw3c.org">www.nw3c.org</a>
<b>Cyber Crime</b>	<a href="https://www.cybercrime.gov">https://www.cybercrime.gov</a>

**OTHER PHONE RESOURCES FOR ADVICE AND INFORMATION:**

Federal Government Information Center- (800) 688-9889

**WHAT YOU CAN DO TO PROTECT YOURSELF AND YOUR FAMILY FROM BEING VICTIMIZED:**

- Do not leave your wallet, purse, computers, or valuables in a locked or unlocked vehicle at any time
- Do not leave your wallet or purse unattended while at work, school, church, a social gathering, or at a health club
- When you are away from your office and house, lock the doors. Lock your house and garage doors at night. Keep your overhead garage door closed when you are not using the garage
- Don't put your driver's license number on your checks. This makes it easy to get a false ID made
- Keep all credit card receipts safe. Many criminals use numbers off receipts to defraud
- Shred credit card offers you receive in the mail. Thieves steal mail and trash to get these
- **Never** give your credit card number out to someone calling you. Make charges only when you call and remember, card fraud investigators will never call and ask you for your number and expiration date

**THE GOOD NEWS:**

**You are NOT responsible for monetary losses.** The banks and credit card companies may refund your money losses (if any), although it may take some time while they are investigating on the case. Some can charge up to \$50 per account, but most do not.

# Social Engineering Red Flags

## FROM

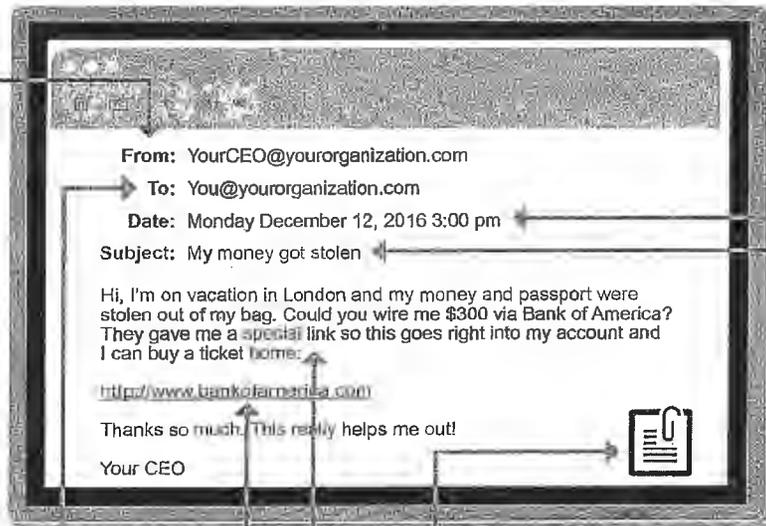
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofarnerica.com](http://www.bankofarnerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

## ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

## Do Not Call Lists

- ▶ Place your name on the **DO NOT CALL REGISTRY**
  - National 1-888-382-1222
  - [www.donotcall.gov](http://www.donotcall.gov)
  - *It usually takes 31 days to activate the process once the initial call is made.*

## Consumer Credit Reporting Industry

- ▶ Credit reporting industry opt-out service (Stops some credit card and insurance offers)
  - 1-888-576-8688
  - [www.optoutprescreen.com](http://www.optoutprescreen.com)

## Direct Marketing Association

- ▶ **Consumer Opt-Out Service**
  - [www.dmachoice.org](http://www.dmachoice.org)
  - Legitimate mail-order businesses will take your name off their mailing lists
  - Opt-out service is free if you register online

## Reporting Identity Theft

- ▶ Call the Inspector General's hotline at 1-800-447-8477
- ▶ Place a "fraud alert" on your credit by contacting the three major credit bureaus. Also consider requesting a "credit freeze". Request a copy of your credit report from one of the credit bureaus and review the report carefully.
  - Equifax: 1-800-525-7289
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
- ▶ Close compromised accounts immediately:
  - Close any accounts that have been tampered with or established fraudulently.
  - Call the security and fraud departments of each company.
  - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- ▶ File a police report with your local police department:
  - Get a copy of the police report for your records.
- ▶ Report the theft to the Federal Trade Commission:
  - Online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or phone at 1-877-ID-Theft (438-4338)

If you have questions about this information or need help in reporting identity theft contact:

**Senior LinkAge Line® at 1-800-333-2433**



# Beware of New Medicare and Social Security Scams

From the Office of Minnesota Attorney General Lori Swanson

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](http://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](http://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](http://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](http://www.experian.com/freeze)

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
(800) 685-1111  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

**TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19016  
(800) 680-7289  
[www.transunion.com/securityfreeze](http://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](http://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 Lori Swanson as follows:

**Office of Minnesota Attorney General**

**Lori Swanson**

445 Minnesota Street, Suite 1400  
St. Paul, MN 55101  
(651) 296-3353 (Twin Cities Calling Area)  
(800) 657-3787 (Outside the Twin Cities)  
TTY: (651) 297-7206 or (800) 366-4812  
[www.ag.state.mn.us](http://www.ag.state.mn.us)

# 5

## Ways to Spot a Lottery Scam



According to the FBI, in 2014 consumers lost more than \$8 million to solicitation scams. These scams, commonly referred to as “advance fee,” “lottery” or “sweepstake” scam, often begin with fraudsters telling the victim they’ve won a lottery or sweepstake raffle. The consumer is issued a check worth more than the amount owed and instructed to pay taxes and fees before receiving a lump sum payment. Unfortunately, the check—in addition to the raffle—is bogus.

- 1. Don’t be fooled by the appearance of the check.** Scam artists are using sophisticated technology to create legitimate looking counterfeit checks. Some are counterfeit money orders, some are phony cashier’s checks and others look like they are from legitimate business accounts. The company name may be real, but someone has forged the checks without their knowledge.
- 2. Never “pay to play.”** There is no legitimate reason for someone who is giving you money to ask you to wire money back or send you more than the exact amount—that’s a red flag that it’s a scam. If a stranger wants to pay you for something, insist on a cashier’s check for the exact amount, preferably from a local bank or one with a local branch.
- 3. Verify the requestor before you wire or issue a check.** It is important to know who you are sending money to before you send it. Just because someone contacted you doesn’t mean they are a trusted source.
- 4. Ensure a check has “cleared” to be most safe.** Under federal law, banks must make deposited funds available quickly, but just because you can withdraw the money doesn’t mean the check is good, even if it’s a cashier’s check or money order. Be sure to ask if the check has cleared, not merely if the funds are available before you decide to spend the money.
- 5. Report any suspected fraud to your bank immediately.** Bank staff are experts in spotting fraudulent checks. If you think someone is trying to pull a fake check scam, don’t deposit it—report it. Contact your local bank or the National Consumers League’s Fraud Center, [fraud.org](http://fraud.org).

For more information, visit [aba.com/Seniors](http://aba.com/Seniors)



**SAFE BANKING  
FOR SENIORS**

ABA FOUNDATION

# Don't Fall Victim to the Grandparent Scam



According to the Federal Trade Commission, between 2012 and 2014, consumers reported more than \$42 million in losses from scams involving the impersonation of family members and friends. This scam, commonly known as the “grandparent scam,” is a form of financial abuse that deliberately targets older Americans.

To commit this crime, fraudsters call claiming to be a family member in serious trouble and in need of money immediately. The scammer might say he's stranded or has been mugged, and call in the middle of the night to add to the urgency and confusion. Once the money is wired, the victim later finds out that it wasn't their grandchild they were helping, it was a criminal.

- **Confirm the caller.** Fraudsters are using social networking sites to gain the personal information of friends and relatives to carry out their crimes. Verify the caller by calling them back on a known number or consult a trusted family member before acting on any request.
- **Don't be afraid to ask questions.** Fraudsters want to execute their crimes quickly. The more questions you ask the more inclined they will be to ditch the scam if they suspect you're on to them.
- **Never give personal information to anyone over the phone** unless you initiated the call and the other party is trusted.
- **Never rush into a financial decision and trust your instincts.** Don't be fooled—if something doesn't feel right, it may not be right. Feel free to say no and get more information before you send money to someone.

For more information, visit [aba.com/Seniors](http://aba.com/Seniors)



**SAFE BANKING  
FOR SENIORS**

ABA FOUNDATION

# What is a Scam?



A scam is a trick a con artist plays on an unsuspecting victim to extort money. If the scam succeeds, the victim's money is gone, and the scammer will move on to the next victim.

## **A scammer is the ultimate salesperson with a tempting offer or a skilled liar with a plausible story**

- Easily pinpoints a victim's vulnerabilities and appeals to emotions: sympathy, fear, loneliness
- Quickly gains trust
- Insist on secrecy
- Shows no mercy, e.g., doesn't take "no" for an answer

## **Know the Red Flags of a Scam**

- Immediate action required
- Insistence on secrecy
- Money needed up front
- Hard-to-track payment methods

## **Build Your Scam Defenses**

- Do not be rushed into any financial decision
- Assume that insistence on secrecy is a ploy to deceive you
- Be suspicious of any situation that requires you to send money up front
- Confirm all stories, offers or charities independently
- Be very cautious about clicking on email links

## **Block Those Scammers**

- Register with National Do Not Call Registry at [www.donotcall.gov](http://www.donotcall.gov) to limit legitimate telemarketing phone calls, making phone scams easier to detect
- Register with [www.DMAchoice.org](http://www.DMAchoice.org) to limit legitimate advertising mail, making mail scams easier to detect
- Limit personal information on social media and choose the strictest privacy settings on social media accounts
- Use antivirus software on your computer

## **What to Do If You Are Scammed**

- Don't be embarrassed or afraid
- Tell someone you trust
- Report the scam to your bank immediately to limit losses
- Contact your local police and federal agencies, like the Federal Trade Commission

For more information, visit [aba.com/Seniors](http://aba.com/Seniors)



**SAFE BANKING  
FOR SENIORS**

ABA FOUNDATION