

Identity Theft – Are you are Risk?

Chances are you think that *you* won't be affected by the nation's number one fast-growing crime. Think again. Identity theft is on the rise.

In 2005, 9.3 million Americans were victims of identity theft according to the Javelin Better Business Bureau survey. 68.2 percent of the cases involved thieves who obtained personal information off-line vs. only 11.6% obtained online. ID theft through lost or stolen identification, misappropriation by family and friends, and theft of paper mail are among the most common ways thieves gain access to your information.

Most people do not have a clue how to protect themselves.

For a moment, let's just examine what could happen in your life if you are targeted for this crime:

- Victims now spend an average of 600 hours recovering from identity theft over a period of years. This equals nearly \$16,000 in lost potential or realized income. Typical out-of-pocket expenses are \$1,500 on average.
- Even after a thief is stopped from using your information, sometimes up to as much as 10 years, victims still struggle with the impact of identity theft. That includes increased insurance or credit card fees, inability to find a job, higher interest rates, as well as continuing to battle collection agencies that refuse to clear records despite substantiating evidence of the crime. How stressful do you think this situation would be?
- The emotional impact on victims is likened to a violation similar to what victims of violent crime describe including rape, violent assault and battering. People feel dirty, ashamed, embarrassed and often are afraid to ask for help. Many have reported a split with a spouse of significant other as well as being unsupported by family members.

Most victims report a lack of responsiveness from those entities they turned to for help including police, collection agencies, credit issuers, utility companies and financial institutions. The average arrest rate for identity theft based on reported cases is 5%. **The message here is crystal clear – we have to fight identity theft ourselves!**

Exactly what are the different types of identity theft and how do identity thieves get access to your personal information?

Financial Identity Theft

This is the kind of identity theft most people think of first. Thieves hack into your computer at home or at the office and steal personal information. It accounts for about 28% of all identity theft happening today.

For example, thieves will:

- use your line of credit to make purchases
- use your credit cards to make purchase
- open up a mortgage using your name and social security number
- create a loan using your name and social security number
- file bankruptcy under your name
- open phone or utility accounts under your name
- attempt checking and/or savings fraud (accessing your accounts)
- attempt to use existing accounts to make purchases

Under the Fair Credit Billing Act, your liability in the case of unauthorized credit use is limited to \$50 per card. However, in order to take advantage of this protection, you must file a dispute letter within 60 days after the first bill containing the error was mailed to you. So what happens if the thief changes your address and you don't receive your bill? Guess what, *you are held financially liable*. In addition, the Electronic Fund Transfer Act has the same 60 day notification provision or your liability is unlimited. Not fair, but it's the reality.

Some credit card companies promote zero liability for these kinds of fraudulent transactions. However the reality is that there are exclusions including cards used by business purposes, ATM transactions, and certain PIN-based transactions, all transactions processed outside the card issuer's network, and cases where the card holder gave permission for someone else to use their card. You have to read your cardholder agreement carefully to find out the exact details.

Financial Identity Theft has significant impact on a person's life including: financial losses, inaccurate credit reports that can mean being denied a job, difficulty getting new lines of credit, trouble opening new accounts as well as higher costs for loans and insurance. The toll of this kind of financial loss can be significant as can be witnessed in a recent lawsuit filed by a plaintiff against Home Depot, Case #02CC13327 in Orange County Superior Court, where a judge awarded the plaintiff \$1 million in damages for identity theft.

Criminal Identity Theft

This is the second most common type of identity theft and most people aren't even aware of it.

In this case, a criminal uses your information during encounters with the police. For example, a thief who has your identifying information gets arrested for a crime and gives them your name and social security number. One day you

are driving along and get stopped for a traffic infraction. The cop runs your name through their database and finds out you just committed a bank robbery in another state. Suddenly you are being hauled off to jail for something you didn't even do!

Never mind how stressful and embarrassing this mistake could be, it can also lead to an erroneous criminal record, outstanding arrest warrants, and possible consequences such as being fired from your job for not disclosing a conviction and even get you thrown in jail. What if this happens on a Friday night and they toss you the local jail overnight? Do you have someone you can call that could bail you out? Can you afford this kind of mistake happen in your life?

The results of this kind of criminal identity theft could include a negative impact on future employment, loss of security clearance, lost jobs and higher insurance premiums. It is the most difficult type of ID theft to clear up and in some cases, almost impossible. Some victims have been reduced to carrying court documentation with them at all times to prove who they really are and not the actual criminal.

Social Security Identity Theft

If someone uses your social security number to get a job and they have a continuous work record, guess who gets to pay the tax bill? The answer is you. There are cases where someone's social security number was used a total of 37 times by different people. In the employment screening business, we see this happen every day.

Medical Identity Theft

This kind of ID theft involves someone using your health insurance for medical and/or hospital care. The result is a mixed up medical record that could result in potentially deadly consequences. For example, what would happen if someone used your identification and health insurance number and got an HIV test that proved positive? Now all of a sudden, that record is attached to your medical records and every time you see a healthcare person, they think you have aids. In addition, this can seriously impact your ability to get insurance and it can result in significantly higher insurance premiums.

A recent article in the November 2006 issues of Reader's Digest reported that "fraud is estimated to account for as much as ten percent of all health care costs ... including medical identity theft." "An insurance card is like a Visa card with a \$1 million spending limit," says Byron Hollis, national anti-fraud director of the Blue Cross and Blue Shield Association. The most frightening part of this article is the fact that organized crime rings are realizing how lucrative identity theft is and are adding a new dimension to the problem.

Driver's License Identity Theft

Our driver's license is the standard and most often used form of identification in United States. ID thieves are professionals at creating fake driver's licenses that are virtually impossible to detect. Having this form of picture ID opens the door to numerous other types of ID theft.

On October 28, 2006 in California, a worker at the Santa Ana DMV was arrested for her alleged role in an ID theft scheme that used applicant information to create fraudulent licenses. The indictment alleged that she used her position to sell fraudulent drivers licenses to co-schemers who paid between \$1,500 to \$5,000 for each fraudulent license. She allegedly obtained the identifications of victims from the DMV database and changed their address and identifiers to match the fraudulent purchaser who then had a new DMV photo taken.

What can You do to Protect Yourself?

The good news is there are many things you can do to protect yourself, but you must be proactive. This is a crime you cannot afford to wait to become of a victim of.

1. Order the Federal Trade Commission's free report on identity theft by visiting www.consumer.gov/idtheft or calling 877 382-4357
2. Get a copy of your own credit report and review it carefully for accuracy. Because of the new Fair and Accurate Credit Transactions Act (FACTA) you can get a free copy once a year at www.annualcreditreport.com
3. Be careful with your mail. Don't use an unsecured mailbox when mailing anything containing financial information. Drop off at the post office or in a post office collection box.
4. Guard your trash. Identity thieves will look for credit card receipts and applications, insurance forms, bank statements etc. Buy a shredder and use it regularly.
5. Use your Social Security Number only when absolutely necessary. Before you give your SS# to anyone, ask why it is needed and how it will be used, or shared with others and how the company protects your personal information.
6. Pay attention to billing cycles. If your bills don't arrive on time, follow up with your creditors. A missing statement can mean an ID thief has taken over your account and changed your billing address.

7. Be cautious with online purchases. Before purchasing anything on the internet, look for the icon of a lock in the lower right-hand corner of your browser windows. If it's there, you're dealing with a secure site. If not, you'll be safer finding another merchant.
8. Remove personal information from old computers. Files you think you have deleted from your computer may remain on your hard drive where hackers can easily access them. Use a wipe utility program to delete files with sensitive data.
9. Opt-out of receiving pre-approved credit cards offers in the mail by calling 888 5-OPT-OUT or going to www.optoutprescreen.com
10. Immediately sign up for an ID Theft Shield program which can not only monitor your credit and let you know when anything changes, but can also provide restoration after the fact. Don't wait on this one - [Click here now for more information](#)

For more information on how to protect yourself against identity theft, contact Cathy Taylor at cathy@apscreen.com or call 800 277-2733 ext 206.