Simple Safeguards: Preventing Identity Theft

1. Protect Your Personal Information

- Don't carry your social security card.
- If asked to provide it -- ask the person what law requires you to give your number and what happens if you refuse.

2. Protect Your Documents

- Shred your confidential trash with a cross-cut or diamond cut shredder.
- Don't leave outgoing mail with personal information in your mailbox for pick-up.

3. Be Vigilant Against Tricks

- Never provide personal information to anyone in response to an unsolicited request.
- Never reply to unsolicited emails from unknown senders or their attachments.

4. Protect Your Communications

- Make sure you have updated security software on your home computer.
- Don't conduct sensitive transactions on a computer that is not under your control.
- If you have wireless internet, make sure it is password protected.

5. Check Your Credit Report

- Order credit reports at least three times per year.
- Check financial accounts often and investigate any unusual activity.

To remove your name from lists:
Mail: www.dmachoice.org; Phone: www.donotcall.gov
To stop preapproved credit card offers:
Web: www.optoutprescreen.com
Phone: 1-888-5-OPTOUT (567-8688)
To hold your mail: www.usps.com

If a loved one dies:

- Send a copy of the death certificate to the three credit reporting agencies.
- Notify the Social Security Administration immediately.
- Don't mention a woman's maiden name or exact birth date in the obituary.

Credit Reporting Bureaus

Equifax: (800) 525-6285
P.O. Box 740241 Atlanta, GA 30374
Experian: (888) 397-3742
P.O. Box 9530 Allen, TX 75013
Trans Union: (800) 680-7289
P.O. Box 6790 Fullerton, CA 92834

- To place a fraud alert on your account with all three credit reporting agencies: www.fraudalerts.equifax.com
- You are allowed 3 free reports per year; to order:
  On Web: www.annualcreditreport.com
  By Phone: 1-877-322-8228

Terms to Understand:

1. **Fraud Alert:** Your credit file at all three credit reporting agencies is flagged and a potential lender should take steps to verify that you have authorized the request.
   Inside Scoop: Fraud alerts only work if the merchant pays attention and takes steps to verify the identity of the applicant. They expire in 90 days unless you have been a victim of identity theft, in which case you can file an extended alert – it lasts for seven years.
2. **Credit Monitoring:** Your credit files are monitored by a third party – if activity occurs, you are notified.
   Inside Scoop: Talk to your insurance agent about what they offer. It is most likely the least expensive way to protect you and your family.
3. **Credit Freeze:** A total lockdown of new account activity in your name. This requires unfreezing before you can open an account.
   Inside Scoop: Although effective, credit freezing can be cumbersome to start and stop. Credit freeze laws vary by state. To check the laws for your state, go to: www.consumersunion.org

To Report Internet Fraud: www.ic3.gov
Key Numbers:
FBI: (202) 324-3000 or your local field office
FTC: 1-877-IDTHEFT
Postal Inspection Service: 1-877-876-2455
IRS: 1-800-829-0433
Social Security Administration: 1-800-269-0271

Simple Safeguards:
Preventing Medical Identity Theft

1. **Keep Track of Your Insurance Cards**
   Protect your health insurance card just as you would your ATM card or Social Security Card. Report lost or stolen cards to your insurer immediately. Never lend your card to someone and never provide your insurance information to someone over the phone.
2. **Scrutinize Your Statements**
   You should receive an "explanation of benefits statement" every time a medical claim is made. You should check these statements carefully for any unusual charges for medical services that you do not remember getting. If you have a question about something listed, call your insurer to get more details.
3. **Get an Annual Statement**
   Sophisticated thieves know how to redirect your explanation of benefits to a fake address. To counter this, ask your insurer for an annual itemized list of all claims billed to you. Fraudulent claims that may not have appeared on your explanation of benefits should show up on this list.
4. **Check Your Credit Report**
   Do it regularly. Unpaid hospital or doctor bills that have gone to a collection agency will eventually show up on your credit report. You can get a free annual copy of your report from all three credit reporting agencies at: www.annualcreditreport.com
5. **Get Copies of Medical Records**
   Do it routinely. Each time you go to the doctor or hospital, request a copy of your medical records and keep them in a safe place at home. That way, if someone does steal your information and your medical records are altered, you'll have the "before" copies. These documents will make it much easier to prove your identity when you report the fraud. They will also help when trying to correct the files.
6. **Avoid Offers of Free Services**
   This is a common ruse for fraudsters. It is better to have routine screenings done through your physician's office.

If You Think You Are a Victim:

Call Your Insurer

Most insurance companies have antifraud units that specialize in medical identity theft problems. If you think you are a victim of identity theft, call the insurer's customer service and ask for the antifraud hotline.

Check Suspicious Medical Records

Contact the provider in question and ask for a copy of the medical records in your name. Do this even if you have to pay for the records.

Do Not Tell Them You Suspect Fraud

The minute you say there may be someone posing as you to get medical care, the provider may not let you see the records. Once you have the records, you can then look for discrepancies, like a different age from yours, or a history of diseases you do not have. This will help prove the fraud.

File a Police Report

You will need this to open an investigation, get access to medical records, and to help clear up any problems on your credit report.

can be cumbersome to start and stop. Credit

Resource:
World Privacy Forum