Am I a Victim of Identity Theft?

Have you had something like this happen?

- You get a phone call or letter telling you that you have been approved or denied credit for something you never requested.
- You're no longer receiving your bank statements.
- You noticed that some of your mail seems to be missing.
- Your credit card statement includes charges for things you never bought.
- A collection agency calls you collecting on an account you never opened.
- You're served papers saying that your home is being sold for non-payment of a mortgage you never had.

If you notice anything like this, it's possible you've become a victim of identity theft.

If nothing is obviously wrong, how can you be sure you're not a victim?

The Facts

There is no doubt that daily we either read or hear of someone that is dealing with identity theft. The FTC says that the average victim of identity theft is unaware of the problem for 12 months.

A 2003 report from the FTC detailed the following:

The age groups most likely to experience identity theft were:

- 18-29 28%
- 30-39 25%
- 40-49 21%

33% of all identity theft crimes reported delt with credit card fraud. With 19% being new accounts and 12% dealing with existing accounts.

21% of all identity theft crimes delt with phone or Utilities fraud. With 10% being new wireless service, 5% being new phone services, and 4% being new utilities.

17% delt with bank fraud, with 8% being exisiting accounts, 5% being electronic funds transfer and 4% being new accounts.

11% delt with employment related fraud - that is applying for a job using your information.

While there were other situations, such as applying for government benefits, fraudulent tax returns, forged Social Security cards, and real estate loan frauds - these situations represented a very small percentage.

How Does It Occur
Identity theft occurs in any number of ways.

It may occur due to deception, like over the internet were someone protrays to be someone they are not (aka phishing).

It can occur due to you losing your purse with important documents inside.
It can occur due to trash diving, when someone rumages through your trash for personal information.

Sometimes it's an internal breach of security within a business, when personal information is released.

But most likely, it is someone you know.

In our many years of assisting consumers with various problems, identity theft by a close friend or family member occurred the most - usually it is siblings. Identity theft by a total stranger didn't even come a close second. Regretfully, the majority of reports you hear about are those that occur with a total stranger.

How to Protect Yourself

The free flow of information and computers have cause a real problem with personal privacy. But there are steps you can control to minimize this.

1) Social Security Number - Your social security number has become a national identity number. This number is ONLY required by your employer or banks for the purposes of withholding taxes PERIOD! Technically, they should be the only one's requesting this information from you.

It's strange but around 1960, the FTC warned the credit bureaus about using social security numbers for the purpose of identification. Yet, today it seems that this number is required for credit too.

We are continually bombarded with requests for this number, from health insurance to dentist offices. They all want your social security number.

Both drivers licenses, schools, and courthouses have been warned to move away from social security numbers. This blatent publication of this personal number on licenses, school cards and public record information has resulted in untold problems.

However, we believe that even more groups need to move away from using this number - they are credit bureaus and insurance agencies.

So What Can We Do?

First try to refuse it. You'd be amazed at the number of people that say, well we just wanted it for our records.

If they say they require it. Then ask - what is it to be used for? If you don't like the response consider going somewhere else. We know several who even go so far as making up numbers. Like we said above, this number is only to be used for taxes PERIOD.

Second, review your wallet for your social security number. If you should find it - ask yourself if that item can be left at home. If you should find it on your insurance card - you may want to consider taking a permanent market and blacking it out or blacking out portions of it. If you find it on your check - remove it when you reorder.

2. Personal Information - We continually provide personal information. We give our name and address and phone number to anyone that needs to contact us. That information is published in numerous areas, from the phone book to internet white pages. We provide it when we order items or when we set-up a credit account. It is held by every business that we have ever delt with.

So What Can We Do?

Some individuals we know have opened post office boxes for the purpose of preserving their privacy. This is the address that they provide to most businesses. While this can certainly help, for most this is too expensive or inconvenient.

Other's may want to OPT-Out of all this personal sharing. For more information on Opting-Out Click Here.

3. Financial Information - With credit card fraud being the number one problem area for identity fraud - there is no question that this is a concern. The internet makes it ease to order items your need. While sitting in front of a computer it's easy to quickly answer personal and private questions to emails and hit send before you really think it over.

So What Can We Do?

First - Don't carry around every credit card that your own. Most businesses can look up your account without your card. Some people have suggested writing "Ask For My ID" on the card. Regretfully, harried store clerks may overlook the statement or they don't know how to carefully check the ID.

Second - Don't respond to e-mails that ask you to confirm personal and private information. See our section on Fraud Alerts.

Third - Try to order on-line from businesses that you know and trust. You also may want to consider setting up a seperate checking account for Pay Pal where you deposit only the money you need for your on-line purchases. With on-line banking it is easy to transfer money from on account to another. This way no one has your credit card number and you can limit your exposure because no one has your active checking account number.

Touted Solutions from the Internet that Don't Work

Free On-Line Credit Reports - They're every where, and everyone is telling you to check your credit report often. We say DON'T USE them. If you read their privacy statements (yes, some have multiple) and you know the lingo, you will see that they are striping you of all your rights granted under the FCRA and they are going to sell your most personal information to whoever will buy it. No one can really determine who some of these businesses are. But these credit reports cost them money - they buy them from the CRA's themselves. The only way they make money is buy selling your information. They are considered "resellers" by the FCRA, and the FCRA says that "resellers" do NOT have to comply with the rules. If you want to take advantage of the new law that allows you to see your credit report annually, see related articles below. There you are given a number that you can call, rather than using the 'On-line' service.

Credit Monitoring - While there maybe a few people who have been helped by this type of services - we find it expensive and ineffective. While they will notify you when something adverse is placed on your file - by then it is too late. When you order them, they immediately try to upsell you into a more expensive package. And then when you try to cancel, the pressure is really on. This service doesn't stop Identity Theft.

MisInformation vs ID Theft

You may of recently received your credit report, on there you see another name - not yours. You may see another spouse - not yours. You may even see former addresses & trade lines & social security numbers that are not yours.

The first tendancy is to scream ID Theft. However, before you hit the panic button, here is something to understand.

Many times, especially if you see another Social Security Number on your file, most likely the national CRA's have accidently merged your credit report with another innocent individual. Common names like Smith, Nelson, etc. who live nearby, or generational information like Junior, Senior, etc. can result in the CRA's accidently putting the two files together.

What also can occur is that an individual, with the same name, may have left town without paying a bill. Creditors, in an attempt to find the person, may accidently find your address instead. This process of skip-tracing can result in that individual's bill being reported onto your credit file.

Neither of these situations are identity theft, they are mistakes caused by individuals or machines. However, it is difficult, sometimes to determine what exactly occurred.

So What Can We Do?

If your name ends in Jr, Sr, III, etc., then you most likely know the other individual. Contact the CRA via written letter, explain the situation, identify which are your bills, addresses, and SSN that belongs to you. You may want to call your relative and tell them what is occurring so that they too can contact the CRA.

If you have a common name, like Smith, then you may not know the other individual at all. You most likely will see a former address that you never lived at, or a SSN you never used. Contact the CRA's via written letter, give them as much information as possible, identify which are your bills, addresses, and SSN that belongs to you..

If there is only one tradeline that appears on your credit report that is not yours, contact the business that reported the information to the CRA directly. As information about the account, former addresses, date of services, etc. Some may require you to submit this information to them in writing, some may request addditional information from you. It may seem like a BIG inconvenience, but it really is the easiest and quickest way to get something like this resolved.

However, if the above problems seem to be re-occurring, then you may want to follow the procedures on "What to do if you're a Victim."

Our List & What to do:

- You get a phone call or letter telling you that you have been approved or denied credit for something you never requested.

- This is true identity theft - immediately inform the creditor and file a police report,

- You're no longer receiving your bank statements.

- Call the bank immediate, find out what happened. If they had received a change of address that you hadn't sent to them, you need to act quickly. Freeze all of your accounts, coordinate with the bank on outstanding checks & amounts. If the thevies get to your money, you may not get it back. Contact other financial institutions, IRA's, pensions, insurance policies, etc. Don't for get accounts you sat up for your children. These funds are seldom recovered & urgency is critical. Then follow the 'Victim' procedures below.

- You noticed that some of your mail seems to be missing.

- See our comments above regarding missing bank statements.

- Your credit card statement includes charges for things you never bought.

- This is usually NOT ID theft. This is credit card fraud. You're liability is limited to $50. Most banks wave this fee for good customers. Merely, notify the bank, coordinate with them on possibly closing the account. You may ask to continue using your credit card until the new one comes in. Sometimes getting a replaced card can take two weeks.

- A collection agency calls you collecting on an account you never opened.

- This may or may not be identity theft. When they call talk to them, ignoring a collection agency is never a good idea. Get information to help you determine what to do. Explain your situation.

- You're served papers saying that your home is being sold for non-payment of a mortgage you never had.

- This may be the most vicious form of identity theft. Individuals with no mortgage on their home are most susceptible to this type of fraud. However, you are protected here too. Follow the 'Victim' procedures below & contact the business that served you the papers.

What to do if You're a Victim

First, Contact your local Police - Most police departments have been trained on how to handle identity theft situations. It is critical that you get a copy of the police report. Remember, do not file a police report merely to get out of paying your bills - filing a false police report in most states is a felony.

Second, Contact the other Victims - these are the businesses that have been defrauded. You do not want them pursuing you, so you need to send them a copy of the police report as soon as you can.

Third, Contact the 3 national bureaus - Call TransUnion, Equifax, and Experian. In this situation, you are elligable for a free credit report. You can also place a "Fraud" Alert onto your credit file. But we want to warn you, that if you place a fraud alert there whill be additional situations that occur. Instant credit will be no more (that can be good or bad). You will also be required to prove who you are when dealing with businesses. Just be aware of these potential inconveniences.

Fourth, Review Your Credit Report - pay close attention to addresses and tradelines that you do not recognize. A very important section of your credit report that is many times overlooked is the inquiry area. This is usually broken down into three sections: Business that pulled your report for the purposes of establishing new credit lines, businesses that have marketed firm credit offers to you, and businesses that have reviewed your account - these are businesses where you already have an account established. Look closely at the names here. Do you recognize them? What about the data of the inquiry - were you shopping that day? Do you have open and current accounts with them? If you don't recognize something immediately begin the dispute process. To see our article on "Your Rights regarding Disputes" - Click Here.

Fifth - Call the FTC's Identity Theft Hotline 877-438-4338

If you should have any questions or problems, please post them on our "Community Forum."

For More information on Identity Theft

2003 Privacy Rights Clearinghouse Survey
FTC's 2003 report on Identity Theft
FTC's ID Theft Affidavit - This is not a substitute for a police report, but it details alot of specific questions you will want to ask yourself. It also provides a good way of tracking each occurance.

If you have other questions, please pose them here.

Written by Guest on 2005-05-24 This site is very informative, Thanks much!

{moscomment}