

# **Don't Become a Victim of 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's 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, Florida was ranked fifth in the nation for identity theft in 2003, with over 14,000 reported victims.

## **How Does Identity Theft Occur?**

- All that is needed is a little information, such as your social security number, birth date, address, phone number, or any other information which can be discovered.
- Armed with this identifying information, and possibly a false driver's license with the identity thief's picture in place of yours, 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.
- As such, once the imposter 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.

When they don't pay the bills, the delinquent account is reported on your credit report!

## **Where Does the Information About You Come From?**

- ID thieves may resort to the old fashion way of simply stealing your wallet or purse from you, your home, or auto.
- You should also be aware that you do not need to lose your wallet or have anything tangible stolen, in order for someone to steal your identity.
- They may steal mail, including bank and credit card statements, pre-approved credit offers, new checks.
- Skilled identity thieves use a variety of ways to gain access to your personal information.
- 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.
- 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 the filing of a public records request.

## **The "Phishing" Scam**

It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

- Phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency.

The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond.

The messages direct you to a website that looks just like a legitimate organization's site, but it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

### **Social Engineering**

- The term "social engineering" is closely related to phishing.
  - **Social engineering** is the practice of obtaining confidential information from someone by trickery or manipulation
  - A social engineer relies heavily on human interaction
  - Social engineers exploit the natural tendency of a person to trust another human being

Social engineering can be done over the phone or in person.

### **How can you tell if you're a victim of Identity Theft?**

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from the three nationwide consumer reporting companies.

If you have lost any personal information – or if it has been stolen – you may want to check all your reports more frequently for the first year.

- Monitor the balances of your financial accounts.
- Look for unexplained charges or withdrawals.
- Other indications of identity theft can be:
  - failing to receive bills or other mail. This could mean an identity thief has submitted a change of address.
  - receiving credit cards for which you did not apply.
  - denial of credit for no apparent reason.

- receiving calls from debt collectors or companies about merchandise or services you didn't buy.
- The following two web sites have a wealth of information, and will assist you with questions or steps to take if you are a victim of identity theft:
- <http://www.myfloridalegal.com/identitytheft>
- <http://www.consumer.gov/idtheft/>

If I am a victim what should I do?

## Step One

### 1. Place a fraud alert on your credit reports, and review your credit reports.

- Fraud alerts can help prevent an identity thief from opening any more accounts in your name.
- Contact the toll-free fraud number of any of the three consumer reporting companies to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.
- The three major credit reporting bureaus
  - **Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241
  - **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013
  - **TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports.
- When you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- Check all information on the credit report like your SSN, address, name or initials, and employers. Make sure the information is correct.
- If you find fraudulent or inaccurate information, get it removed.
- Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

## Step Two

- Close the accounts that you know, or believe, have been tampered with or opened fraudulently.
  - Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents.
- *It's important to notify credit card companies and banks in writing.*
- Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.
- When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, or the last four digits of your SSN.
- If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions:
  - For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms.
  - write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit.
- If not, ask the representative to send you the company's fraud dispute forms.
- If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.
- Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts.
- This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

### **Proving You're a Victim**

- Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours.
- These documents also may contain information about the identity thief that is valuable to law enforcement.
- By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing.
- Be sure to ask the company representative where you should mail your request.
- Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents.

- You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

### **Step Three**

- File a report with your local law enforcement agency or the law enforcement department in the community where the identity theft took place.
  - Then, get a copy of the offense report or at the very least, the case number of the report. It can help you deal with creditors who need proof of the crime. If the law enforcement agency is reluctant to take your report, ask to file a "Information" report.

### **Step Four**

- File a complaint with the Federal Trade Commission.
  - By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

### **What else can I do?**

- **Flag your Florida Driver's License.**
  - At your request, the Fraud Section of the Department of Highway Safety and Motor Vehicles will place a flag on your driver's 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) 488-4760. You will be asked to submit your request in writing to:

Department of Highway Safety and Motor Vehicles  
DDL/BDI - Fraud Section, Room A327  
Neil Kirkman Building  
Tallahassee, FL 32399-0570

- **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 (FDLE) can provide a Compromised Identity Review (based on a fingerprint comparison of state criminal history files) to determine what, if any, criminal history belongs to you, and if any arrest records have been falsely associated with you as a result of someone using your identity.

- 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.

### **Preventing Identity Theft**

- Order and closely review copies of your credit report from each national credit reporting agency once a year.
- Equifax  
P.O. Box 740241  
Atlanta, GA 30374-0241  
To order your report: 1-800-685-1111  
To report fraud: 1-800-525-6285
- TransUnion  
Fraud Victim Assistance  
P.O. Box 6790  
Fullerton, CA 92634-6790  
To order your report: 1-800-888-4213  
To report fraud: 1-800-680-7289
- Experian  
P.O. Box 9532  
Allen, TX 75013  
To order your report: 1-888-EXPERIAN (397-3742)  
To report fraud: 1-888-EXPERIAN (397-3742)
- Empty your wallet of extra credit cards and IDs. Close all unused credit card or bank accounts
- 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.
- Remove your name from mailing lists for pre-approved credit lines by calling 1-888-5-OPTOUT (1-888-567-8688).

Never leave receipts at bank machines, bank counters, trash receptacles or unattended gasoline pumps.

- **Your Mail**
  1. Promptly remove mail from your mailbox after delivery.
  2. Deposit outgoing mail in post collection boxes or at your local post office.
  3. Contact your creditor or service provider if expected bills don't arrive.
  4. Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.

Be aware of Identity Theft and the problems it can cause. If you become a victim, act fast to reduce the damage this crime can cause.

Information provided by Detective D. Wood – PBSO Financial Crimes Unit