



June 2004

FL/Financial Fitness/2004-01

Preventing Identity Theft

Christine E. Jensen, MS, CFCS
Family/Consumer Science Agent

Identity theft is becoming more common and is a very serious crime. Victims of identity theft can spend months or years and a lot of hard earned money cleaning up the mess thieves have made of their good name and credit record. Identity thieves can use your personal information to take over your credit accounts and open new ones. They may even use your good credit to get a job, take out a car loan, or rent an apartment. Identity theft victims may lose job opportunities, be refused loans for education, housing or cars, or even get arrested for crimes they didn't commit.

While it is not possible to totally prevent identity theft and/or credit fraud, you can reduce the likelihood that it will happen by managing your personal information carefully.

The following tips may help you avoid becoming an identity theft victim.

- Find out who has access to your information at work. Be sure to verify that records are kept in a secure location and are accessible only to employees who have a legitimate reason to access them.
- Shred or burn all papers that contain personal information about you. To prevent thieves from going through your trash or recycling bin to obtain personal information, tear or shred your charge receipts, credit applications, insurance forms, bank statements, expired credit cards and pre-approved credit offers. You should never throw them in the garbage intact. Make sure business offices do the same thing with documents containing your information.
- Pay attention to your mail, especially billing cycles. Contact creditors immediately if your bills arrive late. A missing bill could mean an identity thief has taken over your credit card account and changed your billing address. Deposit outgoing mail in post office collection boxes or at your local post office.
- Be careful about giving out personal financial information. Whether by phone, mail, or the Internet, never give anyone who calls your credit card number, Social Security number, or other personal information unless you initiated the activity and understand the transaction. Ask to use other types of identifiers when possible.
- When ordering checks, have only your initials (instead of full first names) and last name printed on them. If your checkbook is stolen, thieves will not know whether you sign your checks with just your initials, your first name, or a shortened name. Your bank will know how you sign your checks, and will pull suspicious checks and call to verify the purchase.
- When using your checking account to pay on your credit card accounts, DO NOT put the complete account number on the "Memo" line. Instead, just put the last four digits of the account there. The credit card company knows the rest of the number and anyone who might be handling your check as it passes through the processing channels won't have access to the full number.
- Put your work phone number on your checks instead of your home number. If you have a post office box, use that instead of your physical address.
- Never have your driver's license number printed on the checks.
- Never have your Social Security number printed on the checks.
- Avoid carrying your Social Security card in your wallet unless you know you will need it for a specific purpose. It is the most important and consequently the most sought-after piece of your personal information. Also be cautious with your health insurance card, since your account number is often the same as your Social Security number. College students should be especially careful with student identification cards, since the student identification number is often a Social Security number. Students should ask for a randomly generated number if possible. Refrain from giving out your number unless it is for a legitimate purpose, such as completing a loan application. Any agency or business can ask for your Social Security number, but only a few entities, such as motor vehicle departments, tax departments, welfare departments, banks, brokerages and employers, can actually demand it.
- Place the contents of your wallet on a photocopy machine. Copy both sides of each license, credit card, etc. This will give you all the account

numbers and phone numbers to call if it becomes necessary to cancel them. Keep copies in a safe place separate from your wallet. Usually the phone number for reporting stolen cards is on the back of the card. If you don't have the card, it is more difficult to report theft.

- If you have a passport, make a photocopy and keep in a safe place. This will aid you in replacing the document if it is ever stolen.

Credit Cards

- Guard your credit cards. Minimize the information and the number of cards you carry in your wallet. If you lose a card, contact the fraud division of the credit card company. If you apply for a new credit card and it doesn't arrive in a reasonable period, contact the issuer. Watch cashiers when you give them your card for a purchase. Make sure you read your receipt. Check to make sure the balance is correct and the same as the cashier told you. Do not leave any carbons or other items which may give your number to would-be thieves. Also, when you receive a new card, sign it in permanent ink and activate it immediately. Make sure all cards are signed. Do not leave cards blank, since anyone can sign and use a blank card.
- Never fax your credit card number. Your credit card number can lie for hours in the fax basket at the other end. Anyone passing by can record your number and begin to use your card number fraudulently. It is even possible for criminals to intercept your credit card number while the fax is in transmission.
- Be smart about passwords and Personal Identification Numbers (PINs). Memorize your passwords and PINs instead of carrying them with you. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- On the Internet, look for an Internet address that begins <https://>. The "s" indicates that it is a secure connection and a small padlock symbol should appear in the bottom right hand corner of your screen, indicating it is safe to transmit your credit card number.

If your purse or wallet is stolen:

- Cancel all credit cards immediately. Contact the financial institution where you have your checking and savings accounts. Generally, your local bank can place a fraud alert on your accounts faster than a central number.
- Call the three national credit reporting agencies immediately to place a fraud alert on your name and Social Security number. This alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit. To place a fraud alert on your account or report fraud contact:

Equifax: 1-800-525-6285 or write:
P.O. Box 740241,
Atlanta GA 30374-0241

Experian (formerly TRW):
1-888-397-3742 or write:
P.O. Box 9532, Allen TX 75013

Trans Union: 1-800-680-7289, or write:
Fraud Victim Assistance Division,
P.O. Box 6790, Fullerton CA 92834-6790

Social Security Administration (fraud line): 1-800-269-0271

- File a police report immediately in the jurisdiction where it was stolen. This indicates to credit providers you were diligent in handling the theft. It's also the first step if a criminal investigation is ever needed.
- Check your credit report regularly. Checking your credit report will ensure an early alert on possible accounts, or fraudulent activity with your credit. This can help to prevent costly problems. You may need to pay a nominal fee for a copy. Requesting a copy of your credit report does NOT affect your credit report in a negative way. It's also a good idea to review your credit report from each of the three major credit reporting agencies every year. It's possible that information is being reported to one but not the others.

Utah State University is committed to providing an environment free from harassment and other forms of illegal discrimination based on race, color, religion, sex, national origin, age (40 and older), disability, and veteran's status. USU's policy also prohibits discrimination on the basis of sexual orientation in employment and academic related practices and decisions.

Utah State University employees and students cannot, because of race, color, religion, sex, national origin, age, disability, or veteran's status, refuse to hire; discharge; promote; demote; terminate; discriminate in compensation; or discriminate regarding terms, privileges, or conditions of employment, against any person otherwise qualified. Employees and students also cannot discriminate in the classroom, residence halls, or in on/off campus, USU-sponsored events and activities.

This publication is issued in furtherance of Cooperative Extension work. Acts of May 8 and June 30, 1914, in cooperation with the U.S. Department of Agriculture, Jack M. Payne, Vice President and Director, Cooperative Extension Service, Utah State University.