How to Protect Yourself from Identity Theft

The single most important thing you can do is check your credit report at least once a year. If you are a victim of identity theft, you will catch it early by checking your credit report regularly.

Reduce access to your personal data:

- Do not carry extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse, except when needed. At work and at home, store your wallet, cards and important documents in a safe place.
- If possible, do not carry other cards that include your Social Security number (health insurance cards, etc.), except on days you need them.
- Consider removing your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian, and Trans Union. This will limit the number of pre-approved credit offers you receive. Call 888-5OPTOUT or go online to www.optoutprescreen.com.
- Choose to Opt-out when your bank, credit card, insurance, or investment companies ask you if they can sell or share your financial information, just say, "No".
- Sign up for the Federal Trade Commission's National Do Not Call Registry. www.donotcall.gov, (888) 382-1222; TTY (866) 290-4236
- Have your name and address removed from the phone book and reverse directories.
- When you are away from home for an extended time, have your mail held at the Post Office.
- When you pay bills through the mail, do not leave envelopes containing checks in an unlocked mailbox, or at the receptionist's desk in your workplace, for postal pick-up.

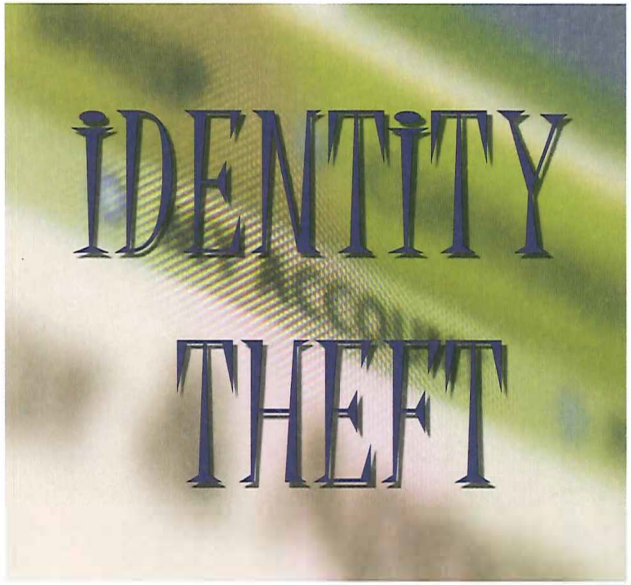
Protect your credit cards and credit reports:

- Reduce the number of credit cards you actively use and carry to a minimum. Consider canceling unused accounts.
- Make a list or photocopy your credit cards, bank accounts, and investments, including account numbers, expiration dates and the telephone numbers of customer service and fraud departments. Keep the list in a secure place (not your wallet or purse) to quickly contact these companies in case your credit cards are lost or stolen or the accounts are used fraudulently.
- Never give out your Social Security Number, credit card number or other personal information over the phone, by mail, or on the Internet unless you have a trusted business relationship with the company and you have initiated the call.
- When shopping, always take credit card receipts; put them in your wallet, not in the shopping bag, and never in public trash containers.
- Never permit your credit card number to be written onto your checks.
- Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive.

Passwords and PINS:

- Create passwords and PINs (personal identification numbers) that combine letters and numbers. Do not use any part of your Social Security number, your mother's maiden name, birthdate, middle name, pet's name, or anything else that could easily be discovered by thieves.
- Memorize all your passwords. Don't record them on anything.
- Shield your hand when using ATM machines or when making phone calls with your phone card. "Shoulder surfers" may be nearby with binoculars or video camera.

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation



What To Do...

If you suspect that someone has used your personal information to get a credit card or a loan.

How to Protect Yourself

You can reduce your risk of fraud by following the tips in this guide.

University of Florida Privacy Office
http://privacy.health.ufl.edu
privacy@ufl.edu

If you think your identity has been stolen, here's what to do:

1. Contact the fraud departments of the three consumer reporting companies to place a "fraud alert" or a "credit freeze" on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts.

2. Close accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit form, found on the Federal Trade Commission's website, when disputing new unauthorized accounts.

3. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report, to submit to your creditors and others that may require proof of the crime.

4. File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps us learn more about identity theft and the problems victims are having so that we can better assist you.

What is a Fraud Alert?

There are two types of fraud alerts: an **initial** alert, and an **extended** alert.

To place a fraud alert, you only need to contact one of the three companies, then that company is required to contact the other two. All three are to place an alert on their versions of your report. You will be required to provide appropriate proof of your identity, including Social Security number, name, address and other personal information.

• **An initial fraud alert stays on your credit report for at least 90 days and is free.** The fraud alert flags a creditor to contact you and speak with you directly prior to issuing you any credit. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or may be a victim of identity theft. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer-reporting companies.

• **An extended fraud alert stays on your credit report for seven years. There is a fee for this service.** In addition, your name will be removed from lists marketing prescreened credit offers for five years. You can have an extended alert placed on your credit report if you provide the consumer reporting company with an "identity theft report." After you have placed an extended alert, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer-reporting companies.

What is a Credit Freeze?

A **credit or security freeze** is a notice, placed at the request of the consumer, that prohibits the credit reporting agency from releasing any consumer credit information to a third party without the consumer's written authorization. A freeze is a permanent action, but can be lifted temporarily as needed, using a password. Lenders and other businesses would not have access to your credit report to approve new credit, loans, and services.

With a credit freeze, your credit information can still be released to your existing creditors or to collection agencies acting on their behalf. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

To place a freeze, you must request it in writing to each of the three credit bureaus. There is a $10 fee to place, remove, or temporarily lift a security freeze. No fee is charged if you provide proof that you are a victim of identity theft or are more than 65 years old. A copy of the police report concerning identity theft must be provided to show that you are a victim of identity theft.

Important Contact Information

There are a number of services to help you respond if you have been a victim of identity theft. Below is a list of resources that we have compiled on your behalf.

Federal Trade Commission's Identity Theft Hotline: The FTC operates a call center for ID theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.consumer.gov/idtheft).

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790