Identity Theft

Types of Identity Theft

Identity theft can enter into many areas of our lives. It involves any instance where a person uses someone else's identification documents or other identifiers in order to impersonate that person for whatever reason. According to the Federal Bureau of Investigation, it affects 900,000 new victims each year. More appropriately titled **identity fraud**, your identity might be stolen in order for someone to commit:

- **Financial fraud** - This type of identity theft includes bank fraud, credit card fraud, computer and telecommunications fraud, social program fraud, tax refund fraud, mail fraud, and several more. In fact, a total of 25 types of financial identity fraud are investigated by the United States Secret Service. While financial identity theft is the most prevalent (of the approximate 10,000 financial crime arrests that Secret Service agents made in 1997, 94 percent involved identity theft), it certainly isn't the only type. Other types of identity theft, however, usually involve a financial element as well -- typically to fund some sort of criminal enterprise.
- **Criminal activities** - This type of identity fraud involves taking on someone else's identity in order to commit a crime, enter a country, get special permits, hide one's own identity, or commit acts of terrorism. These criminal activities can include:
    - **Computer and cyber crimes**
    - **Organized crime**
    - **Drug trafficking**
    - **Alien smuggling**
    - **Money laundering**

Stealing Your Identity

Have you ever eaten at a restaurant, paid with a credit card, and forgotten to get your copy of the credit card receipt? Did you know that many of these receipts have your credit card number printed right there for anyone to see (and use)? And, if you've signed them, your signature is also right there for someone to carefully copy. This can lead to the most simple form of identity theft. With this bit of information, some unscrupulous person can be well on his way to making purchases either by phone or on the Internet using your credit card number. You won't know about it until you get your statement (a good reason why you should always study the charges on your credit card statements!). All they have to have, in most cases, is your mailing address, which can be looked up in a phone book or easily found on the Internet.

Credit card fraud is identity theft in its most simple and common form. It can be accomplished either through a scenario like the one we just mentioned, or it can happen when your pre-approved credit card offers fall into the wrong hands. All a person has to do is get these out of your mailbox (or trash can) and mail them in with a change of address request and start spending. Someone can even apply for a credit card in your name if they have the right information. You won't know a thing about it until the credit card company tracks you down and demands payment for the purchases "you" have a racked up.

With a person's name, social security number and date of birth, someone can get loans, access the person's existing bank accounts, open new bank accounts, lease or buy cars, get insurance, you name it. Think about the things you throw in the trash. Do you throw your pay stubs away once you've recorded the amount in your checkbook? Take a look at some of the information on that seemingly unimportant piece of paper:

- Your full name
- Your address
- Your social security number
- Your complete bank account number (if you have direct deposit)
- Your employer and its address
- Your rate of pay

Now, think about the types of information you have to provide in order to get a credit card or a loan or lease a car. There is very little additional information that is needed in order to get that loan. I recently got a home equity loan and did all but the final signing of the documents over the phone, and faxed all of my financial information

directly to the loan officer. It would not have been that difficult to "create" those documents using someone else's social security number, bank account numbers and other personal information. That's a scary thought! Imagine finding out that someone had gotten a mortgage in your name. Clearing that up with the bank and getting it off of your credit history would be quite a battle. You are left with the time-consuming task of repairing your credit and getting your finances back on track.

Accessing Your Personal Information

Your personal information can be found in many places. It can be:

- Dug out of trash cans and dumpsters, known as "dumpster diving"
- Memorized or copied by sales clerks and waiters
- Removed from your mailbox in the form of tax notices, financial account statements and other bills before you have a chance to get them or even know they are there
- Removed from your employer's files, either secretly or with the help of an inside accomplice
- Removed from your hospital records, usually with the help of an inside accomplice
- Removed from your financial lender's files
- Removed from your landlord's files
- Purchased (or found free) in online (or offline) databases
- Collected from "cloned" Web sites (Someone may recreate a legitimate merchant Web site in order capture your personal information and credit card information when you place an order.)
- Stolen from a merchant database through computer hacking (This is not as simple as other forms of theft.)
- Stolen through hacking into commercial Web sites or your personal computer and using software to mirror keystrokes to capture credit card account information
- Collected from "cloned" chat rooms that include links to outside Web sites that offer services or products (None of these are real merchants; your information is simply gathered so the criminals can make purchases elsewhere.)

Basically, anywhere you've provided that information can be a target. Often, employees who have access to the information are bribed or offered a cut of the profits in exchange for personal information about other employees. The more sophisticated the perpetrator, the more money is stolen and the more people scammed. Clerks can even put **skimmers** on the credit card machines that will record credit card information for later use. Temporary employees seem to be more frequently involved in identity theft scandals than permanent employees, simply because fewer background checks are done on them.

Public information

What about all of the publicly available information someone can access about you? Sources for this information include:

- Public records - These records that are open for public inspection include driver's license information, real estate records, business records, vehicle information, certain types of professional certifications and licensing information, and any other types of data collected by public entities.
- Information that is publicly available - This means non-government information that is found in newspapers, such as classified advertisements and reports, as well as phone book entries.
- Open-source information - This refers to information about you that may be found in periodicals and on Web sites.

While some information about your life is pretty well protected, such as medical, financial and academic records, your other identifying information (social security number, home address, etc) is not so protected. One scary statistic: According to the Federal Trade Commission (FTC), in 2000, 19 percent (as opposed to 13 percent in 2001) of all victims of identity theft who completed that section of the FTC identity theft complaint form had a personal relationship with the thief. In 2000, 10 percent of those thieves were family members!

How To Protect Yourself

Protecting yourself from identity theft takes proactive effort. You can't simply assume it's not going to happen to

you and go on about your life -- it can happen to anyone. It even happens to celebrities. Oprah Winfrey, Tiger Woods, Robert De Niro and Martha Stewart have all had their identities stolen. While you can't ever totally protect yourself from these thieves, you can at least make yourself less attractive as a victim by doing what you can to make it more difficult for them to access your information. Here are some things you can do to protect yourself:

- DON'T give out your Social Security number unless it is absolutely necessary. Many companies collect more information than they really need. Make sure that it's something they have to have and make sure they'll protect your privacy.
- DESTROY any unwanted credit card offers. This means rip, shred, burn, whatever you can do. These pre-approved offers come almost daily. If you don't want the three major credit bureaus to sell your name to these companies, you can "opt out" by either writing to the three major credit bureaus or by calling (888) 5OPTOUT (567-8688). This will remove your name, for two years, from mailing and telemarketing lists that come from TransUnion, Equifax, Experian, and INNOVIS. You can also write to the Direct Marketing Association's mail preference service to have your name removed from some mailing lists.
- DON'T put any other information besides your name and address on your checks, and keep a close watch on your checkbook both when you're writing checks and when it is lying around. Someone can memorize your name, address and phone number during the short time it takes you to write a check.
- SHRED (cross-cut) any sensitive documents before you throw them into the trash. This may seem like an extreme measure, but dumpster diving happens all the time and turns up a lot more personal information than you may realize.
- DON'T carry your Social Security card, passport, or birth certificate in your wallet or purse. Also, only carry as many credit cards as are absolutely necessary. It has also been suggested that you photocopy everything you carry in your wallet to make canceling things easier in the event that your wallet is stolen.

- REVIEW your credit report every year to make sure there haven't been any new credit cards or other accounts issued (to someone other than you) and to make sure there haven't been inquiries by people you haven't initiated business with. There are also services you can subscribe to that will alert you to any changes in your credit file.
- NEVER give out personal information on the phone to someone you don't know and who initiated the call. Often, scam artists phone unsuspecting victims pretending to be their financial services company and request information to be provided over the phone. Usually, the story is to "update records" or sell a product. Get their name, phone number and address, and then call them back at the number you have on file or that is printed on the statements you receive.
- REVIEW your monthly credit card statement each month to make sure there aren't any charges showing up that aren't yours. Also, make sure you *get* a monthly statement. If the statement is late, contact the credit card company. You never know when someone may have turned in a change-of-address form so they could make a few more weeks of purchases on your credit card without you noticing.
- DON'T mail bills or documents that contain personal data (like tax forms or checks) from your personal mail box. Take them directly to the post office or an official postal service mailbox. It's too easy for someone to take mail out of your mailbox on the street. From there, they can dip your checks in special chemicals to remove the ink and then rewrite them to themselves!
- If you're ever denied credit, FIND OUT WHY, especially if you haven't reviewed your credit report lately. This may be the first indication you get that someone has stolen your identity and is racking up charges in your name.
- REACT QUICKLY if a creditor or merchant calls you about charges you didn't make. This too may be the first notice you get that someone has stolen your identity. Get as much information from them as you can and investigate immediately.
- GUARD deposit slips as closely as you do checks. Not only do they have your name, address and account number printed on them, but they can also be used to withdraw money from your account. All a thief has to do is write a bad check, deposit it into your account and use the "less cash received" line to withdraw your money.

Identity Theft Insurance?

Some insurance companies offer identity theft insurance. While these policies don't cover everything, they certainly help out by covering a

portion of lost wages for time spent dealing with the theft, mailing and other costs associated with filing paperwork to correct the problem, loan re-application fees, phone charges and even some attorney fees.

These steps *can* help lessen your chances of becoming a victim of identity fraud, but nothing is a sure thing. The thing to remember is that documents you throw away often have all the information a thief needs to steel your identity and wreak havoc on your life.

Internet Transactions

The ease of shopping and comparing products and prices online has made it an attractive option for many shoppers. How can you make sure your transactions are safe and your credit card information going only where you intend it to? There are several ways to help ensure safe transactions on the Internet, and more are becoming possible all the time. Some of these include:

- Stored-value cards (cards that you can buy with specified, loaded dollar amounts)
- Smart cards (cards that can act as credit cards, debit cards and/or stored-value cards)
- Point-of-sale (POS) devices (like your PDA or mobile phone)
- Digital cash
- E-wallets
- Online payment services like PayPal

The most prevalent method for paying for the things you purchase online is still the credit card. The following list provides some tips on how to make sure your transaction is secure. For a more extensive explanation of encryption and Internet security, check out How Encryption Works.

- **Use the latest Internet browser.** The program that you use to surf the Internet is called a browser. This software has built-in encryption capabilities that scramble the information you send to a server. Using the most recent browser ensures that the data is protected using the latest encryption technology. This technology also uses a Secure Sockets Layer (SSL), which is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. The server receiving the data uses special "keys" to decode it. You can make sure you are on an SSL by checking the URL -- the http at the beginning of the address should have changed to **https**. Also, you should notice a small **lock icon** in the status bar at the bottom of your browser window.

- **Look for digital certificates** that authenticate the entity you are dealing with. Independent services like VeriSign will authenticate the identity of the Web site you are visiting. Web sites that use this service (usually those that sell items or services online) will have the VeriSign logo. By clicking on the logo, you can be assured that the site is legitimate, rather than a clone of the legitimate company set up to collect your personal and financial information.

- **Read the privacy policy**. The information you enter on the Web site should be kept confidential. Make sure you read the company's privacy policy to ensure that your personal information won't be sold to others. Services like Trust-E review a company's privacy policy (for a fee) and then allow the company to post the Trust-E logo if its privacy policy follows certain industry standards for consumer protection.
- **Only use one credit card** for all of your online purchases.
- **Never give out passwords or user ID information online unless you know who you are dealing with** and why they need it. Don't give it out to your Internet service provider if you get an e-mail requesting it. This is a relatively recent scam used to access your account and get your credit card number, along with whatever other personal information is there.
- **Keep records of all of your Internet transactions.** Watch your credit card statement for the charges and make sure they're accurate.

After you've made purchases online, check your e-mail. Merchants often send confirmation e-mails or other

communications about your order

If It Happens To You

What if you find out through a phone call from a creditor, a review of your credit report, or even a visit from the police, that your identity has been stolen. The **first** thing to do is report the crime to the police and get a copy of your police report or case number. Most credit card companies, banks, and others may ask you for it in order to make sure a crime has actually occurred.

You should then **immediately contact your credit card issuers**, close your existing accounts and get replacement cards with new account numbers. Make sure you request that the old account reflect that it was "closed at consumer's request" for credit report purposes. It is also smart to follow up your telephone conversation with letters to the credit card companies that summarize your request in writing.

Close any accounts the thief has opened in your name. If you open new accounts yourself, make sure you request that passwords be put on those accounts. As with any password, make sure you use something that is not obvious to others. Don't use your mother's maiden name, the last four digits of your social security number, or anything else that would be obvious.

Next, **call the fraud units of the three credit reporting bureaus** and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged with a "fraud alert." This usually means that someone can't set up a new account in your name without the creditor calling you at a phone number you specify. Verify with the credit bureau representative you speak with that this will happen, and provide them with the number at which you want to be reached. The down side of this is that you won't be able to get "instant credit" at department stores. This flag, also known as a "victim's statement," is the best way to prevent unauthorized accounts.

The Credit Bureaus

Equifax Credit Information Services - Consumer Fraud Div.
P.O. Box 105496
Atlanta, Georgia 30348-5496
Tel: (800) 997-2493
www.equifax.com

Experian
P.O. Box 2104
Allen, Texas 75013-2104
Tel: (888) EXPERIAN (397-3742)
www.experian.com

TransUnion Fraud Victim Assistance Dept.
P.O. Box 390
Springfield, PA 19064-0390
Tel: (800) 680-7289
www.transunion.com

Make sure to keep a log of all conversations with authorities and financial entities, and keep copies of any documentation you provide to them.

If your social security number has been used, notify the Social Security Administration's Office of Inspector General.

File a complaint with the Federal Trade Commission (FTC) by contacting the FTC's Consumer Response Center. The FTC is the federal clearinghouse for complaints by victims of identity theft. The FTC does not have the authority to bring criminal cases, but it does assist victims by providing information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to

other appropriate government agencies and private organizations for further action.

The FTC also has an online identity theft compliant form that can help them gather information about identity theft and lead to law enforcement actions. The form can be found here.

The Consumer Assistance Initiative (a part of the FTC) provides an Identity Theft Affidavit that is a single form that can be used to notify a number of companies and other groups of the theft of your identity.

Reporting to the FTC

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
Toll-free 877-FTC-HELP (382-4357)
On the Web: www.ftc.gov/ftc/complaint.htm
For consumer information:
www.ftc.gov/ftc/consumer.htm