Resources

To File a Complaint Online:
www.ftc.gov/IDTheft

Blue Cross/Blue Shield's antifraud site:
www.bcbs.com/blueresources/anti-fraud/prevent-medical-identity-theft.html

Credit-Related Fraud:
This site includes guidelines and a chart to organize and document your efforts if you should become the victim of identity theft.
www.ftc.gov/bcp/edu/pubs/consumer/credit/cre16.shtm

Financial Fraud:
Contact your financial institution. If you have any trouble getting your situation resolved, visit The National Information Center of The Federal Reserve System (www.ffiec.gov/nicpubweb/nicweb/nichome.aspx), then click on the link for Institution Search. You will get information on the institution that oversees your bank.

Investment Fraud:
www.sec.gov/complaint.shtml

Bankruptcy Fraud:
www.usdoj.gov/ust

Fraud Related To Student Loans:
http://ed.gov/about/offices/list/oig/hotline.html?src=rt

Fraud Related To Federal Taxes:
http://www.irs.gov/privacy/article/0,,id=186436,00.html

Healthcare-Related Fraud:
If your suspect identity theft related to Medicare or Medicaid, call **(**800) HHS-TIPS (800-447-8477**).**
www.ftc.gov/IDTheft.

American Association of Retired Persons (AARP):
www.aarp.org/learntech/personal_finance

American Health Information Management Association:
www.myphr.com

Social Security Benefits Fraud:
www.socialsecurity.gov/oig/hotline
The Social Security Administration maintains an informational site related to identity theft at
www.socialsecurity.gov/pubs/idtheft.htm

Identity Theft Involving a Minor/Child:
E-mail childidtheft@TransUnion.com

Better Business Bureau:
www.bbb.org

Blue Cross/Blue Shield:
www.bcbs.com/antifraud

Consumers Union - Summary of freeze laws:
www.consumersunion.org/campaigns/learn_more/003484indiv.html

Organizing Your Case:
The Federal Trade Commission has published a very useful guide, "Take Charge: Fighting Back Against Identity Theft." The following guidelines and tables will help you organize your case and resolve it quicker. These were taken directly from the FTC's site www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm

For the latest scams, schemes and trends related to identity theft, monitor the following:

Technorati
www.technorati.com/tags/identitytheft

Fight Identity Theft Blog
www.fightidentitytheft.com/blog

Schneier On Security
www.schneier.com/blog

Identity Theft Blog By Truston
www.mytruston.com/blog

Protecting Your Digital Footprint: Practical Tips for Protecting Your Personal Identity

Identity Theft Resource Center
www.idtheftcenter.org

- The ITRC educates consumers, corporations, government agencies and other organizations on best practices for fraud and identity theft detection, reduction and mitigation.
- The ITRC provides best in class victim assistance at no charge to consumers throughout the United States.

What is Identity Theft?

Identity theft occurs when an imposter gains access to personal identifying information and uses it for personal gain and exploitation.

Who is at Risk?

Everyone that has information collected and stored about them ***anywhere*** and at ***any time*** in the past **is at risk**!

What are The Forms of Identity Theft?

- Credit cards, including fraudulently charging goods/services on someone's existing account, and opening a new line of credit and obtaining a new card based on information stolen from another person.
- Phone/utilities, including fraudulently gaining access to services on someone's account
- Banks, including unauthorized transfer of funds from a checking account, fraudulent loans and forged checks.
- Employment, including scammers who pretend to be prospective employers, who attempt to gather personal information from people looking for a job.
- Government documents/benefits, including fraudulently receiving Social Security and Medicare benefits.

Finger Lakes Library System
119 E. Green St. Ithaca, NY 14850
Phone: 607-273-4074 www.flls.org

Protecting Your Digital Footprint:
Practical Tips for Protecting Your Personal Identity

How Do You Protect Yourself?

- Take inventory of **everything in your wallet or purse** in case anything is stolen so you can notify the appropriate organization(s). Photocopy the front and back of all cards and documentation that you need to carry with you. However, be sure to remove anything that includes your social security number (SSN).
- Safeguard your **private financial information**, including your SSN, checking account numbers, credit card numbers and any other information that can identify any of your accounts.
- Safeguard any **documents in your home** (including near windows) and **car** that contain personal information.
- Monitor your earnings through the Social Security Administration www.ssa.gov/mystatement; (800) 772-1213).
- If your reported earnings are greater than what you know to be your actual earnings, report possible fraud to the Administration.
- Report **lost/stolen checks** as soon as possible.
- Advise your bank if you receive **phone inquiries** related to any type of "statement" or "prize".
- Shred any **financial offers** or **statements** with a crosscut shredder, including credit card solicitations and pre-approved offers that include pre-printed checks.
- Opt out with marketing companies of future **credit card solicitations** by calling (888) 5OPTOUT.
- Shred **pieces of mail** that contain **any** personal information (solicitations, financial or medical forms, etc.)
- Never leave documents where criminals can gain possession of them.
- Place your **outgoing mail** in an official Postal Service box, give it to a postal carrier or bring it to the post office.
- Retrieve your **incoming mail** from a locking mailbox or a Postal Office Box.
- Direct your bank to deliver your **new checks** directly to your bank where you can pick them up.
- Advise any organization you do business with if you are expecting a **regular invoice** and it does not arrive.
- Make sure that background checks are con ducted on any in-home or institutional caregivers.
- Advise any of your financial institutions if any of your **regularly scheduled statements** does not arrive on time. If you are told that it has been sent to a different address, you may already be a victim.
- Investigate any unexplained items on your **bills** or **statements**.
- Close any **unused/inactive lines of credit**, asking the creditor to note in your file that the "account was closed at the request of the customer"
- **Notifying the credit reporting agencies of the death** of a loved one to prevent anyone from opening a new line of credit in the decease's name.
- **When writing an obituary**, don't use an exact date of death or birth
- Check your **credit report** once a year by requesting a free report from www.annualcreditreport.com
- Consider **freezing your credit** so that no one but you can open a new line of credit in your name without you temporarily lifting the freeze.
- Closely monitor **Explanation of Benefits Forms** from any health insurer, even if you don't owe any money
- Once a year, request a **listing of benefits** from your health insurers that have been paid in your name.

Finger Lakes Library System
119 E. Green St. Ithaca, NY 14850
Phone: 607-273-4074 www.flls.org

What to Do If You Become A Victim:

Please note that it is important to follow proper procedures in order to preserve your rights under The Fair Credit Billing Act

If You Are The Victim of Credit-related Fraud :

Contact the card issuing company within 60 days of the date that the first bill that containing the error was mailed to you. You'll need to use the "Billing Inquiries" address of the company, not the address to which you send your payments.

- Contact each of the three credit reporting agencies to place a fraud alert on each of your credit reports, and request a free copy of your credit report from each agency.
- Review your credit reports.
- Close any accounts that have been opened fraudulently or exhibit suspicious activity.
- Contact all applicable creditors in writing, notifying them that you are disputing the transaction(s) and alerting them to the possibility of fraud
- Change all associated passwords, if applicable.
- File a "miscellaneous incidents" report with local law enforcement
- File a complaint with the Federal Trade Commission
- Follow-up in writing at Identity Theft Clearinghouse
- Have a plan when you contact a company. Prepare a list of questions to ask the representative, as well as information about your identity theft.
- Write down the name of everyone you talk to, what he or she tells you, and the date the conversation occurred.
- Follow up in writing with all contacts you've made on the phone or in person. Use certified mail, return receipt requested.
- Keep copies of all correspondence or forms you send.
- Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.
- Keep old files even if you believe your case is closed.