

Identity Theft Prevention - Tips on Avoiding Disaster

Article by: Delia Galley

Identity theft is a malicious crime with serious implications. It can wreck havoc on your credit file, your ability to purchase a home in the future and interfere with potential job opportunities.

Approximately 246,000 cases of identity theft were filed between January, 2004 and December, 2004 – a staggering increase of 52% since 2002. Statistics of victimization by age group revealed that anyone from 18 to 65 is fair game. The breakdown by fraud subject were as follows:

- Credit card fraud – 28%
- Phone and utilities – 19%
- Bank fraud – 18%
- Employment – 13%
- Other (government documents, benefits, insurance, bankruptcy, etc) – 22%

So what is “Identity Theft”? Identity theft happens when, someone steals your personal information and commits fraud in your name. Examples include situations where your your name, social security number, home address and/or date of birth is used to open fraudulent credit card, telephone and utility accounts.

Perpetrators of identity theft should not be underestimated – some are clever and make a good living doing what they do. They have perfected ways to find your personal information and bleed you dry. Here are a few of their information pilfering methods:

- Obtaining your information while on the job or bribing someone who works in a certain organization to steal your information.
- Rummaging through your trash.
- Stealing your mail (including any bank and credit card statements, checks, tax information, etc.)
- “Skimming” your information by attaching devices to an ATM and stealing your information once you swipe your card and enter your PIN number.
- Hacking information databases.
- Stealing your wallet or purse.
- “Phishing” for information through phone calls or email under the guise of correcting erroneous information about your account.

Once they have acquired your information, they will use it in a number of ways to harm your personal finances. The FTC sites the following ways, in which they utilize your information:

- Open credit card accounts in your name and charge up the accounts. In order to avoid detection, they will file a change of address request with the local post office so that you do not receive your credit card bills. Out of sight – out of mind.
- Establish wireless and phone service accounts in your name.
- Buy an automobile in your name.
- Get an identification document such as a drivers license in your name.
- File a tax return in your name.
- Get a job in your name.
- Give your name to a police officer in an arrest and not show up to court.
- Open a bank account in your name and write bad checks.
- File for bankruptcy in your name to avoid paying for debts incurred in your name.

So what can you do? You cannot make yourself 100% theft-proof, when it comes to this crime but there signs to look for and ways to lessen the likelihood of becoming a victim of identity theft. Any of these signs should raise a red flag:

- Your credit report shows accounts that you are not familiar with. If you have not done so already, get your free credit report.
- You are not getting bills on time.
- You are receiving credit cards that you did not apply for.
- You are being denied credit.
- You are getting phone calls from debt collectors about an outstanding debt.

In addition, to monitoring red flags, the FTC recommends the following guidelines:

- Put passwords on all your credit card, utilities, bank, phone and wireless accounts. Avoid using the common passwords such as your mother’s maiden name, spouse’s name, date of birth, last four numbers of your social security number, phone number, etc. If a business uses one of these passwords, inquire about putting your own password on the account.
- Secure personal information, when you are having work done at your house or if you have roommates.
- Monitor your credit report every few months.

Do not give out personal information over the phone, email or internet unless you are sure of the other person's identity.

Remove your mail promptly.

Shred mail and trash with personal information .

Deposit outgoing mail in the post office mail box rather than an unsecured mailbox.

Do not carry your social security card with you.

Do not give out your social security number unless it is necessary. If your state and medical insurance programs use your SSN as identification – you may request that they use another number.

Pick up bank checks from the bank rather than through mail.

Be cautious when responding to promotions.

Run a virus protection software on your computer.

Don't open files that are from strangers.

Use a firewall program especially if you have DSL or a T-1 line.

Ensure that websites that you purchase products from or enter your personal information have SSL (secure socket layer) encryption. You will be able to tell by the "lock" on the bottom right-hand corner of your browser.

Delete personal information before disposing of your computer.

If you believe that you are a victim of identity, fight back.

The author is the owner of the information-rich website <http://www.poorcreditgenie.com> The website offers free advice on how to rebuild credit and manage debt. The site also features numerous articles and news stories on credit report, credit cards and bankruptcy.