

- Use Direct Deposit for your checks.
- Do not leave money or valuables in plain view.
- Sign your own checks. Do not sign "blank checks" where another person can fill in the amount. (If you need someone to help you write out checks before you sign, ask a third party to review the check and take it to the bank.)
- If someone is helping you manage your finances, get a trusted third person to review your bank statement.
- Do not sign any document without reading it carefully.
- Do not sign any agreement until it has been reviewed by a trusted friend or other advisor, or an attorney. If possible, have two advisers look at the agreement.
- Do not lend money in return for a general promissory note.
- Do not sign over money or property to anyone in return for care, even a family member or friend, without having the agreement reviewed by an attorney. The agreement must be written. Give someone else a copy.
- Do not allow anyone, even a relative, to put their name on your account without your express consent. Your bank can set up a separate account in both names with automatic transfer of limited funds.



- Do not allow anyone else to use your debit card.
- Cancel your debit card if you do not use it.
- Do not give anyone your Personal Identification Number (PIN).
- Do not use an easily detectable PIN (a birthdate or social security number).
- Check bank statements carefully for unauthorized withdrawals.
- Be cautious using an ATM at night.
- Do not use a badly lit ATM. This is a danger sign because they are designed to be brightly lit for your safety. Report the situation to your bank.
- Be aware of people around you as you use the ATM don't let them watch you enter your PIN number.
- Put your money safely away before exiting the ATM area.
- Look around as you exit the ATM area. Do not leave if you do not feel safe.
- Do not open the door of the ATM area to anyone without a card.



- Establish relationships with personnel at your bank.
- Cultivate friends of all ages so you maintain a strong support network.
- Become familiar with resources in the community designed to help older people and their families.
- Execute a Power of Attorney that will grant financial decision making power to a trusted friend, relative, or attorney. Know the person to whom you are granting this authority. A Power of Attorney can be as limited or as broadly defined as you wish, and can be revoked at any time. The specific "powers" given to this person should be detailed in writing. Give your bank a copy.
- Consider a Durable Power of Attorney that will remain in effect even if you become incapacitated.
- Consider a Trust a legal arrangement where a person or financial institution manages assets for you.
- Put all financial instructions in writing. Be specific.
- Keep accurate and complete financial records of all transactions.
- Gather all important documents together (wills, insurance policies, and bank account information). Tell someone you trust where these documents are kept.



- If a deal seems too good to be true it probably is!
- Never let yourself be rushed into a "deal." This usually means the person is up to no good. Ask for details in writing and time to review them with a trusted friend, advisor, or attorney.
- Never give out credit card numbers over the phone unless you placed the call.
- Never give out your Social Security number or bank account number over the phone.
- Give to charities you know. Check out unfamiliar charities.
- Get several estimates before you have any home renovations or work done.
- As a rule, do not have work done on your home by companies or individuals contacting you and offering deals.
- Do not pay for work in advance.
- Check references, telephone numbers and home addresses.
- Contractors must be licensed by law. Check license numbers.

If you have any questions or concerns about a business or activity contact:

#### **Office of Minnesota Attorney**

1400 Bremer Tower • 445 Minnesota Street St. Paul, MN 55101 (651) 296-3353 1-800-657-3787 TTY: (651) 297-7206 TTY: 1-800-366-4812



The most empowering tool citizens have to protect themselves against identity theft and fraud is their credit report. Consumers are now able to receive this report on an annual basis for free.

The nationwide consumer reporting agencies have a centralized source from which consumers may order and receive a **free** annual credit report. Minnesotans may request a copy of their credit report through:

- a. the Internet: annualcreditreport.com
- b. a toll-free number: 877-322-8228
- c. by mail:

Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281

A standardized form for requesting a free credit report may be found at: <u>https://www.annualcreditreport.com/index.action</u>

# Credit Reporting Agencies:

#### Equifax

PO Box 740241 Atlanta, GA 30374 Telephone: (800) 685-1111 www.equifax.com

# Experian

PO Box 2002 Allen, TX 75013 Telephone: (888) 397-3742 www.experian.com

# TransUnion

Consumer Disclosure Center PO Box 1000 Chester, PA 19022 Telephone (800) 888-421 www.transunion.com

Only the Central Source, Equifax, Experian, and TransUnion have been authorized by law and the government (see FTC.gov) to provide free credit reports. Personal information may not be kept secure and used for proper purposes if you provide information to persons, addresses, numbers, etc. not authorized by the entities listed above.



According to the National Council on Aging, financial scams targeting seniors have become so prevalent that they're now considered "the crime of the 21st century." Financial scams also often go unreported or can be difficult to prosecute, so they're considered a "low-risk" crime. Over 90% of all reported elder abuse is committed by an older person's own family members, most often their adult children, followed by grandchildren, nieces and nephews, and others. The National Council on Aging's top ten scams targeting seniors are:

# 1. Medicare/health insurance fraud

In these types of scams, perpetrators may pose as a Medicare representative to get older people to give them their personal information, or they will provide bogus services for elderly people at makeshift mobile clinics, then use the personal information they provide to bill Medicare and pocket the money.

# 2. Counterfeit prescription drugs

Most commonly, counterfeit drug scams operate on the Internet, where seniors increasingly go to find better prices on specialized medications. The danger is that besides paying money for something that will not help a person's medical condition, victims may purchase unsafe substances that can inflict even more harm.

### 3. Funeral & cemetery scams

The FBI warns about two types of funeral and cemetery fraud perpetrated on seniors. In one approach, scammers read obituaries and call or attend the funeral service of a complete stranger to take advantage of the grieving widow or widower. Claiming the deceased had an outstanding debt with them, scammers will try to extort money from relatives to settle the fake debts. Another tactic of disreputable funeral homes is to capitalize on family members' unfamiliarity with the considerable cost of funeral services to add unnecessary charges to the bill.

# 4. Fraudulent anti-aging products

Whether it's fake Botox or completely bogus homeopathic remedies that do absolutely nothing, there is money in the anti-aging business. Botox scams are particularly unsettling, as renegade labs creating versions of the real thing may still be working with the root ingredient, botulism neurotoxin, which is one of the most toxic substances known to science. A bad batch can have health consequences far beyond wrinkles or drooping neck muscles.

#### 5. Telemarketing

Perhaps the most common scheme is when scammers use fake telemarketing calls to prey on older people, who as a group make twice as many purchases over the phone than the national average. With no face-to-face interaction, and no paper trail, these scams are incredibly hard to trace. Also, once a successful deal has been made, the buyer's name is then shared with similar schemers looking for easy targets, sometimes defrauding the same person repeatedly.



Examples of telemarketing fraud include:

### The pigeon drop

The con artist tells the individual that he/she has found a large sum of money and is willing to split it if the person will make a "good faith" payment by withdrawing funds from his/her bank account. Often, a second con artist is involved, posing as a lawyer, banker, or some other trustworthy stranger.

### The fake accident ploy

The con artist gets the victim to wire or send money on the pretext that the person's child or another relative is in the hospital and needs the money.

### Charity scams

Money is solicited for fake charities. This often occurs after natural disasters.

### 6. Internet fraud

Pop-up browser windows simulating virus-scanning software will fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that will open up whatever information is on the user's computer to scammers. Another example includes email/phishing scams where a senior receives email messages that appear to be from a legitimate company or institution, asking them to "update" or "verify" their personal information or a senior receives emails that appear to be from the IRS about a tax refund.

#### 7. Investment schemes

Because many seniors find themselves planning for retirement and managing their savings once they finish working, a number of investment schemes have been targeted at seniors looking to safeguard their cash for their later years. From pyramid schemes like Bernie Madoff's (which counted a number of senior citizens among its victims) to fables of a Nigerian prince looking for a partner to claim inheritance money to complex financial products that many economists don't even understand, investment schemes have long been a successful way to take advantage of older people.

#### 8. Homeowner/reverse mortgage scams

Scammers like to take advantage of the fact that many people above a certain age own their homes, a valuable asset that increases the potential dollar value of a certain scam. A particularly elaborate property tax scam in San Diego saw fraudsters sending personalized letters to different properties apparently on behalf of the County Assessor's Office. The letter, made to look official but displaying only public information, would identify the property's assessed value and offer the homeowner, for a fee of course, to arrange for a reassessment of the property's value and therefore the tax burden associated with it.



With legitimate reverse mortgages increasing in frequency, scammers are taking advantage of this new popularity. As opposed to official refinancing schemes, however, unsecured reverse mortgages can lead property owners to lose their homes when the perpetrators offer money or a free house somewhere else in exchange for the title to the property.

## 9. Sweepstakes & lottery scams

Here, scammers inform their mark that they have won a lottery or sweepstakes of some kind and need to make some sort of payment to unlock the supposed prize. Often, seniors will be sent a check that they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected. During that time, the criminals will quickly collect money for supposed fees or taxes on the prize, which they pocket while the victim has the "prize money" removed from his or her account as soon as the check bounces.

### 10. The grandparent scam

Scammers will place a call to an older person and when the mark picks up, they will say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity. The fake grandchild will usually ask for money to solve some unexpected financial problem (overdue rent, payment for car repairs, etc.), to be paid via Western Union or MoneyGram, which don't always require identification to collect. At the same time, the scam artist will beg the grandparent "please don't tell my parents, they would kill me." While the sums from such a scam are likely to be in the hundreds, the very fact that no research is needed makes this a scam that can be perpetrated over and over at very little cost to the scammer.

# Resources

FBI Common Fraud Schemes: https://www.fbi.gov/scams-safety/fraud/seniors

Department of Human Services: Adult protection in Minnesota: Preventing maltreatment of vulnerable people over 18: <u>https://edocs.dhs.state.mn.us/lfserver/Public/DHS-6665-ENG</u> and Help Protect People Who are Frail or Vulnerable: <u>https://edocs.dhs.state.mn.us/lfserver/Public/DHS-2754-ENG</u>

http://www.fraud.org/learn/older-adult-fraud/they-can-t-hang-up

MN AG Seniors Guide to Fighting Fraud http://www.ag.state.mn.us/consumer/publications/seniorsguidefightfraud.asp

Senior fraud videos in multiple languages: <u>http://www.bbb.org/minnesota/news-events/news-releases/2015/area-agencies-partner-to-combat-senior-fraud/</u>



- 1. Never leave your purse or wallet in the car, even if it is hidden.
- 2. Do not load your purse or wallet down with credit cards.
- 3. Never carry your Social Security card or birth certificate in your purse or wallet.
- 4. Do not keep debit card personal identification numbers (PIN) or other passwords in your purse or wallet.
- 5. Avoid using easily discovered passwords or PIN number/codes, such as your birth date, phone number, or address.
- 6. Keep a list or photocopy of all of your credit accounts and bank accounts in a secure place, such as a safe, lock box or locked file cabinet.
- 7. Keep tax records, canceled checks, and paid bills in a secure place, or shred them before throwing them away.
- 8. Be very careful when ordering something over the Internet. Make sure the server is secure.
- 9. When you purchase items with a credit card, always take your credit card receipts with you. Never toss them in a wastebasket.
- 10. Shield your hand when entering your debit card password.
- 11. Be aware of who is around you when approaching an ATM.
- 12. Do not leave printed receipts behind at bank machines or gas pumps.
- 13. Do not say or press your credit card or bank account numbers over a wireless or cordless phone unless it is equipped with encryption technology.
- 14. You can also protect your identity by changing your passwords and PIN numbers regularly.
- 15. Consider purchasing an inexpensive paper shredder for your home.
- 16. Do not throw away receipts with credit card numbers clearly shown.

(Source: A Comprehensive Report On Identity Theft, ACFE Research Committee, December 2001)



- Nationally, half of the victims of financial exploitation are 80 or older.
- By 2020, there will be more Minnesotans older than 65 than children in public schools, and by 2035, Minnesota's population older than 65 will more than double, as will its population 85 and older.
- The number of seniors living alone is growing. Currently 1 in 3 of Minnesota seniors live alone, and 2 out of 3 women aged 85-90 live alone. These numbers will double by 2030.
- In Minnesota, there are an estimated 30,000 documented senior fraud cases each year, but most of these crimes go unreported only 1 in 44 seniors actually report that they are victims of a fraud scheme, and victims often face confusion on where to turn for help.
- In 2012, people 60 years and older made up 26% of all fraud complaints tracked by the Federal Trade Commission, the highest of any age group. In 2008, the level was just 10%, the lowest of any adult age group.
- Four years ago, in Hennepin County, financial exploitation cases accounted for 15% of reports to adult protection. Now they account for more than 20%.