## How can you review & monitor your personal information?

According to the US government, the first signs of Identity Theft often go unnoticed. The best way to detect any fraud against you is to monitor your accounts each month and access your credit report regularly. This will allow you to take actions necessary to correct your records and prevent any further problems.

There are three major credit reporting agencies in the United States. As a consumer, you are able to request and correct any information that is reported there. Typically, one report from each agency is available every year at no cost. You should order your credit report every year from all three companies. Many experts recommend that reports be staggered throughout the year to review your credit information regularly (still at no charge). The three major companies are:

**Equifax:** +1 800-685-1111

**Experian:** +1 888-EXPERIAN (397-3742)

**TransUnion:** +1 800-680-7289

Any mistakes or errors listed in your credit report should be corrected immediately! Always submit your correction requests in writing to the reporting agency, with a return receipt requested to verify delivery.

## Are you an identity victim?

If you believe you may be a victim of this crime, you should take immediate steps to protect against continued damage. You can always dispute any unauthorized transactions with your banking, credit, and other financial institutions. It is also appropriate to notify the major credit reporting agencies that you have been a victim of identity theft and to file a police report. For more guidance and to report this crime to the government, contact the US Federal Trade Commission:

Internet: www.consumer.gov/idtheft
Telephone: +1-877-IDTHEFT

## Additional Resources:

US Social Security Administration:
www.socialsecurity.gov

Consumer Government Agencies:
www.consumer.gov/idtheft
www.ftc.gov/bcp/edu/microsites/idtheft/

Major Credit Reporting Agencies:
www.equifax.com
www.experian.com
www.transunion.com

## Credits:

Information for this bulletin was adapted from the following resources:

- US Department of Justice
- State of New York, Office of the Attorney General

# PROTECTING YOUR IDENTITY IN THE UNITED STATES

*Understanding the risks of Identity Theft and how to keep your Social Security Number & other personal information safe*

**International Services Office**

213 Morey Hall, Box 270446
Rochester, NY 14627
Phone: +1 585-275-2866
http://www.iso.rochester.edu

## What is Identity Theft?

Identity theft is the crime of wrongfully obtaining and using someone's personal information to cause fraud or deception, usually for economic gain. Most often, victims will experience this as fraudulent access to their financial accounts or unauthorized debt collected under their name. Serious damage to the victim's reputation and credit standing can also occur. Many forms of identity theft exist and the time and energy to resolve such problems can be overwhelming. The best defense against such crimes is to keep personal details private and safe, to avoid becoming a victim.

## How does Identity Theft happen?

Identity theft is possible when a criminal obtains your personal information, especially your SSN, bank account or credit card numbers, and new offers for credit or financial services. Thieves typically gain access to personal information by:

- Stealing wallets, purses and mail items (bank and credit statements, pre-approved offers, and tax forms).
- Viewing details you provide to an unsecured site on the Internet.
- Posing as someone who legitimately needs information about you, such as employers or landlords.
- Sorting through trashed items for personal data.

## How can you protect yourself?

***Protecting Social Security Numbers:***

Your Social Security Number (SSN) is assigned to you for life and is used to identify you within the United States for legal and financial purposes, such as reporting employment wages, taxation, and monitoring your credit history. The SSN is a useful tool for identifying yourself in the United States, but this and other important details can be used against you if they are not well protected.

You should only give out your SSN when it is absolutely necessary and only to a legitimate representative. Your employer and financial institutions will need your SSN for wage and tax reporting purposes.

Some private businesses may ask for the SSN in order to perform a credit check before agreeing to serve you. It's up to you to decide whether to share it, but it is also their right to refuse service without that info. If asked for your SSN, find out if you can provide some other form of identification instead. Ask why your SSN is needed, how it will be used, and what will happen if you refuse to disclose it.

DO NOT carry your Social Security Card with you! Since the SSN is assigned for life, you can replace a lost card but the number may be found and used without your permission. **Keep it in a safe place, but not with your immigration documents.**

***Other recommended strategies:***

- Do not give out personal information over the phone, Internet, or by mail, unless you have initiated the contact or know whom you are dealing with.
- Don't give out personal information without asking how it will be used and whether it will be given to others. Ask to keep your information confidential.
- Minimize the identification details and number of credit or debit cards you carry. Take only what you'll actually need. Do not list phone numbers on your personal checks.
- Do not use personal information when creating passwords (SSN, date of birth, mother's maiden name, etc.)
- Pay attention to your billing cycles and statements. Follow up with creditors immediately if bills don't arrive on time or list fraudulent charges. A missing bill could indicate that your address was changed without your permission.
- Shred all documents with personal or financial information you intend to discard, including pre-approved credit applications, insurance forms, bank checks, and old financial statements. Request a hold on your incoming mail if you will be traveling.
- Be alert when using ATMs and phone cards in public. Thieves may be trying to see your access codes.