



What is Identity Theft?

Identity theft is the criminal use of an individual's personal identification information. Identity thieves steal information such as your name, Social Security number, driver license information, or bank and credit card accounts and use the information to establish credit, make purchases, apply for loans or even seek employment.

The statistics are staggering. According to the Federal Trade Commission (FTC), Florida was ranked fifth in the nation for identity theft in 2006, with 17,780 reported victims and 25,902 cases of fraud reported.



Identity thieves often steal thousands of dollars from unsuspecting victims, in the victim's own name, without the victim knowing about the fraud for months or sometimes years.



How Does Identity Theft Occur?

All that is needed is a little information. Armed with this identifying information the identity thief can apply in person for instant credit, or through the mail by posing as you. Often, an identity thief will provide their own address (claiming to have moved) in an effort to prolong the fraud. Negligent credit grantors, in their rush to issue credit, do not verify information or addresses. Once the impostor opens the first account, they can use this new account, along with the other identifying information to bolster their credibility and obtain even more credit in your name.



Where Does the Information About Me Come From?

Many places! You do not need to lose your wallet or have anything tangible stolen in order for someone to steal your identity.

By simply failing to shred your confidential information, utility bills, credit card slips and other documents, it is easy for an identity thief to "Dumpster dive" your garbage and retrieve your most personal identifying information.

In addition, if an identity thief were to illegally obtain your credit report, they would have all the information necessary to become you.

You should also know that much of your identifying information is readily available on the Internet, or even at your local courthouse, where it is accessible by filing a public records request.



What Can I Do?

Florida's Identity Theft Resource and Response center is a good place to start. This resource provides exhaustive information regarding how to prevent ID theft, as well as a step-by-step walkthrough for reporting victimization and rebuilding credit.

Florida's Identity Theft Victim Kit, www.myfloridalegal.com/identitytheft provides everything from contact information for the three major credit bureaus, to standard affidavits.

This kit is designed to help you through the process of resolving your identity theft case and clearing your name.

Navigating through the system as an identity theft victim can be a lengthy and confusing process. As you contact law enforcement, creditors, and financial institutions, it is important that you keep track of the actions you take.

When your identity is stolen your personal identifiers can be misused in a variety of different ways. As soon as you become aware that your information has been misused, there are several basic steps you should take that apply to nearly all kinds of identity theft cases:



Step 1 Report the incident to the fraud department of the three major credit bureaus.

1. Ask the credit bureaus to place a "fraud alert" on your credit report.

2. Order copies of your credit reports and review for fraud.

Equifax

www.equifax.com

To order your report: 1-800-685-1111

To report fraud: 1-800-525-6285

TDD: 800-255-0056

TransUnion

www.transunion.com

To order your report: 1-800-888-4213

To report fraud: 1-800-680-7289

TDD: 877-553-7803

Experian

www.experian.com

To order your report: 1-888-EXPERIAN(397-3742)

To report fraud: 1-888-EXPERIAN (397-3742)

TDD: 800-972-0322

Step 2

Contact the fraud department of each of your creditors.

Report the incident to each creditor, even if your account at that institution has not been tampered with.

Follow up in writing immediately.

Step 3

Contact your bank or financial institution.

If your checks have been stolen, or if you believe they have been used, contact your bank or credit union and stop payment right away.

Call SCAN at 1-800-262-7771 to learn if bad checks have been passed in your name.

If you suspect your accounts have been compromised, cancel your checking and savings accounts and obtain new account numbers.



Step 4

Report the incident to law enforcement.

Contact your local police department or sheriff's office to file a report. Under Florida law, the report may be filed in the location in which the offense occurred or the city or county in which you reside.

When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief.





What else can I do?

File a complaint with the FTC's Identity Theft Clearinghouse

The Clearinghouse is the federal government's repository for ID theft complaints. Information is entered into a central database which is accessed by many local and state law enforcement agencies in Florida, as well as Florida's Attorney General, for identity theft investigations. Call the toll-free hotline at 1-877-IDTHEFT.

www.ftc.gov/idtheft

Flag your Florida Driver License

At your request, the Fraud Section of the Department of Highway Safety and Motor Vehicles will place a flag on your driver license if you are a victim of identity theft (regardless of whether your Florida Driver's License has been compromised). To reach the Fraud Section, call (850) 617-2405.

Get assistance through Florida's Fraud Hotline

Florida's Attorney General provides a toll-free fraud hotline for Floridians who are the victims of fraud. Contact 1-866-9-NO-SCAM (1-866-966-7226). Trained advocates can help provide additional information.

Check your Florida criminal history information

In some instances of identity theft, a victim may be faced with a criminal record for a crime he or she did not commit. The Florida Department of Law Enforcement can provide a Compromised Identity Review (based on a fingerprint comparison of state criminal history files). If a fingerprint check determines you are an identity theft victim, FDLE will work with local law enforcement agencies to attempt to clear fraudulent data from the criminal

history files and provide you with a Compromised Identity Certificate. Contact FDLE at 850-410-8880.

Remove your personal identifiers from Florida court records

Any person has the right to request the Clerk of the Circuit Court to redact/remove his or her Social Security number, bank account number, credit, debit or charge card number from an image or copy of an Official Record that has been placed on such Clerk's records, or in a court file. If you believe your personal information appears in a publicly available record, contact your County Clerk's Office.

Report Mail Theft to the U.S. Postal Inspection Service

The U.S. Postal Inspection Service will investigate if your mail has been stolen by an identity thief and was used to obtain new credit or commit fraud. Incidents should be reported to your nearest U.S. Postal Inspection Service district office.

Report Passport Fraud to the U.S. Department of State

If your passport is lost or stolen or you believe it is being used fraudulently, contact your local Department of State field office.

Protect your Social Security number

The Social Security Administration can verify the accuracy of the earnings reported on your social security number. To check for inaccuracies or fraud, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) from the Social Security Administration. Call 1-800-772-1213 or visit www.socialsecurity.gov



Preventing Identity Theft

Reduce your chances of being a victim of identity theft by remaining vigilant in all financial matters and taking precautions to protect your personal identifiers.

1. Order and closely review copies of your credit report from each national credit reporting agency once a year.
2. Reconcile your financial statements (bank and credit card) on a monthly basis.
3. Empty your wallet of extra credit cards and IDs. Close all unused credit card or bank accounts.
4. Shred pre-approved credit applications, credit card receipts, bills, and other financial information you don't want before discarding them in the trash or recycling bin.
5. Only release your personal data to businesses that require it for action you have initiated. Never give this information to unsolicited telephone callers or over the Internet.
6. Guard your passwords and PIN numbers closely.
7. Memorize your social security number and all passwords. Do not record them on any cards or on anything in your wallet or purse.
8. Deposit outgoing mail in mail collection boxes or at your local post office.
9. Contact your creditor or service provider if expected bills don't arrive.
10. Use caution when disclosing checking account numbers, credit card numbers, or other personal financial data at any web site or online service location unless you receive a secured authentication key from your provider.
11. Don't e-mail your personal data unless you use encryption technology.

Identity Theft

Protecting Your Good Name

Bill McCollum
Attorney General

Gerald M. Bailey, Commissioner
Florida Department of Law Enforcement

2007