

## From the TechnoManor

This week I digress. Let's talk a little bit about *identity theft*. I haven't received a direct question, but people have asked my opinion on this topic. This isn't exactly a computer question, yet computers are often involved.

Have you gotten a letter beginning something like the following:

*"Dear Sir or Madam:*

*BNY Mellon Shareowner Services provides .... On February 27, 2008, our archive services vendor notified us that they could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility. The missing tapes contained certain personal information, such as your name, address, Social Security number, bank account number and/or shareowner account information that we maintain in providing these services...."*

Or you may have seen a headline like the following...

*U.S. Indicts 11 in Global Credit-Card Scheme  
(The Wall Street Journal, August 6, 2008)*

These are examples of the growing problem of identity theft. That is, someone - without your knowledge - has stolen a piece of your strategic information: your Social Security Number, driver's license number, bank account number(s), credit card number(s), or other information

And they are using your information to obtain money, buy stuff, or to masquerade as you.

This hasn't happened to me (yet). However, this is what I would do if I learned my identity had been stolen.

First, stay calm, but act with diligence. Now is not the time to get wigged out, pointing fingers, guessing who might be the culprit. Besides, after you follow through with *Things You Can Do*, you will have a better idea of what has happened and its implications.

Second, by the time you learn your identity has been stolen, it is too late. Your information has most likely been used. So, let's properly frame what you're doing next: You are playing cleanup.

### Things You Can Do

- Log your actions. Tracking stuff down can quickly get confusing. Record the date, what you did, what organization you contacted, who you spoke to, and the results. You can refer back to this log to give you some sense of balance as you work through the cleanup.

- Contact the company that notified you of the identity theft. They may be able to give you additional information that was not in the initial notification. This may include any accounts affected by the breach.
- Create a list of account names and numbers impacted by the theft.
- File a police report. This may be necessary for creditors who want proof of the crime.
- Monitor your statements. Look for charges or entries that you didn't make or that seem odd. This may also be the time to sign-up and use your financial institution's Web-based tool for managing your account. This will allow you to check for rogue transactions before you receive your statement in the mail.
- Contact the account-holders. Tell them of the possible identity theft and when you believe it occurred. Ask them what is their procedure for dealing with such a theft. Be sure to record this in your log
- Enroll in notification services. Some credit card issuers offer a service to contact you if they detect suspicious transactions (e.g., unusual purchase items, large purchase amounts, or purchases from a foreign country)
- Contact credit reporting agencies and place a *fraud alert* on your credit report. Following are the three major credit reporting agencies:

Equifax  
1-800-525-6285  
**[www.equifax.com](http://www.equifax.com)**

Experian  
1-800-EXPERIAN (397-3742)  
**[www.experian.com](http://www.experian.com)**

TransUnion  
1-800-680-7289  
**[www.transunion.com](http://www.transunion.com)**

- Learn your rights under state and federal laws, and any resources available to you. The following Web sites are good starting points:

Texas State Web site for identity theft:  
**[www.texasfightsidtheft.gov](http://www.texasfightsidtheft.gov)**

Federal Trade Commission Web site for Identity Theft:  
**[www.ftc.gov/bcp/edu/microsites/idtheft/index.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html)**

Federal Trade Commission Web site with links to federal and state laws establishing your rights related to identity theft  
**[www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/laws.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/laws.html)**

- Cancel the affected accounts. This is a last resort step, but one that may be needed.

How will you know if you're successful in your cleanup? Basically, time has passed and nothing unusual has occurred. In fact, by the time you were initially notified, chances are you already experienced some unwanted activity in your account *if it was going to happen*. Like bread out of the oven, information is most valuable when it is fresh. The longer it is unused, the more likely it will change (like you'll close that account).


Companies that notify you of identify theft often don't figure out a theft occurred for weeks, or months after it happened. It then takes more time for them to determine who to notify and how. Allow a few more days for the letter to be delivered. So, when you learn of the theft, you may already have been impacted.

(Side Note: The letter I reference above bears out this time delay. The theft occurred on 2/27/2008, yet the notification letter was dated 6/17/2008...nearly four months after the theft.)

Ok, so what if you've been lucky so far. Is there anything you can do to reduce your risk of identity theft (Note: I didn't say *prevent*)?

#### Here are Things You Can Do

- Shred that paper! When you're finished with a statement, report, or anything bearing your name and a number, put it through a paper shredder (unless you're like me who "pack rats" all financial information). This prevents "dumpster diving" which is a source of identity theft.
- Monitor your statements. Look for charges or entries that you didn't make or that seem odd. Have you received your statements on time lately? This can be an early-warning clue that someone may have already stolen an account number and changed the mailing address. This may also be the time to sign-up and use your financial institution's Web-based tool for managing your account. This will allow you to check for rogue transactions before you receive your statement in the mail.
- On the computer: make sure your anti-virus software, anti-spyware software, firewall, and computer updates are turned on and current. This will help prevent unwanted software from sneaking onto your computer to steal account numbers and passwords.
- On the computer (#2): Never, never, never, click on links in e-mail that purport to be from a bank, the federal government, or other institution. These are fraudulent (known as *phishing*). Only initiate a session by going to a known Web site (something printed and verifiable in a statement).
- On the computer (#3): If you conduct online banking or purchase things through the Web, only go to known Web sites. When you're about to

enter sensitive information, always look for a little lock icon () near the top or bottom of your Web browser. This lock indicates that it is a secure session and information exchanged is encrypted. It also means the Web site you're going to has purchased an electronic certificate which verifies their identity.

- On the telephone: Do not give out vital information to someone who calls you. If it sounds legitimate, get their name and organization – but not their number. Call an official number for this organization (from the phone directory or a statement), and ask for the person. Then give your vital information.
- Question Authority: Why does someone need your driver's license or Social Security Number? Always question any request. Many times, these numbers are used to simplify record keeping – not because they're required by law. Lax record keeping is another source of identity theft. If the answer sounds fishy, the request probably is, too.

Sorry to be a little long-winded on this...and yet I barely scratched the surface. May you never be faced with having your identity stolen. If it happens, I hope this article gives you the tools and grounding to survive it.

As always...got a computer, e-mail, Web, or related question? Cobble together an email message and send it to me at:

frenchygrey@gmail.com

I'll attempt to answer one each week in *The Link*. If you don't send me questions, I have to shake my Magic "8" Ball for ideas!

Dave Gillen