

## **Tech Talk**

### **Identity Theft ... Are You Who You Think You Are???** **Are You Sure???**

**By Irene Morrill, CPCU, CIC, ARM, CRM, LIA, CPIW**  
Vice President of Technical Affairs



137 Pennsylvania  
Avenue  
Framingham, MA  
01701  
(800) 972-9312 -  
(508) 628-5452

July 2005

### **What's the big deal ...**

Haven't we all seen those commercials on TV where a big burly guy is sitting there talking with a Fran Drescher "nanny-like" voice detailing all the cutesy little things "she" charged on this guy's credit card. The identity theft commercials are some of my favorite commercials ... if one can really have a favorite. They always make me laugh. However, after doing some research ... identity theft is NO laughing matter, for sure!

In January 2005 the Better Business Bureau released a report stating that 9.3 million Americans were subject to identify fraud in the preceding 12 months! Over 27 million Americans have been victim to identity theft in the last 5 years. Even though there certainly are security issues inherent in those who use the Internet, over 68% of information obtained in the identity theft claims was from information obtained OFF line!

A 2003 study by the Identity Theft Resource Center (ITRC) of 173 victims provided the following information:

The leading uses of the victim's personal information was to:

- open NEW credit accounts in victim's name
- make charges on existing credit card accounts of victim
- purchase new cellular phone service
- purchase new cable TV or energy utility account
- make charges over the Internet for goods/services
- take over victim's existing checking account via theft or check washing
- open a NEW checking or savings account
- create checks using victim's name/address with false account info
- obtain personal loan
- obtain auto loan

### **How did victim learn of identity theft?**

According to this study over 85% of victims learned of their identity theft in a belittling/denigrating manner. Some of the revelations were by:

1. creditor demanded payment on a late bill
2. debt collection agency contacted victim for unpaid bills
3. victim's mail service was disrupted
4. victim was denied credit or a loan
5. victim not allowed to open a bank account
6. IRS notified victim

Those that were "lucky" learned of the identity theft by:

1. Credit card company called regarding unusual credit activity
2. Victim noticed funds missing from bank account
3. One of victim's creditors called to ask if he had moved
4. Victim notices something unusual on his/her credit report
5. Victim received credit cards that he/she never ordered

### **What does identity theft "cost" the victim?**

The IRTC study portrays the costs as:

1. Time .... The average amount of "man-hours" that the victim had to devote to clearing his/her credit history was 607 hours! In a 2000 study, the average amount of man-hours spent to clear credit history was only 175. This is an increase of 247%.
2. Expenses ...The average amount of loss in these man-hours to clear one's credit was about \$17,500 which includes out-of-pocket expenses as well as lost wages. The 2000 study showed the average cost was about \$800 and only out-of-pocket expenses. This is an 85% increase in the cost to clear one's credit issues!

Expenses include the cost of certified mail receipts which are REQUIRED in many situations, notarizing fees, telephone calls, court documents, travel expenses, photocopying, court transcript purchases, police reports, fingerprinting, etc. Over 20% of the victims have increased medical expenses due to stress resulting from the emotional impact of the identity fraud.

(Another survey performed by Javelin Strategy and Research found that the mean cost was over \$6,000 and \$600 or so of it was "out-of-pocket" expenses by online "phishing". The mean loss was over \$15,000 when identity theft loss was generated by family and friends and over \$9,000 when originating from the theft of paper mail. The mean time for resolving the identity theft was a mere 30+ hours!)

### **Are YOU at risk for identity theft?**

Both the Privacy Rights Clearing house website

<http://www.privacyrights.org/fs/fs17-it.htm> and the Identity Theft Resource Center website <http://www.idtheftcenter.org/index.shtml> contain an "identity theft IQ test." I FLUNKED!

### **Some of the questions asked in the survey...**

- Do you receive offers of pre-approved credit every week?
- Do you SHRED such offerings?
- Do you have a PO Box or a locked, secured mailbox?
- Do you provide your SSN whenever asked, without asking question as to how that information will be safeguarded?

### **Try this survey at either of those sites ... to see how "safe" YOU really are ...**

Just how DO those hoodlums get the personal information necessary for identity theft? Some of the more prevalent modes of identity theft were:

1. Steal/hack/con information from businesses or its employees
2. Steal victim's mail including bank and credit card statements or offers for new credit cards, new checks victim ordered, tax information
3. Rummage through victim's trash, trash of businesses or public trash dumps (This is affectionately referred to as dumpster diving).
4. Steal victim's credit/debit card information by
  - a) accessing their employer's files where victim information kept
  - b) using data storage devices attached to ATM machines which "skims" debit card information for future illegal use
  - c) taking victim's wallet or purse
5. Complete a change of address form to divert victim's mail to another location
6. Elicit personal information from victim through email or phone by posing as a legitimate business and claiming that there is a problem with victim's account. This is "phishing" online and "pretexting" by phone.
7. Using computer viruses, spyware or other software that logs computer keystrokes or otherwise allows the hacker to steal victim's personal information

### **What do you do when your information has been stolen/accessed?**

All of the identity theft websites that I visited described four basic steps to resolving one's identity theft.

1. Contact your credit card companies and banks and other creditors where your accounts could be compromised and close them. Use the ID Theft

affidavit that was created with the auspices of the Federal Trade Commission and can be accessed at:

<http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

2. Place a FRAUD ALERT with the Major credit bureaus. This then requires any creditors to contact you before a new account can be opened. You only have to contact one of the three bureaus as whoever is contacted is obligated to tell the other two. Once you have issued a FRAUD ALERT all three companies must send you a free credit report.

Equifax at 1-800-525-6285

Experian at 1-888-397-3742

TransUnion at 1-800-680-7289

An INITIAL FRAUD ALERT lasts 90 days and is appropriate if you have lost your wallet or otherwise THINK that your credit could be compromised.

An EXTENDED FRAUD ALERT would last for seven years and is appropriate when you have actually been a victim of identity fraud.

3. File a report with your local police or the police in the community where the identity theft took place.
4. File a complaint with the Federal Trade Commission. (This can be done online at <http://www.consumer.gov/idtheft/> and the particular address for the complaint form is [https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z\\_ORG\\_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03))

The FTC website provides GREAT information on how to compile your report when you are actually a victim of identity theft. The key is DOCUMENT, DOCUMENT, DOCUMENT ... and certainly, as insurance professionals, we can understand the necessity of proving WHO, WHAT and WHEN you talked to someone.

It is the running around and documentation that could create BIG BUCKS out of pocket and loss of wages for the victim depending on how many accounts have been created/affected and how long the identity theft perpetrator(s) had been running rampant. Much time, effort and expense can be involved when trying to fix one's credit or prove that YOU never CREATED that account and YOU are not in "arrears" for something that YOU didn't authorize in the first place!

### **PREVENTION is the KEY to keeping identity theft from victimizing YOU ...**

Again, an insurance professional can certainly understand the validity of "safe

procedures."

1. SHRED papers with confidential information ( I have now moved my paper shredder next to the waste basket!!!)
2. NEVER carry your social security number and don't carry all your credit cards with you (This contains a loss if your wallet/purse is stolen).
3. Deposit outgoing mail in an "official mail receptacle." Don't leave it in your mailbox with the red flag up for the "post person" to get! (A "special thank" to you "helpful" class participants who earlier this year suggested that I leave my mail to be picked up in my personal mailbox if I couldn't find an official mailbox .....)
4. Don't give out personal information on the phone, email or by mail. Thieves "phish" by email ... saying there is a problem with your account and that you need to furnish certain pieces of info. either by mail or at a website that is embedded in the email ... this is a fictitious website! If someone solicits over the phone don't give out credit card or other personal information to someone that you don't know ... no matter how good the "deal" sounds!!!! (What was that PT Barnum said ... there's a WHAT born every minute?)
5. Check your banking statement EVERY month so you can identify unauthorized transactions. And, actually the articles point to online checking being SAFER than "paper" checking! (Per the Electronic Fund Transfer Act, if you report your card lost or stolen within 2 days, your losses are limited to \$50. If you report the stolen card after 2 days but within 60 days of your statement showing unauthorized transfers, you are limited to a \$500 loss. If you wait MORE than 60 days, you could lose ALL your money ... so look at your statements!!!!)
6. Check your credit card statement each month to make sure that the transactions are YOURS! (We are not responsible for more than \$50 per card ... but multiple cards can add up. It is the paperwork to remove these unauthorized charges that is the hassle!)
7. Get your credit report EVERY YEAR ... and a recent amendment to the Fair Credit Reporting Act REQUIRES the major nationwide consumer reporting companies, as previously listed, provide you with a FREE copy of your credit report EVERY YEAR upon your request. (This requirement is effective September 1st 2005 for those of us who live in the Northeast.) (BEFORE you get a loan or credit card declined ... look at your credit history yearly to see unwarranted activity ... nip it in the bud before it becomes a problem.)
8. When choosing a PIN number for credit cards, ATM cards or a password for various websites ... NEVER choose
  - a. your mother's maiden name
  - b. last 4 digits of your SSN

- c. birthdates of ANY family members
  - d. pet names
  - e. hometown baseball team
  - f. the word "password"
  - g. chronological number patterns
- Always try to choose something that is HARD to guess ... just remember it ... it is best is one mixes letters, symbols and numbers.
9. Don't have your SSN or phone number on your checks ... and DON'T have your checks delivered to your home ... PICK THEM UP AT THE BANK.
  10. Stop receiving pre-approved credit offers by calling 1-888-567-8688 or going to <https://www.optoutprescreen.com/> (Opting out of pre-approved credit offerings will certainly make less junk mail ... and less to SHRED!!!!)
  11. CONSIDER BUYING IDENTITY FRAUD INSURANCE  
ISO created an Identity Fraud Expense Endorsement HO 04 55 and many companies offer it ... or something like it. ISO's version has a \$15,000 limit for an "insured's" "EXPENSES" arising out of "identity fraud."

**Identity fraud is defined as:**

"Identity fraud" means the act of knowingly transferring or using, without lawful authority, a means of identification of an "insured" with the intent to commit, or to aid or abet another to commit, any unlawful activity that constitutes a violation of federal law or a felony under any applicable state or local law. Which is what was described in the Identity Theft Resource Survey as the uses to which the victim's personal information was put!

Which is what was described in the Identity Theft Resource Survey as the uses to which the victim's personal information was put!

**The covered "expenses" are defined as:**

"Expenses" means:

- a. Costs for notarizing affidavits or similar documents attesting to fraud required by financial institutions or similar credit grantors or credit agencies.
- b. Costs for certified mail to law enforcement agencies, credit agencies, financial institutions or similar credit grantors.
- c. Lost income resulting from time taken off work to complete fraud affidavits, meet with or talk to law enforcement agencies, credit agencies and/or legal counsel, up to a maximum payment of \$200 per day. Total

payment for lost income is not to exceed \$5,000.

d. Loan application fees for re-applying for a loan or loans when the original application is rejected solely because the lender received incorrect credit information.

e. Reasonable attorney fees incurred as a result of "identity fraud" to:

- (1) Defend lawsuits brought against an "insured" by merchants, financial institutions or their collection agencies;
- (2) Remove any criminal or civil judgments wrongly entered against an "insured"; and
- (3) Challenge the accuracy or completeness of any information in a consumer credit report.

f. Charges incurred for long distance telephone calls to merchants, law enforcement agencies, financial institutions or similar credit grantors, or credit agencies to report or discuss an actual "identity fraud."

All of the out-of-pocket expenses seemed to be covered such as notarizing fees necessary to confirm that YOU are the "TRUE individual" and certified mail fees to PROVE that you sent the information in your quest to document.

The endorsement also provides for LOST WAGES due to the time off from work necessary to straighten out your credit. This could include travel time to other states where your credit has been maligned by those crooks! Telephone charges are covered where you are on hold "forever" or just plain talking up a blue streak trying to obtain or give information to alleviate your identity theft crises!!!!

And, last not but least, attorney's fees which we hope we won't need because legal fees could certainly gobble up this \$15,000 coverage limit. The need for defense fees will depend on whether criminal or debt collection activity had occurred during your identity theft. Luckily, in all the websites that I browsed it doesn't seem like a lawyer is always necessary. It is OUR footwork and OUR time and our out-of-pocket expenses for various fees that seem to be the worst of it.

Of course ALL the transactions committed by one or more persons acting in conjunction are considered subject to that ONE overall limit for "identity fraud". ISO suggests a \$250 deductible per "Identity Fraud" yet some companies have reduced the deductible to \$100. The going rate for this coverage seems to be around \$25.00.

THAT'S A DEAL!!!

12. You might also want to increase the ISO HO Additional Coverage of Credit Card, Fund Transfer Card, Forgery and Counterfeit Money since this coverage applies to the actual LOSS of dollars from your banking account or charging of dollars to your credits cards.

### ISO HO-91 version

#### 6. Credit Card, Fund Transfer Card, Forgery and Counterfeit Money.

We will pay up to \$500 for:

- a. The legal obligation of an "insured" to pay because of the theft or unauthorized use of credit cards issued to or registered in an "insured's" name;
- b. Loss resulting from theft or unauthorized use of a fund transfer card used for deposit, withdrawal or transfer of funds, issued to or registered in an "insured's" name;
- c. Loss to an "insured" caused by forgery or alteration of any check or negotiable instrument; and
- d. Loss to an "insured" through acceptance in good faith of counterfeit United States or Canadian paper currency.

The ISO HO-2000 version is the same except wording is enhanced to clarify that unauthorized access of ATM machines is covered.

#### 6. Credit Card, Electronic Fund Transfer Card Or Access Device, Forgery And Counterfeit Money

Both the ISO HO-91 and the HO-2000 forms limit coverage to \$500. The **HO 04 53 Credit Card, Fund Transfer Card, Forgery and Counterfeit Money - Increased Limit** endorsement can be used to increase this "basic" \$500 coverage limit up to \$10,000 ... or more with some companies.

One needs BOTH these endorsements to be protected from Identity Fraud.

#### For those who want to know more ... try checking out these websites

<http://www.usdoj.gov/criminal/fraud/idtheft.htm> <http://www.idtheftcenter.org/index.shtml>

↓  
(US Department of Justice website on identity fraud) Identity theft resource center (ID test)

<http://www.idtheftcenter.org/idaftermath.pdf>  
2003 survey results

<http://www.privacyrights.org/fs/fs17-it.htm>

Privacy Rights clearing house  
Reducing the risk of identity theft-

<http://www.consumer.gov/idtheft/>  
Federal Trade Commission Identity theft  
website

[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z\\_ORG\\_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)  
complaint input site

Also has identity theft survey  
<http://www.ago.state.ma.us/sp.cfm?pageid=998>  
MA Attorney General Website  
look for Identity Fraud publication

\* \* \* \*



Copyright © 2005 Massachusetts Association of Insurance Agents  
Send comments or questions about this publication to [imorrill@massagent.com](mailto:imorrill@massagent.com)