

Identity Theft - "It Will Never Happen to Me"

Article by: James Hurst

When a criminal wrongfully obtains and uses another individual's personal data in a manner that involves fraud the act is referred to as identity theft.

Unfortunately, just about everyone knows someone who has been a victim. A good friend of mine recently became a victim. His case, (and 16 years of law enforcement experience), prompted me to write this article.

*(If you have senior citizens in your life, PLEASE have them read this and make sure that they understand. Seniors are targeted more than anyone).

The following are actual incidents involving identity theft:

The victim - A medical doctor practicing at his successful twenty-year-old office in central Georgia

The victim realized that several important pieces of mail that he had been expecting at his residence hadn't arrived yet. He had expected two of the items to arrive more than two weeks earlier. While attempting to telephone one of the companies whose package had not arrived, the victim received a telephone call from the sales manager at an automobile dealership located in central Alabama. The manager stated that he was calling to insure that all was well with the new automobile that the doctor had purchased several days earlier. The manager also stated that he would have contacted the doctor earlier, however, all of the telephone numbers listed on the doctor's purchase agreement were incorrect. The manager had located the victim's telephone number via the Internet. The victim had not purchased a new automobile in over eight years.

Further investigation revealed that a nineteen-year-old female from Nigeria who was legally in the United States on a student visa had stumbled across the victim's ad for his medical practice in the local Yellow Pages. After leaving his office one evening, the victim was followed home by the female subject. The next morning the subject walked into the local post office and filled out a change of address card, replacing the victim's home address with a post office box address that the female subject had purchased earlier in the week. All of the victim's personal mail would be sent to the P.O. box instead of to his residence. Within days the subject had received several items of mail addressed to the victim, including pre-approved credit card offers and other documents containing his social security number and date of birth. Within two months the subject had acquired two automobiles, a motorcycle, a house and multiple credit cards on the victim's credit. The subject was arrested and charged by the local authorities within three months of the initial criminal act, however, the victim's credit was completely destroyed.

A detective with the local police department who had befriended the victim during the investigative process stated that he telephoned the victim approximately two years after the subject had been arrested. The victim had been forced to close his medical practice and retire early due to the incident.

The victim - A regional sales manager traveling in Georgia

The victim fell asleep in his hotel room early one evening after a day filled with meetings and conference calls. After exiting the shower at approximately 7:00AM the next morning, the victim noticed that his wallet, briefcase and laptop computer were missing from the hotel room. Further investigation revealed that the victim had not secured the dead-bolt lock on the hotel room door the night before. Someone utilized a pass card-key to enter the victim's hotel room while he was sleeping and acquired the missing items.

Before the victim could finish speaking with the local police and report the incident to his corporate office, his corporate calling card number had been sold to several subjects at the local airport. During the six-month investigative process involving the victim's case along with several others, (all of which originated at the same hotel), the victim's personal information was utilized to open several credit card accounts and to receive several high interest cash loans.

The victim - A Georgia homeowner

The victim received a telephone call one morning from a major credit card company customer service representative who worked in the theft and fraud department. He was calling to inquire about the unusually high dollar amounts that had been charged on the victim's recently opened credit card account. The victim had not opened any credit card accounts in over five years. The representative then recommended that the victim call the local police and file a police report.

The victim was informed by a police department supervisor that for three days they had received several similar complaints from the same subdivision. Further investigation revealed that a male subject posing as a door-to-door solicitor had retrieved several envelopes containing pre-approved credit card promotions from mailboxes throughout the subdivision.

(I was an arresting officer involved with the following case)

The victims - Five major Atlanta area retail outlets

A search warrant was successfully obtained for an apartment located in Dekalb County. The two male residents were suspected of fraudulently ordering and receiving merchandise via the Internet from several Atlanta area retail locations. Upon entering the residence officers observed several expensive and obviously new items of merchandise located throughout the entire home, including:

- One twelve foot tall artificial Christmas tree containing hand-blown glass ornaments valued at \$3000.00
- Two forty inch projection television sets (one in the living room and one in the master bedroom)
- Unopened boxes in the dining room containing several sets of crystal and china valued at \$10,000.00
- Several unopened boxes located throughout the home containing computer equipment including monitors and PC towers valued at \$16,000.00

Investigative efforts revealed that the two subjects had obtained a Customer Credit Listing book from another individual who was at one time an employee of a credit reporting agency. The book was the size of a telephone book and contained thousands of listings in alphabetical order of Atlanta area credit customers by full name, last known mailing address, last known level of income and even social security and date of birth information.

The subjects had highlighted certain names, (prioritized by income level), and had utilized the victim's personal information to obtain several credit cards from the retail locations. The subjects would then utilize the credit cards to order merchandise.

Five retail outlets dispatched seven large panel trucks to retrieve their merchandise from the residence.

During the preliminary hearing for one of the subjects, officers knew that the subject was a major flight risk and were not pleased with the inadequate cash bond amount that the presiding judge had placed on the subject. An officer approached the bench and placed the large Customer Credit Listing book down in front of the judge, opened it to a book-marked page and pointed to the only line of highlighted text on the page. Both subjects were denied bail by the judge and were ordered to remain in jail until their trial date.

The judges' credit information was highlighted.

Identity thieves will utilize anyone's personal information in any way imaginable in order to profit financially, including but not limited to:

- Procuring monies from the victim's established accounts
- Obtaining credit cards from banks and retailers
- Applying for and receiving cash loans
- Financing the purchase of anything from automobiles to firearms (identity theft is a simple way for convicted felons to by-pass gun laws, including background checks and waiting periods)
- Establishing accounts with utility companies
- Obtaining a home loan or renting a home or apartment
- Obtaining employment
- Filing for bankruptcy (in the victim's name)

Methods utilized by identity thieves for obtaining a victim's personal information include but are not limited to:

- "Dumpster diving" or sifting through garbage at a victim's residence, place of business or any retail establishment, restaurant, night club, school, doctor's or dentist's office or any location where there may be copies of credit card receipts and other documentation containing personal information.
- Mail theft. Pre approved credit card offers and other mail material containing personal information are too often easily obtainable by identity thieves.
- The theft of proprietary data containing employee information from a company's human resource department or even a briefcase. If employee spreadsheets contain no date of birth or social security information, the names and telephone numbers are sold to telemarketing or other similar organizations for a profit.
- "Shoulder surfing." Identity thieves will even resort to sitting in their automobile in a parking lot and will utilize

binoculars to read a victim's PIN number at an ATM machine, or credit and/or calling card number at a payphone.

The following proactive steps will aid in the prevention of identity theft and fraud:

- Insure that new orders of personal checks are delivered to your bank, not your residence.
- Mail payments containing personal checks or money orders from a secure public mailbox or the post office, not your residential mailbox.
- When ordering a new or replacement credit card by mail, write down the name and the extension of the representative you speak with, as well as the expected arrival date for the card. If the card does not arrive by the expected date, telephone the representative immediately to inquire about the disposition of your credit card.
- If an expected mail item does not arrive on the expected date, or you notice a sudden decrease in your normal amount of delivered mail or no mail delivery at all, inquire regarding a possible fraudulent change of address at your local post office.
- Credit accounts that are not used regularly are attractive targets for identity thieves. Cancel accounts that have not been used in the last six months or longer, and destroy the credit cards.
- Purchase a crosscutting shredding machine. All pre-approved credit promotion documentation, check stubs, receipts and any documentation containing personal information should be shredded before disposal.
- Do not give out any personal information over the telephone. If a creditor "representative" calls and requests that you provide them with any personal information, suggest that the representative provide you with his or her telephone number and extension, and inform them that you will call them back momentarily with the information that they are requesting. If the telephone number does not match the toll free customer service number found on a monthly statement or on the back of the credit card issued to you by that creditor, call the actual customer service toll-free telephone number to inquire about the validity of the call.
- Order an unlisted home telephone number, or at a minimum request that your name be listed in the local telephone directory by an initial and last name, and request that your home address be removed from your listing.
- Do not participate in telemarketing promotions, and have your information removed from promotional lists. Telemarketing lists are bought and sold by companies and individuals on a daily basis. Once you have participated in a promotion over the telephone or by mail, (even if the promotion offers a free product or service), you will notice an immediate increase in the amount of promotional mail and in the number of telemarketing calls you receive. This greatly increases your risk of becoming an identity theft victim.
- Do not utilize your credit card on the Internet until you have read in full the company's privacy policy, and the company's web site provides a secured page that utilizes data encryption for credit card information. Many companies inform e-commerce customers in the fine print contained in their privacy policy that by purchasing their products via their web site, you agree to accept all of the terms and agreements contained in their privacy policy. Quite often those terms include the re-distribution of your personal information to other companies and creditors.
- Do not use a check or bank card on the Internet.
- Closely monitor all monthly bank and credit card account statements for fraudulent withdrawals and charges. Keep monthly statements for a minimum of one year.
- If your social security number is utilized as your drivers license number, have it changed. Do not have your social security number printed on personal checks.
- Order a copy of your credit report at least twice annually.
- Maintain one document, preferably in a fire proof security file or safe along with birth certificates, social security cards, your home inventory and other important documentation that contains the company name, account number, telephone number and the family member names on each open credit account. This will speed up the reporting process should you ever become an identity theft victim.

If you suspect that you or someone that you know has become a victim of identity theft, contact your local law enforcement agency immediately to obtain a police report. Early documentation is crucial. Send a copy of the following letter to the major credit reporting agencies:

//////////SAMPLE LETTER//////////

Re: (Your full legal name/no initials)
Social Security No: _____
Date of Birth: _____
Social Security No: _____

Date of Birth: _____
Spouses' Name: _____
Social Security No: _____
Date of Birth: _____

Dear _____,

In accordance with the Fair Credit Reporting Act, and for the protection of my credit information, I respectfully request that you take the following actions immediately:

- Provide me with my current credit report. (Enclosed find \$_____)
- Please add the following consumer alert to my credit report: "Do not issue credit without telephoning me first at the following number: _____." (This is an excellent deterrent for imposters!)
- Please remove my name from any and all market mailing and promotional lists. (Call 888-5OPTOUT to request information removal for all three credit-reporting agencies as well.)
- Please do not change my mailing address or telephone number without my prior authorization in writing.
- My current address is: _____
- My current telephone number at my office is: _____
- My current telephone number at my home is: _____

Enclosed you will find a copy of a current utility bill to confirm the accuracy of the above information.

Please do not provide my credit information to anyone without my prior authorization via telephone, fax, or in writing.

Please provide me with the necessary information so that I may set up a password to use for telephonic communications with your agency.

If I do not receive anything from you in writing within ten (10) business days from the date in which you signed the return receipt for this letter, I will assume that you unconditionally agree to insure that the above actions are taken.

Thank you in advance for your prompt attention to this matter.

Respectfully yours,

//////////SAMPLE LETTER//////////

J.C. Hurst is the IT/Internet Marketing Director
for The Ziegler Corporations.

You may contact J.C. at 800.726.0510 -or-
JCHurst@ZieglerSuperSystems.com

J.C. Hurst is the IT/Internet Marketing Director for The Ziegler Corporations.

You may contact J.C. at 800.726.0510 -or-
JCHurst@ZieglerSuperSystems.com