

Title:

My Identity Was Stolen Because Of Someone Else's Mistake

Word Count:

1086

Summary:

A true story about a financial organization losing my personal financial information - Identity Theft

Keywords:

Identity Theft, Bank Lost My Information, Computer Stolen, Mortgage Company Theft, Credit Report Monitoring

Article Body:

Giving Total Strangers Your Personal Information

How often would you say you trust total strangers with some of your most confidential information? I think I can answer this question for just about everyone. The answer is, nearly everyday. To illustrate this, I recently made a list of people or organizations that I have provided the following information to;

My social security number;

Birth date;

Tax Identification number;

Bank account numbers;

Medical information;

Checking account number

Just to name the top few forms of personal identification and confidential information. The list of those other than my self that have access to this information is made up of but not limited to the following;

My doctors office;

Banks that have issued me credit cards;

Computer stores (Best Buy, CompUSA, CDW, Circuit City);

Online music purchases through Wal-Mart (Formerly Liquid Audio);

Restaurant staff;

Hospitals;

Medical procedure companies (X-ray's, Ultra-sounds,....

And many more...

Be careful When Giving Your Credit Card Number Over The Phone

It seems like almost everyday someone is asking me for my social security number. I think most of us just get use to provided this information to various people and companies.

I recently ordered Italian food for dinner from one our favorite local restaurants. Every time I place an order the person taking the phone order repeats, out loud, my credit card information as I provide it to them over the phone. This includes the account number, my name, and expiration date. Every item that someone standing in line waiting to pick up their Pizza needs to purchase anything they wish online with my credit. I know why they do this, to make sure they are getting the right information. However, I finally told the person to please stop repeating this information out load. They were a little confused at first of why I made this request but after explaining to them my concern they said "Wow, I never really thought about that before". "How in the world can you remember all these things about computers?" Sometimes I wonder this myself.

To share another, more serious experience with you here is something that happened to me in just the last week or so. My wife walked into my office after returning from the mailbox and the first words out of her mouth was "Are you ready for this". When ever she utters that phrase I know it's not something pleasant. The letter she was holding was from our mortgage company. A company we have been doing business with for many years. It turns out that approximately 4 months ago a computer they were shipping from one office to another was stolen in transit. This computer contained my mortgage account number, balance, credit lines, social security number, business tax identification number, and much more.

When Should A Company Notify You That Your Personal Information Has Been Stolen?

The letter indicated that they were just notifying me now because law enforcement asked that they not contact any customers at the time the event took place, several months prior to receiving the letter, because it may impact the investigation. Well, they never found the computer or the thief so they decided to start notifying the affected customers. The letter also stated that the stolen computer had two levels of security and that they were not overly concerned that the thief would gain direct access to my information. Being in the computer security business, I thought to myself "Let's see, two levels of security, well that could be a password to logon to the computer, and Anti-Virus

software, or maybe they were using whole disk encryption and some sort of 1024bit pass-phrase to access the system". Quite frankly, chances are the system was not protected by anything as sophisticated as whole disk encryption. Of course they would not give me this information when I called. They did have a plan of action though to help me. You ready for this, a 1 year free subscription to Equifax (A Credit Reporting Agency) to alert me if someone is using my stolen information. That is about it. Oh, and they would assist me in the event that something showed up on my credit report. It's nice to see a multi-billion dollar company taking responsibility for the theft of my financial information. I know I'm not the only person that has these little "moments". My New Years resolution this year was to simplify my life. I'm not embarrassed to say that I've not made much progress yet but I am not going to give up. I am going to bring harmony to my life if it kills me in the process.

I share this information with you for several reasons. First, in the computer security business we are constantly talking about trusted and un-trusted computers and networks. Trusted networks are under a local administrators control and un-trusted networks are under the control of someone else. The same situation exists in real life. I keep safe my personal and private information as much as possible, but there are others that have this information as well. How well do they safe guard this information? I have no idea, but I am forced to trust them. Second, to show you that even security professionals, people like me who tend to be slightly more paranoid then the rest about our private information are just as much at risk as everyone else. Finally, to get you thinking about your confidential and private information, how many people have access to it, and why you need to take more than reasonable steps to keep it confidential?

Conclusion

Don't for one minute think that identity theft or fraud can't happen to you. In fact, I would say that it is not if but when it will happen, at least to one degree or another. Keep your private information confidential as much as possible. When people ask you for this information, ask them why they need it and how they plan to keep it secure. Also, keep track of who you give this information and for what reason. Finally, monitor your credit report frequently. Trans Union, Equifax, and Experian, the three largest credit reporting agencies, now offer inexpensive monthly services that can provide you with important information that could alert you to various forms of electronic fraud.

You may reprint or publish this article free of charge as long as the bylines are included.

Original URL (The Web version of the article)

[http://www.defendingthenet.com/NewsLetters/MyIdentityWasStolenBecauseOfSomeoneEl
sesMistake.htm](http://www.defendingthenet.com/NewsLetters/MyIdentityWasStolenBecauseOfSomeoneEl
sesMistake.htm)