# *Identity Theft*

*Charles L. Winstead, NSCI*
*December 8, 2010*

## Introduction

Did you read about the indictment last month of the five employees at the Johns Hopkins University Hospital for apparent fraud and aggravated patient identity theft? Allegedly, employees of the hospital illegally accessed the records of an untold number of patients and guardians of patients in their hospital to steal their personal information--names, ages, addresses, social security numbers, and other personal data. Using this illegally obtained information, the five suspects were able to apply for instant credit at local Maryland businesses and then make purchases before the credit cards were received by the identity theft victims. Over a two year period, the five were charged with obtaining more than $600,000 in credit from more than 50 businesses before being apprehended.[1] Or how about the detention in India earlier this year of Sergey Storchak, who is accused of hacking into the networks of Barnes & Noble, OfficeMax, Sports Authority, and a host of other large-scale businesses. Once inside their networks, sniffer programs were released and began collecting names, birthdates, credit card numbers, passwords, and other forms of account information of some 40 million international victims. Some of the stolen data was encoded onto empty cards which were then used to withdraw tens of thousands of dollars from unsuspecting identity theft victims from around the world. Some of the other stolen numbers were sold on the net to other criminals from around the world for their own use. Storchak, a Ukrainian, has been identified as the leader of the identity theft ring responsible for this larceny and whose members included other Ukrainians, Chinese, Estonians, a Belarusian, U.S. citizens, and others, according to the U. S. Justice Department. Extradition to the U. S. for this crime ring is underway, according to the FBI.[2]

***"I've heard of it (identity theft) happening, I just never thought it would happen to me."***
***Jay Marley, ID theft victim***

These incidents and others led us to speculate just how pervasive and insidious this issue of identity theft around the world really is today. What are the risks today, and how are these risks different from the risks yesterday? This paper will answer those questions with the most current information we can ascertain about this issue. We will start off with a definition of what identity theft really is, followed by a discussion of who is most at risk of being an identity theft victim and why. We will also look at who is actually stealing the personal information from others and what their motivations are. We will then look at the various tactics criminals use to get at victims' personal identities. Finally, we will end with a discussion and some suggestions on techniques one can use to prevent or at least decrease the risks of becoming an identity theft victim.

## What is Identity Theft?

The on-line Merriam Webster dictionary defines identity theft as "the illegal use of someone else's personal information (as a Social Security number) in order to obtain money or credit."[3] However, we agree with attorney Bernadette Safrath who asserts that the object of identity theft is much more comprehensive, extensive, and consequential. "Because the possibilities for an identity thief are endless, it could take you years to reclaim your identity and repair the damage done."[4] Safrath continues that thieves could actually provide your identity information to law enforcement officials during an arrest which may result in your arrest or other civil and/or legal actions when you fail to appear in court for the offense at some point in the future. She points out that "there is a common misperception that identity theft began with the internet. However, while the Internet has made identity theft much more widespread and pervasive, identity thieves started out getting information from telephone scams and from going through people's garbage looking for personal information on bills and other documents containing

[1] http://www.darkreading.com/insiderthreat/security/government/showArticle.jhtml?articleID=227600057
[2] http://www.darkreading.com/database_security/security/cybercrime/showArticle.jhtml?articleID=224701874
[3] http://merriam.webster.com/dictionary/identity%20theft
[4] http://www.ehow.com/about_5100724_history-identity-theft.html

important financial information."[5] For the purposes of this paper, we will use the Federal Trade Commission's (FTC) definition: " Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes." [6]

> **"Identity theft occurs when someone uses your personally identifying information like your name Social Security number or credit card number without your permission to commit fraud or other crimes."**
> **Federal Trade Commission**

The FTC details that about 50% of identity theft victims reported that a credit card was opened in their name. Another 25% reported that someone established a telecommunications service, either a landline, cellular, or another service in their name. About 15% reported that someone withdrew money from their bank account or established a new account in their name. Almost 10% reported that someone secured a loan using their credentials, and another 10% reported that the thief used their stolen identity to secure fraudulent documents such as drivers licenses.[7]

## Who is at risk?

The Federal Trade Commission is the U.S. government's agency chartered to protect the American consumer, and the task of assisting identity theft victims falls squarely in their court. In 1997, the FTC set up the Consumer Sentinel Network (CSN), a secure online database to manage the millions of consumer complaints received by the FTC each year. According to data released earlier this year by the CSN, identity theft has increased from 31,140 reported cases in 2000 to 278,078 cases in 2009. But these are only documented complaints formally registered with the FTC, which acknowledges that only about 60% of complainants even bothered to report the identify theft to their local law enforcement agencies as well.[8] However, the research firm Javelin estimates that when you add in other forms of identity fraud into this calculus and the unreported cases for a wide variety of reasons, over 11.1 million adults in the U.S. were victims of identity theft and fraud in 2009. This number represents a 12% increase from the previous reporting period in 2008, and is estimated to cost businesses and consumers over $54 billion in 2009 alone. Further, this statistic is expected to rise for the remainder of the decade.[9] According to age groups of victims, the CSN reports that the 20-29 year old group reports the most identity theft complaints (24%), while the 70 and over group reports only 5%. Victims in the 19 and under group report in at 7%. Citizens of Florida, Arizona, Texas, and California reported the largest percentages of complaints, while citizens of Iowa, Maine, and the Dakotas reported the fewest.[10]

And the costs for repairing the damage to one's financial records are astounding. "On the average it takes more than 600 hours to run around various agencies to clear your name. Worse still, it costs on the average of over $92,000 to restore your identity.[11] That's quite an investment.

We surmise that in any given year, anyone who has either a Government ID, a Social Security number, a credit or debit card, a check book, a drivers license, an e-mail address, a telephone number, or even a physical address is at some level of risk of identity theft. Others would disagree. A recent survey of college students and their parents shows that while 74% of parents believed their college-aged offspring were at moderate to high risk of having their identities stolen, only 21% of students felt likewise.[12]

[5] Ibid
[6] http://www.ftc.gov/bcp/edu/microsites/idthest/consumers/about-identity-theft.hteml
[7] http://www.hesaa.org/index.php?=identity-theft
[8] http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf
[9] http://www.internetnews.com/security/article.php/3864801/Study-puts-Identity-Theft-costs-at-54B-in-2009.htm
[10] http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf
[11] http://www.youngmoney.com/conusmer_fraud/133/
[12] http://www.infosecisland.com/blogview/8108-College-Students-At-Risk-For-Identity-Theft.html

We also surmise that this extraordinary explosion in the numbers of identity theft cases from 2000 to 2009 is directly correlated with the ever-increasing percentage of internet users in the U.S. While in 2000, only 44% of U.S. citizens used the internet, now over 77% are users.[13] We do not think these two increases are coincidental.

## Who Commits Identity Theft?

Our research has validated what the Greek philosopher Aristotle told us in the third century B.C.: "Every rascal is not a thief, but every thief is a rascal." [14] While we'd like to think that most identity theft is brought on by some brilliant but sinister cybercriminal sitting in some far away Eastern European country smoking strong cigarettes and drinking steeping hot tea, the unfortunate reality is that the rascals who most often misappropriate our identities are people we already know best--our family members, friends, neighbors, and co-workers. Of course, there are cybercriminals who work in commerce and professional identity thieves whom we have never met who steal our identities as well. We will capture a few current examples from each of these categories of rascals in the following paragraphs to document just how omnipresent identity theft really has become.

Desperate parents have been known to use their children's identity to extend their credit, get their utilities services such as electricity, heating, cable TV, or phones turned back on, and for countless other reasons. Take for instance the college student in Washington D.C. who told CNNMoney.com recently about her father taking out educational loans in her name. She had no idea that her father had taken out loans using her Social Security number and didn't find out about this until she was denied her first credit card. Her credit was already shot, and she had never even applied for credit. And then there was college student, Alex, from Ann Arbor, who found out that his dad had opened three credit cards in his name, charged them to their maximum limit, but had failed to make even the minimum payments. Alex's credit score had dropped almost 200 points before he even found out about this. Another student, Thomas, reported that his dad had used his son's identity to get a Vermont state drivers license to gain additional credit.[15] We have also found instances where the children in some families have taken out credit cards using their parents credentials. The list of family misappropriating identity continues on strongly today, unfortunately.

We also discovered instances of co-workers becoming identity thief rascals. Take the case of the Kansas City gaming casino employee who appropriated her co-worker's personal information and used this information to withdraw $18,000 from the friend's 401 (k) account.[16] This is not an isolated incident, regrettably.

We have found cases where both employees and employers steal the identities of their customers. Take the case of the Quest Diagnostics employee, for instance. Quest is a well known provider of blood screenings and urine testing for the government and private industry. An employee with Quest did some investigative work and determined that the Navy was sending in specimens for officers preparing for a deployment aboard the aircraft carrier USS George Washington to the Persian Gulf. Knowing that these six officers would be out of town and unable to check on personal affairs for six to nine months, the Quest employee used the victims' names, Social Security numbers and other private data provided in the screening to get credit in their names at local auto dealers and retailers. The rascal employee was eventually caught, however, but not before he had bought a $42,100 Cadillac Escalade and a $50,900 Nissan 350Z with the stolen ID's.[17] Then there was the case of the restaurant waiter who would steal the credit card numbers from patrons who he believed hadn't tipped him appropriately. This employee would

[13] http://internetworldstats.com/am/us.htm
[14] http://quotationsbook.com/quote/9138/
[15] http://money.cnn.com/2010/06/08/pf/parents_financial_abuses/index.htm
[16] http://benefitslink.com/boards/index.php?showtopic=42732
[17] http://www.leatherneck.com/forums/showthread.php?t=1392

then sell the card information to collect what he determined was his "earned tip".[18] One of the most costly cases of employee ID theft that we uncovered occurred in a small New York software business. It appears that no one canceled an employee's password after he left the company, and he was able to steal the credit reports of thousands of consumers, which he ultimately sold for about $30 each. He wasn't caught until he had received about $100 million.[19]

Employers misappropriate their customer's identities as well. Recently a medical transportation company employer was found guilty of aggravated identity theft when he was caught submitting fraudulent Medicaid claims using the stolen identities of his customers. This employer was able to collect at least $303,329 before he was caught.[20]

Of course, there are the professional identity theft rascals whom we have never met as well. There are plenty of thieves in this category. It has been estimated that there are approximately 6,000 criminal gangs in Moscow, for instance, and almost all of them are believed to be involved in some type of cyber identity theft.[21]

But you certainly don't have to leave the shores of the Unites States to find identity theft gangs. Operation "Smoking Gun" in Fort Lauderdale earlier resulted in agents discovering "a treasure trove of guns, drugs, and identity theft instruments in a room full of names, bank account info, and credit card machines,"[22]prompting U.S. Attorney Jeff Sloman to comment, "I think it speaks to the evolution of crime in society today."

Some professional identity theft rascals have achieved quite a bit of notoriety. Perhaps the most famous is hacker Albert "Soupnazi" Gonzalez who is currently serving 20 years in prison for the largest identity-theft case in U.S. history. Gonzalez was convicted in the hacks of TJX, Hannaford Brothers, and others, resulting in the theft of more than 200 million credit- and debit-card numbers. Gonzalez eventually led investigators to more than $1 million in cash buried in a barrel in his parents' backyard.[23] Even more disconcerting than the extraordinarily-large loss of cards is the fact that Gonzalez was assisted in this crime by a former network security manager at Barclays Bank, Humza Zaman, who was also convicted and sentenced to four years in prison.[24]

Being famous certainly does not protect your identity either. A 32-year-old busboy from Brooklyn successfully stole the identities of Oprah Winfrey, Steven Spielberg and Warren Buffet, and others as well. When he was finally apprehended, he had over 800 credit cards in his possession. And then there was the case of Tiger Woods, the world famous golfer. It seems that Tiger's first name is Eldrick, and Anthony Taylor was successful in finding out Tiger's birth name, birth date, and Social Security number. He then was able to purchase goods on Eldrick T. Wood's credit line. Anthony got away with about $17,000 before he was apprehended. By the way, this was Anthony's third criminal felony in California, so he was sentenced to 200 years in prison.[25] This sentence is under appeal today.

All of the cases of our identities being compromised thus far have involved rascals actively working to steal our ID's, but how about our identities being released inadvertently? It happens more often than we'd like to think. A recent example of this inadvertent release of personal information occurred in November of this year. It seems that a General Services Administration employee e-mailed the names and Social

[18] http://www.privacymatters.com/identity-theft-information/who-is-identity-theft.aspx
[19] Ibid
[20] http://health.cch.com/news/healthcare-compliance/030110a.asp
[21] http://www.privacymatters.com/identity-theft-information/who-is-identity-theft.aspx
[22] http://www.nbcmiami.com/news/local-beat/Your-bank-account-in-the-hands-of-violent-street-gangs-84829172.html
[23] http://www.wired.com/threatlevel/tag/albert-gonzalez/
[24] http://benefitslink.com/boards/index.php?showtopic=42732
[25] http://www.identitysupport.com/118-famous-identity-thieves.html

Security numbers of the entire GSA staff to a private e-mail address. This action, of course, exposed the 12,000 workers' private information to those on the internet. The GSA notified the employees and provided them with $24,000 identity theft insurance.[26] This was a nice gesture by the GSA, but it is still very disconcerting to have your personal identification available to others on the net. But these workers join the ranks of millions of other Americans. Privacy Rights Clearinghouse reports that since 2005, more than 341,742,628 records containing sensitive personal information were involved in security breaches in the United States."[27] This is an enormous problem for our society and our personal security.

Adding insult to injury is the fact that only 138 identity theft criminals were convicted last year in the U.S. This is not good news for identity theft victims and represents a downward trend, going in the wrong direction. In fact, the Office of the Inspector General of the Justice Department (DOJ) reports that in 2008, convictions for identity theft totaled 144. The report goes on to say, "We believe that the DOJ needs to ensure that its efforts to combing identity theft are coordinated and are given sufficient priority."[28] We agree with this assessment -- it's time to get serious about prosecuting these cybercriminals.

## How do Criminals Commit Identity Theft?

We mentioned earlier that it has been estimated that identity theft costs Americans approximately $54 billion each year. When considering the worldwide effect, however, the Aberdeen group estimates that identity theft accounts for about $221 billion a year.[29] That is a staggering number and raises the question of just how thieves can be so successful in obtaining personal identification information. We will provide some of their most frequently used methods in the following paragraphs.

> Skimming: Worldwide, skimming is a gigantic business, costing consumers and the banking industry over $8.5 billion annually.[30] Skimming takes place when criminals attach a counterfeit card reader on top of an actual card reader at an ATM, thereby capturing and storing the magnetic strip information on the credit card. The crime is completed when a fake PIN pad is used in place of the actual PIN pad or a strategically placed camera snaps a photo of the card holder punching in the PIN. Now the criminal has both the card and the PIN of the unsuspecting card holder. Skimmers are a difficult criminal type to apprehend. They usually work on weekends when banks are slow to process charges and recognize physical changes to their ATMs. Detective Pedro Palenzuela from Palm Beach County reported earlier this year, "They are not idiots or drug-addled junkies trying to get $20. They're consummate businessmen. They adjust for the last countermeasure that we put in place. We build the wall higher, but they keep coming back with taller ladders."[31] In the near future, look for the magnetic strip on credit cards to be replaced with a processor chip holding the same information but much more securely. This technology is called EMV, named for the world's three largest credit card companies, Europay, MasterCard, and Visa. This replacement is scheduled to happen in Germany next year and will be the international standard for all in the very near future . [32]

[26] http://fcw.com/articles/2010/11/08/gsa-data-breach.aspx
[27] http://blog.executivebiz.com/five-myths-about cybersecurity/6102
[28] http://www.esecurityplanet.com/features/article.php/3873996/FBI-DOJ-Falling-Short-on-Identity-Theft-Report.htm
[29] http://www.spamlaws.com/what-is-id-theft.html
[30] http://www.thenewnewinternet.com/2010/03/11/skimming-off-the-top-crimes-easy-target/
[31] Ibid
[32] Ibid

Phishing: Phishing involves internet criminals who send spam or pop-up messages to ensnare personal information from unsuspicious victims. Phishers are looking for credit card numbers, bank account information, Social Security numbers, passwords, or other personal identification information. A couple of examples provided by the FTC are: “We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.” Or “During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.”[33] Consumer Reports claims that phishing is also a huge business and estimates that Phishing cost consumers more than $500 million over the past two years.[34]

Pretexting: Essentially, this scheme involves using false pretenses to obtain personal identification information. For instance, someone may phone your home and claim that he is conducting a survey in order to gather personal information from you. When he has as much information as you are willing to provide, he may then phone your bank and pretend to be you to gather further information by asserting that you have lost your checkbook and need account numbers for a deposit. One of the most widely documented cases of pretexting involved Hewlett-Packard's (HP) attempt to gather information about their employees, board members, reporters, and family members to determine who was leaking information about their company to the press. HP eventually settled for $14.5 million.[35] You might recall in the movie Live Free or Die, Justin Long pretexts a BMW representative convincing him that his father is dying and conning the BMW representative into remotely starting his car to get him assistance.

Dumpster Diving: Thieves rummage through trash routinely looking for credit card applications, banking information, insurance information, tax information, and any other personal identification information that has been discarded. Once your trash leaves your home, it no longer belongs to you but instead belongs to the person who recovers it. "The reality is that most company trash is fairly clean, and provides a gold mine of information."[36] An ID criminal could easily complete a credit card application sent to someone and have it delivered to a different address. It could be months or even longer before the victim is notified.

Shoulder Surfing: This involves the practice of watching someone from a nearby location as they punch in PIN codes or listen to someone as they provide personal identification information to others during a phone call. As SearchSecurity states, "Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices."[37]

Stealing: ID theft criminals steal wallets, purses, or even mail, where they can obtain consumer account information, bank account numbers, credit card statements, or other personal identification information. This happened to one of our associates recently when she was visiting Chicago. With a purse zippered closed and on her shoulder, a thief was able to unzip the purse and remove an ID wallet sometime between 9 am and noon. When she attempted to pay for

[33] http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm
[34] http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/phishing-costs-millions/state-of-the-net-phishing-costs-millions.htm
[35] http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=196602512
[36] http://www.iss.net/security_center/advice/Underground/Hacking/Methods/WetWare/Dumpster_Diving/default.htm
[37] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci802244,00.html

lunch, she discovered the theft and immediately notified the credit card company. The thief had already used the card for purchases of more than $2500.

Changing your address. We could not find any reports on exactly how much identity theft cost consumers and industry as a result of someone fraudulently changing an address. However, we do know that financial institutions spend an estimated $300 million each year to send out confirmation letters when they receive a change of address form.[38] We assume that the financial institutions would not engage in such an expense if they had not suffered some significant losses in the past.

## How to Prevent Identity Theft

As we pointed out earlier, Albert Gonzalez successfully hacked into the TJX network and had access to over 200 million credit and debit card accounts with personal identification information. A case we didn't point out is the successful hack into Heartland Payment Systems early last year. Heartland handles about 100 million transactions each month for almost a quarter of a million businesses.[39] All of that personal identification information was exposed to hackers for their use and for sale to others. Add to these two cases the report by Privacy Rights Clearinghouse that about 342,000,000 records containing sensitive personal information were involved in security breaches in the United States last year, and one must come to the conclusion that your data is probably already out there in someone's possession. If not, it's only a mouse click away. With these facts in hand, there are still steps we believe you should take to reduce the odds of your becoming a victim of identity fraud.

We like the Department of Justice approach which centers on the word "SCAM." These rules are available on their website at http://wwww.justice.gov/criminal/fraud/websites/idtheft.html in full, but I will summarize below the essentials of their recommendations.[40]

**S**--be stingy about providing your personal information to others. Make people prove to you that they "need to know" this information. And don't provide personal data over the phone if someone calls you. Ask for a written form to be mailed to your home. If they do, use the Better Business Bureau as a guide for whom to trust. If an emergency situation does occur when you must provide personal information, be very careful about those around you.

**C**--check on your financial information on a regular basis. Look for documents that both should be there and those that should not be there. You should have credit card statements, bank statements, etc. If you are not receiving them, phone the company immediately and check to find out why your statements didn't show up.

**A**--ask for a free copy of your credit report. Federal law requires that major nationwide consumer reporting companies provide you a free report yearly. Review this report carefully to make sure no one has opened up any accounts you are unaware of.

**M**--maintain vigilance of records for all banking and financial accounts. DOJ recommends you maintain monthly statements for 12 months at a minimum.

The FTC has a similar program for consumers to use termed "Deter, Detect, and Defend." "While you can't entirely control whether you will become a victim (of identity theft), there are steps you can take to minimize your risks."

[38] http://www.bankinfosecurity.com/articles.php?art_id=1282
[39] http://www.informationweek.com/shared/printableArticle.jhtml;jsessionid=LY2XLG4IPMB2HQE1GHRSKH4ATMY32JVN?articleID=212901505
[40] http://wwww.justice.gov/criminal/fraud/websites/idtheft.html

**Deter**--safe guard your personal information by shredding financial documents before you discard them. Only release your Social Security number when absolutely necessary, and don't provide any personal information over the phone or internet unless you are positive about who you are dealing with.

**Detect**--routinely monitor your financial accounts and billing statements. Be alert to events that require immediate consideration such as bills not arriving on time, unanticipated arrival of new credit cards or account reports, or denials of credit. And, of course, letters about purchases you did not make.

**Defend**--if you think your identity has been breached, contact the fraud department of the three consumer reporting companies--TransUnion, Experian, and Equifax. Provide them with your information and have them place a fraud alert on your accounts. And, of course, close the accounts you believe are counterfeit. You should also file a report with your local law enforcement agencies. And, finally, you should file a report with the FTC.[41]

Our advice to all is to maintain vigilance on of all of your accounts--chances are that someone already knows much more about you that you would feel comfortable with them knowing. It's not all bad to be a little suspicious about releasing your personal information.

[41] http://www.ftc.gov/idtheft