Identity Theft

Identity theft occurs when thieves steal your personal information (e.g., your Social Security number (SSN), birth date, credit card numbers, personal identification numbers (PINs), or passwords). With sufficient information, another person can use your identity to commit fraud or other crimes.

How to Avoid Identity Theft

- **Protect your Social Security number, credit card and debit card numbers, PINs, passwords, and other personal information.**
  Never provide this information in response to an unwanted telephone call, fax, letter, or email, no matter how friendly or official the circumstances may appear. Watch out for people who may be trying to look over your shoulder while you use the ATM, seeking to steal your personal identification number. In case your wallet is lost or stolen, carry only the identification you really need: checks, credit or debit cards. Keep the rest, including your Social Security card, in a safe place. Do not preprint your Social Security number, telephone number, or driver's license number on your checks. You do not have to give merchants your Social Security number; if requested, ask the merchant to use another form of identification that does not include your Social Security number (e.g., a passport or driver's license).

- **Protect your incoming and outgoing mail.**
  For incoming mail: Try to use a locked mailbox or other secure location (e.g., a post office box). If your mailbox is not locked or in a secure location, try to promptly remove mail that has been delivered or move the mailbox to a safer place. When ordering new checks, ask about having the checks delivered to your bank branch instead of having them mailed to your home where you run the risk of a thief finding them outside your front door.

  For outgoing mail containing a check or personal information: Try to deposit it in a United States (U.S.) Postal Service blue collection box, hand it to a mail carrier, or take it to the post office instead of leaving it in your doorway or home mailbox. A mailbox that holds your outgoing bills is a prime target for thieves who cruise neighborhoods looking

for account information. Avoid putting up the mailbox flag to indicate that outgoing mail is waiting.

- **Sign up for direct deposit.**
  Sign up for direct deposit of your paycheck, retirement check, and/ or state or federal benefits, (e.g., Social Security). Direct deposit prevents someone from stealing a check out of your mailbox and forging your signature to access your money. Direct deposit is also beneficial in the event of a disaster.
- **Keep your financial trash "clean."**
  Thieves known as dumpster divers search through garbage looking for pieces of paper containing Social Security numbers, bank account information, and other details they can use to commit fraud. What is your best protection against dumpster divers? Before tossing out these items, destroy them, preferably using a crosscut shredder that turns paper into confetti that cannot be easily reconstructed.

Contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious.

- **Keep a close watch on your bank account statements and credit card bills.**
  Monitor these statements each month and contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious (e.g., a missing payment or an unauthorized withdrawal). Contact your institution if a bank statement or credit card bill does not arrive on time. Missing financially related mail could be a sign someone has stolen your mail and/ or account information, and may have changed your mailing address to run up bills in your name from a phony location.

- **Avoid come-ons for personal information on the internet.** As was mentioned in the section on Computer/Internet Scams, never provide bank account or other personal information in response to an unsolicited email, telephone call, text message or when visiting a website that does not explain how personal information will be protected. Legitimate organizations would not ask you for these details because they already have the necessary information, or can obtain it in other ways. If you believe the correspondence is fraudulent, consider bringing it to the attention of the Federal Trade Commission (FTC) via its online complaint form: **ftccomplaintassistant.gov**.

  If you do open and respond to a phony email, contact your financial institution immediately and follow the steps listed in the FTC brochures listed at the end of this guide. For more about avoiding phishing scams, visit **consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams**.

- **Review your credit report annually (every 12 months) and report fraudulent activity.** Review your credit report carefully for warning signs of actual or potential identity theft. For example, items that include mention of a credit card, loan, or lease you never signed up for, or requests for copies of your credit report from someone you do not recognize could be a sign that a con artist is snooping around for personal information. To obtain a free copy of your credit report, visit **annualcreditreport.com.**

You can submit a complaint about problems with credit reporting companies or information about your credit reports to the CFPB at **consumerfinance.gov** or 1-855-411-2372. For more information: **consumer.ftc.gov/blog/2017/09/fraud-alert-or-credit-freeze-which-right-you** or Ask CFPB at **consumerfinance.gov/askcfpb.**

Fraud Alert: Social Security Administration

The Inspector General for the Social Security Administration (SSA) is warning the public, and Social Security beneficiaries in particular, to be aware of fraud scams that target personal information.

In the most recent scam, identity thieves obtain the personal information of Social Security beneficiaries and use that information to attempt to open a counterfeit "my Social Security" online account on SSA's website **ssa.gov**. If successful, they then use that account to redirect the beneficiary's direct deposit benefits to an account controlled by the thief.

Protect your personal information as you would any other thing of value.

This should not discourage people from using SSA's "my Social Security" feature, which enables the public to set up an online account to view earnings history and estimated benefits, and allows beneficiaries to obtain a host of services online. Establishing your "my Social Security" account yourself eliminates the risk of a phony account being opened by an identity thief. This type of crime does, however, serve as a reminder to protect your personal information as you would any other thing of value. Once thieves have your personal information, they can use it to open credit accounts, buy homes, claim tax refunds, and commit other types of costly fraud.

If you receive information from SSA indicating that you have opened a "my Social Security" account, and you did not open the account, you should contact Social Security promptly so that appropriate action may be taken, and the matter may be referred to the Office of the Inspector General. You can do so by visiting or calling a local SSA office or calling SSA's toll free customer service at 1-800-772-1213. Individuals who are deaf or hearing-impaired can call Social Security's TTY number at 1-800-325-0778.

Identity Theft: If You Think You May Be a Victim

If you believe you are a victim of identity theft, the FTC recommends that you immediately take the following actions:

- Place an initial fraud alert with one of the three nationwide credit reporting companies.
- Order your credit reports and review for incorrect information or new, unauthorized account activity.
- Create an identity theft report.
- Consider placing an extended fraud alert or security freeze on your credit report to limit the circumstances under which a credit reporting company may release your credit report.

The FTC has many resources available to help you. Call the FTC's Identity Theft Hotline at 1- 877-IDTHEFT (438-4338) or visit **identitytheft.gov**. Its online toolkit includes:

- A detailed guide for protecting your information, with instructions and sample letters to help identity theft victims.
- Sample letters to help you dispute unauthorized charges or the opening of new accounts in your name. Sample letters and forms are available at **identitytheft.gov/Sample-Letters**.

Medical Identity Theft

Medical identity theft is serious business. According to one study, about 1.5 million adults are victims of medical identity theft each year.

What Is Medical Identity Theft?

Medical ID theft occurs when someone steals personal information — such as your name and Medicare number — and uses the information to get medical treatment, prescription drugs, surgery and/or other services and then bills Medicare for it.

A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file phony claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, or credit report may be affected.

Every time a thief uses your identity to get care, a record is created with incorrect medical information about you.

If you see signs of medical identity theft, order copies of your records and check for mistakes. You have the right to correct these mistakes.

Medical ID theft can cause financial harm but it is about more than just losing time and money. Sometimes people are denied Medicare coverage for a service or medical equipment because their records falsely show they already received it, when in fact it went to someone posing as them.

It can affect your medical and health insurance records. Every time a thief uses your identity to get care, a record is created with incorrect medical information about you. That information might include:

- A different blood type
- An inaccurate history of drug or alcohol abuse
- Test results that are not yours

- A diagnosis of an illness, allergy or condition that you do not have, which could lead to you receiving the wrong treatment and even being injured or getting sick due to an incorrect treatment.

All types of people, including doctors and medical equipment companies, have been caught stealing people's medical identities. There have even been links to the mafia and thieves in other countries. Sadly, about one-third of medical identity thieves are family members.

How Do You Learn if You Are a Victim?

Here are some warning signs that your identity may have been stolen:

You are denied insurance for a medical condition you do not have.

- You get a bill for medical services you did not receive.
- You are contacted by a debt collection company for money you do not owe.
- Your insurance company says you've reached your limit on medical benefits.
- You are denied insurance for a medical condition you do not have.

How to Avoid Medical Identity Theft

- Protect your Medicare and other health insurance cards in the same way you would protect a credit card.
- Review your Medicare Summary Notices (MSN), Explanations of Benefits (EOB) statements and medical bills for suspicious charges. If you find incorrect information in your records, insist that it be corrected or removed.
- Only give personal information to Medicare-approved doctors, other providers and suppliers, your State Health Insurance Assistance Program or Senior Medicare Patrol (SMP) program, or the Social Security Administration. Call 1-800-MEDICARE (1-800-633-4227) if you aren't sure if a provider is approved by Medicare.
- Beware of offers of free medical equipment, services or goods in exchange for your Medicare number.
- Shred papers with your medical identity before putting them in the trash.
- Remove or destroy labels on prescription bottles and packages before you put them in the trash.

Remove or destroy labels on prescription bottles and packages before you put them in the trash.

How to Respond if You Suspect Medical Identity Theft

- Ask your health care provider for a copy of your current medical file. If anything seems wrong, write to your health plan or provider and ask for a correction.
- Contact your local Senior Medicare Patrol (see contact information below).

How Your Senior Medicare Patrol (SMP) Can Help

Your local SMP is ready to provide you with the information you need to protect yourself from Medicare errors, fraud and abuse, detect potential errors, and report your concerns. For more information or to locate your state SMP go to **smpresource.org**.

ACTIVITY 3: Identity Theft Self-Check

Review each response on the list and indicate whether you perform this action always, sometimes, or never. Then, tally your score and see how well you are taking measures to avoid identity theft.

	Always 2 points	Sometimes 1 point	Never 0 points
1. Cover or block the Point of Service (POS)/ATM keypad when I enter my PIN			
2. Carry only the identification, checks, credit cards, or debit cards I really need			
3. Use direct deposit for paychecks, tax refunds, benefits payments, etc.			
4. Shred documents with personal/financial information before disposing of/recycling them			
5. Use complex passwords with a mix of numbers, symbols, and letters instead of easily guessed words			
6. Review financial statements/bills monthly and identify/correct errors			
7. Review my credit report annually and identify/correct errors			
8. Use secure mailboxes for incoming/outgoing mail			
9. Avoid providing/sharing personal information (e.g., SSN) whenever possible			
10. Review my Medicare Summary Notices (MSN), Explanations of Benefits (EOB) statements, and medical bills for suspicious charges.			
Total each column			

Grand Total _____

Scores:

0–6: You are not taking many actions to minimize your risk of identity theft. Consider what you have learned today, and see what steps you can take to protect your identity.

7–13: You have developed some good practices to avoid identity theft; however, you have room for improvement. Consider what actions you need to take or apply more regularly to better protect your identity.

14–20: You are doing a great job at minimizing your risk of identity theft. Continue to apply these actions regularly and determine what additional steps you can take to protect your identity