Identity Theft and the Internet.

By: Stephen Schaefer

Georgia State University College of Law
Law and the Internet
Professor Wiseman
Fall 2002

Table of Contents:

Introduction

Identity theft is a prevalent crime in America today. It is easy for someone to steal your identity in many ways so as to apply for credit cards in your name, charge goods to your credit cards, get loans in your name, and even take money from your own checking accounts. The theft of one's identity can be done by stealing your mail, getting receipts from stores, or even by gaining access to information you have on your computer or on web sites you access to buy goods. If one steals one's identity it can be a long, tedious, and sometimes painstaking process to correct the wrongs that were done. The Internet is becoming an ever popular way for thieves to gain information to conduct identity theft. How do they do this? Is it easy for these thieves to perform this process? What laws are out there to protect the consumer? I will go through what constitutes your identity, how a hacker can steal your identity on-line, what rules protect people on-line, and what steps one should take to protect one from identity theft online.

Back to table of contents

What is identity?

From your date of birth you start out as a person with a name. The world has come to know each individual in many ways so to keep track of you. For tax purposes, identity purposes, and cross checking each person applies for a Social Security number (SSN). This number along with many pieces of information only relevant to that individual constitutes what the financial world considers as one identity for a person. Such items that financial institutions look at are:

· Current and last five addresses

· Social Security number

· income and sources of income

· taxes paid

· criminal record

· financial status

· charitable donations

· what you have owned (cars, house, etc.)

· credit card numbers

· where you have traveled

· mother's maiden name

Each time one applies for a credit card, one uses most if not all of the above mentioned information. The same goes for loans, utilities, driver's license, etc. This is the way people are identified from one another. A problem comes in when someone finds use from your identity. Whether you are wealthy, middle income, old, or young - if you have any credit you are susceptible to having your identity stolen and used by people for their own personal gains.

Back to table of contents

What is identity theft?

Identity theft is an easy and quick way for one to gain money with low probability of prosecution. All that is needed is your Social Security number, your birth date and other identifying information such as your address and phone number and whatever else they can find out about you. With this information, and a false driver's license with their own picture, they can begin the crime. They apply in person for instant credit, or through the mail by posing as you. They often provide an address of their own, claiming to have moved. Other ways involve lifting people's credit card numbers and trying to use them for personal gains. Sometimes if a person or group steals a bunch of credit cards they will buy a small item here or there to test it out. If successful they will wait to make the large purchase (TV, computer, etc.) and sell that product back for cash. Negligent credit grantors, in their rush to issue credit, do not verify information or addresses. Once the impostor opens the first account, they use this new account along with the other identifiers to add to their credibility. This facilitates the proliferation of the fraud. Now the thief is well on his/her way to getting rich and ruining your credit and good name.

Back to table of contents

Cases of identity theft

Anyone that has access to money is susceptible to identity theft. Whether you use the Internet or not you are privy to this crime. The question is what is the true risk with the use of the Internet. Some cases have come up in the last year that has caused more concern. Vast crimes have been made against professional athletes, fake e-mails have caught unsuspecting people, computer loopholes have been taken advantage of, and other areas of the Internet are open for exploitation by the

computer hacker who is looking for an easy dollar.

Professional athletes have a major problem with identity theft. With the public reporting of salaries, birth dates, and full names, the criminal looking for an easy buck is halfway home to getting easy money. You can sometimes find out where athletes live and what contributions they make. With the problems in sports, you also have their rap sheets in public view. The interesting point is that up to last year most of this information can be found on the league for each professional sport. All a person would need to do is access this information and say he/she is moving and needing to update his/her information. With the fraud in taking this info, he/she can access just about any information one could get one's hands on. Such examples lately of identity theft is for athlete Tiger Woods . He had a suspect run up over $50,000 in credit charges to his legal name in Sacramento stores. The suspect used Woods' identification, including a counterfeit Social Security card with the correct number but an incorrect middle name, to establish credit at Circuit City , and bought a DVD player and a dishwasher. Other noteworthy cases of identity theft in professional athletes have been a man named Jonathan Hoskins who victimized New England Patriots Ty Law by obtaining an Ohio driver's license in Law's name and made two $10,000 withdrawals from Law's bank account. San Antonio Spurs (and ex-Atlanta Hawks) guard Steve Smith's information was used to run up $81,000 in credit card charges, and Washington Redskins quarterback Danny Wuerffel had a store account opened in his name without his knowledge. The NFL says it deals with dozens of identity theft cases every year. Because of this they are not only briefing the players each year on identity theft, but they are also taking out birth dates from the media guides. 1 .

In one widespread case, Yahoo said that many of its customers had been tricked into giving their credit card numbers to an unaffiliated third party that had posed as Yahoo in a mass e-mail. People who pay for services through Yahoo ranging from e-mail service to matchmaking, did not know they were divulging their information to a third party. It was 24 hours until Yahoo realized the snafu in security and informed their customers. During this time many had acted upon the message. By having one's name and credit card number, one can run up many purchases on the Internet before reaching the credit limit of that person. 2 .

Recently it was discovered that a flaw in the Microsoft Windows operating system could allow the hackers to gain unauthorized access to 1000's of computers. The flaw was in the program that handles digital certificates to certify the authenticity of a web site or software code. This program would let a web site with a valid certificate issue a second invalid one which could enable unauthorized access to a computer as well as among other things the theft of user passwords or credit card numbers. The site can pretend to be Amazon.com and get a person to enter his/her credit card number. Microsoft has issued a program for people to use to serve as a patch to alleviate the possibility of this problem. This problem might not notify patrons that someone is diverting them to a non legitimate site where their identity information could be hacked. Getting used to Microsoft or other programs to force you to update the software on demand could allow a loophole where someone does not know they are downloading from a wrong source and may be downloading a Trojan horse that will benefit the hacker. 3 .

A recent story revealed that one individual had taken over 30,000 people's data from a credit data bank that included their credit accounts and passwords. They used the information to take out loans in the names of the victims, buy goods, and wipe out their bank accounts and credit cards. The insider sold the passwords and information for a nominal fee with the buyer using the information for credit lines. The interesting part is that it is hard to trace the links. The only individual who is usually identified is the unsuspecting victim. While they may not be responsible for debts incurred on credit cards, the bank usually does not guarantee funds and the victim's credit history is ruined for seven years. In most of the victim's cases, the only information used to get loans in the victim's names were the victim's address, name, and Social Security number. 4 .

A hacker can have hundreds of opportunities to view all sorts of personal data just by driving around in a big city. Wireless technology can leave gaps that might not be closed by computer techs at companies. If an encryption program is not used on a wireless system, any information transmitted over open wireless waves can be picked up and hacked into. Such information as customer names and credit card numbers can be seen in clear text with no hacking necessary. PDAs and cell phones might store such information and can also leave someone at risk. If someone uses one of these items to

charge a bill, and the hacker is "listening" in for this wireless device, they can gain access to the credit card information and utilize this to his/her advantage. 5 .

A separate plot to show further aggravation against the consumer involved fraud against eBay users. Some people made a fake web site and contacted over 55 million users to update their billing information at this fake site. The e-mail had a link to the non relatedeBay site simply called ebayupdates.com; and people proceeded to re-enter financial data for eBay. The information given could open up loopholes for people to use their credit card numbers or information to gain credit cards. eBay had to send a wide scale message to beware of such fraud. 6 .

Anyone can be involved as a victim of identity theft. Just this year my credit card company called to inform me that someone had used my credit card number to buy items on line for pickup in California the same time I was using my card at Piedmont Hospital buying balloons for my wife after the birth of our first child. After thinking about how easy it is to pick off my personal information, the question came to me as to whether the people got the information on-line, bought the information, or some other unknown way. One question that comes up is how easy is it for a thief to hack into a computer system to gain access to personal information?

Back to table of contents

How the hackers do their dirty work

Identity theft occurs when one person intentionally assumes another person's identity. Identity theft comes in many fashions from in person, to mail, to now the blooming of Internet theft. Thus far, identity thieves have typically gone on shopping sprees at the expense of their victims, but the possibilities for abuse through identity theft will grow as the functionality of the Internet expands. With the Internet, the key goal is to gather information. Some ways to gain information is from credit banks and trying to steal credit card numbers and passwords. Another way of theft is through Internet shops that store credit card numbers for the one step shopping. Another way thieves deceive individuals is to have the victims store his/her credit information on the fraudulent site.
The lowest form of theft is through asking children for key information about their parents (where do you live, what are your parents' names, how long have you lived at that house, what are your grandparents' names, etc.). Through e-mail or chat rooms, unsuspecting children could give away their parents key information - maybe even their credit card numbers. There are many ways that the thieves can get their information - but how are the victims giving it to them unsuspectingly?

One common aspect with all on-line businesses is personal information stored for use of repeat shoppers. The storage of information can save histories of their purchases and can eliminate steps of entering data each time the customer comes back to the site. The hackers look for loopholes in different ISPs to gain necessary information they are looking for. Internet sites not only leave information available each time someone visits a site, but they also sell this information to whoever will buy it. Here is a list of items that are common among web sites:

- web sites may freely gather as much personal data as desirable from consumers.
- web sites need not ask permission to gather personal data.
- web sites need not inform consumers of their data gathering practices.
- web sites may use personal data in any manner they prefer, such as selling or licensing it to third parties.
- web sites need not allow consumers access to their data.
- web sites need not provide security for personal data in their possession. 7 .

Why is it that companies leave such personal data online for others to buy and use? The main reason is that these early web sites used personal data for the interests of the web site industry. They reflect the fact that most web sites, neither legal nor social pressure to respect the data privacy of the visitors to their sites. There was no legal pressure because there were no laws against the practice of selling personal information and there was little social pressure because most people had little or no awareness that these practices were taking place. Personal information is not owned and at this time is not unlawful to collect without consent. This data has become very valuable to companies, the hackers, and anyone who sees

value in it. Take for example the value cards you use at your local grocery store. These grocers make you use the card to get their sale prices while at the same time keeping track of everything you buy and where you buy it. The same is done on the Internet. Every time you sign on to a site, buy an item, or just browse unknowingly you leave a mark you have been there. If you have bought anything, you probably left personal information along with your credit card number, address, and whatever was required of you to make the purchase. While the consumers were unsuspecting to the gathering of their personal data, they were even less suspecting of the selling of their personal data. They did not know that they should bargain for the use of their data. It was just an unsuspecting result of doing business with these companies. 8 .

Despite a lack of bargaining, there may be reason to think these norms were efficient. The companies that utilize the information feel it is justifiable from an economic perspective. These companies can use personal data they take from their web site which can be found in the public domain. This information at the time of the Internet was under utilized, and companies put this personal information to productive use. The perspective is to make use of a common resource that would otherwise be left lying in an unproductive state. Personal data is a good that can be used without competition; collection and use of personal data by one web site does not diminish the amount available, either for other s web sites for the company to use themselves. Because data is non rival, arguably it should be left unregulated so that the greatest number of users will have free access to its use. The problem with this is when the hackers buy the personal data and use this data unscrupulously. Some personal information gathered on web sites can be anything from a name and address to some people leaving their Social Security number, mother's maiden name, income, and spouse's name. Any of these pieces of information can be used to gain access to one's credit information. 9 .

The identity thieves not only look to buy information, but the computer savvy also look to gain access to identity information by hacking into a personal computer or to a company's computer. Personal computers are not the normal route of access. To gain any information the hacker would have to catch a person when they are in the process of making a purchase on line. The most common way that the hackers gain their information is to hack onto corporate storage areas. All business, whether small businesses or fortune 500 companies, are susceptible to the trap. The modern hacker has been highly successful in discovering problems in web site practices making them susceptible to hacking. The hacker uses many steps in gaining information. One example of a hacker technique is called "Root-Access" hacking. First he/she must gain a higher system privilege to the company's site and look for what they call "all access" keys. With these keys, he/she then can hack in to get the directory where the password files are kept. Once into the system and directories, the hacker looks to plant a Trojan, obtaining personal information, downloading the system password files, or stealing stored unencrypted credit card numbers. The last part of the plan is covering his tracks to not tip off his intrusion and installing a "backdoor" that will allow future access to this corrupted site. In this part, the hacker modifies the system logs to remove traces of the attack. Once these steps have been achieved, the hacker "owns" the system. 10 .

For the hacker to gain access to the system, a usual practice is to sign on to the company's site for a trial "shell" account under an assumed identity . With shell access, the hacker telnets into his shell account and enters a series of commands that exploit a loophole that is found in most Sendmail programs. This allows the use of telnet commands to write a message directly to a directory of the ISP that sets up a password free root account for the hacker's use. By performing the Sendmail program, the hacker is taking a chance he could leave several traces, and the program may not grant him the complete access he needs to steal the credit cards. The advantage of using this method is if he is lucky, he can not only have access to system passwords and directories, but he can also plant a daemon for later access. Once he has root access, his next objective is to download the system's passwords so he can log on as another user. By being logged on as a different user, he reduces his chances of being caught by covering up his identity. 11 .

After the hacker has cracked the password, he will log into the business' account by File Transfer Protocol (FTP), try to find the directory where the credit card numbers are stored, and download the files. The hacker takes a chance at this time by leaving a trace of the hacker's access to the directory. The hacker will usually foresee this and either use his root account, or any other password to edit the log files to divert attention from him. If there is no company representative watching the directory's access at this time the hacker will explore the system to find where the log files are stored and uses what is called a " rootkit " that will automatically sweep up his tracks by replacing several critical files with dummy or non-descript files. The hacker will create a separate directory on the server that will avoid detection of intrusion with a

standard Linux "ls" command that shows a list of directories in a given path and hide the "rootkit" in the hidden directory. At the end, the hacker will install a "backdoor" to use in the future for the hopes of bypassing security constraints. In this case, the hacker will place a Trojan program in the directory under a specific user name configured for telnet logins so he can re-enter the system with the minimum amount of attention. A Trojan is a program that does something undocumented that the programmer intended, but that some users would not approve of if they knew about it. In addition, the hacker could plant what is named a " sniffer " that will capture such activity as user names, passwords, and credit card information. The "sniffer" is a program that the hacker makes which saves information into a file set up by the hacker in a company's directory so the hacker can retrieve information at any time. The last measure for the hacker is to initiate a variation of a Trojan program to wipe the log files of any indication he was in the system and log off of the system. **12 .**

Hackers do not always have to hack into a company's web site to gain personal information. In some cases, companies legally take information and sell them in a way not liked by the law. One direct example is when DoubleClick was planning the acquisition of Abacus Direct. It was discovered that DoubleClick had the intention to combine the online and off-line personal data from both enterprises. The media was alerted of this plan and this story was given national attention before the merger. The belief being that the use of this data would not be beneficial to the consumer and in the end could leave the consumer at risk of identity theft. The price of DoubleClick's stock dropped dramatically after the story was released to the media, and the company's net worth became too much for the executives to handle. The company has been involved in lawsuits and subjected to a heightened level of scrutiny from privacy activists and the FTC since the story broke. 13

Another example of the media alerting the public to potential harm is when hackers discovered that Microsoft was building a tracking utility into its software and RealNetworks was tracking the online activities of its customers. The media coverage of these stories typically included a quote from a privacy advocate regarding the threat to personal privacy posed by the technology. Once under the media spotlight, these companies quickly backed away from their planned activities. Known threats to a consumer is starting to gain interest of media outlets, and with the help of their new acquired interest, the public can have nothing but benefit from the spotlight and possible. **14 .**

By looking at how the hackers can take the information and how companies use this information, it is an endless idea of how one's identity can be given to anyone at anytime. Without any circumvention of the law, there is no repercussion to utilizing what is perceived at as public information. Something has to be done to make a deterrent identity theft to crooks. There also has to be some checkpoints to make proper ways that one's personal information is shared (to whom, what information, and with what authorization). How is the government working to protect its citizens from these loopholes?

Back to table of contents

Laws associated with identity theft

There are many areas of the law associated with identity theft and online activity associate with this. Such areas associated with this are fraud, theft, and trespass to name a few. One law developed for online identity theft is ***The Identity Theft and Assumption Deterrence Act of 1998(*** **18 U.S.C. 1028**) 15 . This Act makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a true victim. Previously, only the credit grantors who suffered monetary losses were considered victims. This legislation enables the Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this crime. It allows for the identity theft victim to seek restitution if there is a conviction. It also establishes the Federal Trade Commission as a central agency to act as a clearinghouse for complaints, (against credit reporting agencies and credit grantors) referrals, and resources for assistance for victims of identity theft. This statute may serve as a model for your state to enact similar legislation. It should also provide you leverage to influence law enforcement to investigate your case.

How has Congress developed laws to combat cases like the example stated above about hacker activity? Congress specifically intended to apply 18 U.S.C. 1030 (4) (16) to the use of another's computer processing power. Senator Jon

Kyl noted during Senate discussion of the National Information Infrastructure Protection Act of 1996 that the bill: "Amends 18 U.S.C. 1030 (a)(4) to ensure that felony level sanctions apply when unauthorized use, or use in excess of authorization, is significant. The hackers, for example, have broken into computers only for the purpose of using their processing programs, sometimes amassing computer time worth far more than $ 5,000. The bill would penalize those whose trespassing, in which only computer use is obtained, amounts to greater than $ 5,000 during any one year period. "Companies should not be stuck with the bill for these thieves of information. Although they may not damage information, the hackers who browse through computer systems are a significant liability to businesses which must pay for a new security system, and the expensive time the hacker used.
17 .

In the "root access" hack described above, the potential for serious crime escalates because of the information that can be obtained, the damage that can be caused, and the value of data obtained. The federal government has given some direction in section 1030 as to the type of computer that was targeted and to what crime will be assessed to it. If the computer was a federal government computer or a computer used by or for the federal government, then 1030(a)(1)-(3) could apply. However, in most examples, a thief would most likely target a private ISP computer or a company that uses their own server. One would also have to determine if the hacker obtained information, obtained anything more than $5,000 in value, or damaged the protected computer during his entry to the computer system. By using analysis of the case above, when the hacker targeted the Sendmail program, he did not obtain any information, nor did he obtain anything of value, or do over $ 5,000 damage to the computer at this point. With the analysis of Section 1030, the hacker did not commit a crime because he did not cause any damage, steal money, or use a federal computer. **18**

What about when the hacker downloaded the password files? That is an act of taking informat
for a misdemeanor, unless the prosecution can show that the value exceeds $5,000, was for personal gain, or
Section 1030(a)(2)(3) was meant to protect privacy where the value of the information, although lacking ide
The hacker could be found liable for a felony if the monetary value was above $5000. By looking at this, c
This is more in line with identity theft on a broad spectrum and can be utilized on the federal level. Mos
Georgia law states in Georgia Code §16-9-121 (**20**) a very broad case of what a criminal will b found liable
person's credit card numbers, bank account numbers, Social Security numbers, or even driver's license numbe

Of the 50 states, only New York , Vermont , and Nebraska don't have identity theft laws. **21** .

Analyzing the use of the identity thief's possession of stolen credit card numbers is a violation of several statutes. First, the theft of the stolen credit card numbers could leave the thief liable under 15 U.S.C. 1644 (b). In United States v. Callihan , **22** the court held that the giving of the credit card number over the phone by thedefendant was not considered a "transport". The court concluded a "credit card" is not just numbers, but through section 1644 the court used the term to mean the actual credit card with the account number imprinted. However, a year later, in United States v. Bice-Bey , **23** a different court held that any unauthorized ficicious use of a credit card, with or without use of the actual card violated 15 U.S.C. 1644 (a). The court found that the main component of a credit card is the number. The market has allowed the use of a credit card number over the internet or phone without a company representative actually looking at the card itself. Although the Bice-Bey decision concerned the "use" of the credit card, the court still held that the credit card numbers transferred over the phone constituted a violation of Section 1644(a). 24 .

Another avenue used in the punishment of an identity thief is if the thief stole more than fifteen credit card numbers. The thief can be found in violation of 18 U.S.C. 1029 (a)(3) if he "knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices." **25 .** According to 18 U.S.C. 1029 (e)(1), an "access device" means: "Any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds". 26 . This definition is broad and the scope was meant to go towards any possible use of a person's financial identity. The problem is that with this offense the sentences are light and in most cases the amount of credit card numbers would far exceed fifteen. An additional offense attached to the hacker and the access to credit cards is if the hacker uses one of the credit cards. By doing this he will have violated 18

U.S.C. 1029 (a)(2), if he "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one year period, and by such conduct obtains anything of value aggregating $ 1,000 or more during that period." 27 . If the hacker is found guilty of violating 1029(a)(2) or (3), he can be serve a prision sentance of up to ten years. **28 .**

Back to the intrusion of the company's computer director, when the hacker covered his tracks to his intrusion by editing log files, he caused damage to the computer under 18 U.S.C. 1030 (a)(5)(C), where one commits a crime if he/she intentionally damages a computer. The deletion and changing of the log files constituted an act of reckless or negligent damage, as provided for under 1030(a)(5)((B)-(C)). This is damage to not only to the company's security system, but also the log set up to track use of the company's site. Some have argued that there is no "damage", but this argument has not been successful in courts as of yet. Is the computer actually damaged in the sense of harm, or is the manipulating of one's files actual damage by itself? The hacker also commited another crime when he made his own directory on the company's system and created a "backdoor" to be used on this site. By creating a "backdoor", he commited an act similar to someone cutting a hole in a person's fence or breaking a lock off a door. When the hacker installed the "sniffer" to make a copy of all the network activity, he further damaged the system in violation of 1030(a)(5)(A), possibly violated 1030(a)(4) if he obtained anything of value from the "eavesdropping," and most likely violated 1030 (a)(3)(C) by obtaining information from a protected computer and violated the privacy that Congress specifically intended to protect. This is also an addition to the ISP's software and changed their original log system and security system. By adding on areas that only the hacker has knowledge of and access to, the Internet Sevice Provider (ISP) or company is held helpless to a trap door for damage to their site and stealing of information (i.e. workers who conspire to let others steal merchandise from a store without the owners knowledge). **29 .**

The program writer of the Trojan program could also be held liable under 1030(a)(4). That subsection covers the knowledge and intent to defraud a protected computer and to take anything of value in excess of $ 5,000. This crime with the money value would be a felony. Strange as it may seem, Congress fell short of making this a harsh crime for all intents. Congress did not intend to charge all people who break into computers for a felony, only those with the key elements of knowledge and intent. The hacker could also be liable under the more serious 1030(a)(1) and subject to ten years in prison if the Trojan ends up on any computer used for information of national concern, or which causes injury to the United States or for the advantage of any foreign nation. This section makes a broad basis for "delivery" because it allows for attempted transmission, not just delivery. **30 .**

The need for limiting access to the SSN is important because the potential for abuse is great when vast amounts of personal data are linked to one number. Moreover, the number is easily accessible by numerous people who work in various agencies and organizations that use the number as an identifier. The problem is compounded with the expansion of the Internet and its relatively unregulated transactions. With the ease of a modem and a phone line, much personal information is transmitted about individuals as they converse, shop, and surf the Web. 31 **.**

Growing increasingly common in recent years is a phenomenon known as identity theft , where thieves steal someone's identity to get their driver's licenses and credit cards, buying everything from mobile homes to toys. The use of someone's SSN is one way thieves get their identity. Criminals can get one's personal information by ordering credit reports, digging through garbage, stealing mail, and through other means. There are many "look-up" service companies that provide private information about individuals to law enforcement agencies, private investigators, law firms, banks and various businesses. Although the Federal Trade Commission reported that access provided by these look-up services was not the only factor contributing to fraud, these services greatly increase risks of fraud because they substantially facilitate access to public records. In 1997, the General Accounting Office found that identity theft contributed to the loss of $ 745 million by consumers and institutions. In addition, Trans Union, one of the three major credit reportingagencies, reported a major increase from 1992 (35,235) to 1997 (522,922) in requests for help from fraud victims. **32** .

Public activists have noted a wide variety of harms that may arise due to improper online data collection and use. Activists have sought to inform the public of the causal connection between privacy and web site data collection activities because the potential harms resulting from an inability to control personal data are not readily apparent. Many try to show why this

information is unnecessary for businesses to request. When filling out web use registration, why should a site know your Social Security number, years you have lived in your current home, your mother's maiden name, or your income? While this could serve for identifying the market using the site, it also will serve as a bargaining tool for that site to sell your information if it is valuable to others. The other side looks at the fact that consumers are not significantly harmed by identity theft, as fraudulent credit card billing is insured beyond a $ 50 deductible. While this may be true in the fact that each credit card will only charge up to $50 dollars, but what is done to protect your credit rating? If you cannot clean up your credit for the fraud use, you may have to wait seven years for the fraud to be erased off your record. **33** .

Back to table of contents

How to protect one from identity theft

Protecting your self on-line has become such a key issue that the Federal Trade Commission (FTC) has made a web site available with tips on how to protect yourself. Such issues as how you pay for items on-line, what to look for on web sites, and how to determine if web sites are safe to browse are common issues addressed. Each of these issues separate may seem simple and trivial, but ignoring these issues collectively might leave one's credit open for the taking. 34 .

The ease of shopping and comparing products and prices online has made it an attractive option for many shoppers. How can you make sure your transactions are safe and your credit card information is only going where you intend it to? There are several ways to help ensure safe transactions on the Internet, and more are becoming possible all the time. Some of these include:

- Stored value cards (cards that you can buy with specified, loaded dollar amounts)
- (cards that can act as credit cards, debit cards and/or stored value cards)
- Point-of-sale (POS) devices (like your PDA or cell phones)
- digital cash
- e-wallets
- Online payment services like pay pal. 35 .

The most prevalent method for paying for the things you purchase online is still the credit card. The following paragraphs provide some tips on how to make sure your transaction is secure.

The program that you use to surf the Internet is called a browser. This software has built-in encryption capabilities that scramble the information you send to a web site. Using the most recent browser ensures that the data is protected using the latest encryption technology. This technology also uses a Secure Sockets Layer (SSL), which is an Internet security protocol used by Internet browsers and web servers to transmit sensitive information. The server receiving the data uses special "keys" to decode it. You can make sure you are on an SSL by checking the URL -- the http at the beginning of the address should have changed to https. Also, you should notice a small lock icon in the status bar at the bottom of your browser window. 36 .

Another way to make sure a site is secure is to look for digital certificates. Through Java code different web sites acquire digital certificates that authenticate the entity you are dealing with. Independent services like VeriSign will authenticate the identity of the web site you are visiting. Web sites that use this service (usually those that sell items or services online) will have the VeriSign logo. By clicking on the logo, you can be assured that the site is legitimate, rather than a clone of the legitimate company set up to collect your personal and financial information. Companies such as VeriSign use cryptographic proof of who sent the message. On most lower right hand corners of a Internet browser, one can see a lock (open if unsecured, locked if secure) to show whether the information used is secure. 37 .

Another way to check the security of a site is to read the privacy policy provided by a site . The information you enter on the Web site should be kept confidential. Make sure you read the company's privacy policy to ensure that your personal information won't be sold to others. Services like Verisign review a company's privacy policy (for a fee) and then allow

the company to post the Trust-E logo if its privacy policy follows certain industry standards for consumer protection. Without the knowledge of personal information being held secure, and you still use the site, you are allowing the site to sell any information you give to anyone who wants. The first time you give your consent will serve as consent each time the company sells the information.

Another way to keep tabs on the information you give out at web sites is to only use one credit card for all of your online purchases. By doing this if someone steals your information or acquires your credit card number you are only held liable for that one card. Credit card companies usually have a $50 deductible towards credit card theft. Some cards are now securing all purchases at no cost to the consumer. Either way it would be best to only leave one avenue of theft for thieves. One could watch the use of that one card and make sure there are no unintended charges placed to it. Keep records of all of your Internet transactions **.** Watch your credit card statement for the charges and make sure they are accurate. After you have made purchases online, check your e-mail**.** Merchants often send confirmation e-mails or other communications about your order.

Another way to defend yourself online to identity theft is to never give out passwords or user ID information online unless you know whom you are dealing with and why they need it. Make sure that if an Internet service provider or company is requesting you to resubmit your information that it is really that company you are dealing with. This is a relatively recent scam used to access your account and get your credit card number, along with whatever other personal information is there. eBay had a thief develop a site just for the purpose of people being tricked into submitting their personal information thinking they were updating their eBay account. The best way is to be aware of what information identifies you to thieves and make sure you give out only necessary information. Such items as your birth date, Social Security number, and mother's maiden name are not necessary. Social Security numbers are used as a simple way of identification. If a company asks for this, ask to use a password or id identifier instead. If the company persists at the necessity of your Social Security number, maybe you should not do business with them.

Another line of defense to identity theft is to install a firewall on your personal computer. A firewall is software or hardware designed to block the hackers from accessing your computer. A properly configured firewall makes it tougher for the hackers to locate your computer and get into your programs and files. A firewall is different from anti-virus protection: Anti-virus software scans your incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. Along with a firewall, one should become aware of the software that is installed on your computer. Some features are typically turned on and they should be turned off when you are not using them - such as instant messaging, printer-sharing or file-sharing. In some computers, these features are typically on when a computer is shipped. Because these programs facilitate the passing of information between computers, they are an excellent entry point for the hackers. [38] .

Using all of these ideas can help you in the defense of identity theft. Being careful can help, but sometimes unsuspecting people get taken advantage of due to companies selling personal information. Until the laws attach harsher penalties to identity theft and the selling of personal information can be made an accessory to identity theft if the information is used that way, people will always be at risk. At this time, selling of personal information is legal - but should it be? People should have a choice of whether their information is sold just like they should choose to receive telemarketers phone calls or a filter for Spam mail.

Endnotes

1 . Outside the Lines Weekly : Identity Theft and Athletes, ESPN November 2002.

2 . Bogus E-mail picks up credit card numbers - CNN.com - 10-18-2002

3 . Joe Wilcox, *Credit card theft feared in windows flaw* . CNET News.com; 9-6-02 .

4 . *Ex-Employee faces charges Massive Identity Theft* Atlanta Journal Constitution; November 26, 2002.

5 . Bill Husted, *Lack of Wireless Security an Invitation to the Hackers.* Atlanta Journal Constitution; Sept. 18, 2002 .

6 . *Internet Watchdog Warns of Fake eBay Web Site*, The Mercury News, December 11, 2002.

7 . Winn Schwartau, *Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption.* 88-95. New York : Thunder Mountain Press, 2000.

8 . Steven A. Hetcher, *The Emergence of web site Privacy Norms* . 7 Mich. Telecomm. Tech. L. Rev. 99 (2000)

9 . Id

10 . Eric J. Sinrod and William P. Reilly, *Cyber crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 Computer & High Tech. L.J. 210 (May, 2000)

11 . Id 211.

12 . Id 212.

13 . Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace.* 16 Berkeley Tech. L.J. 877 (Summer, 2001).

14 . Id.

15 . 18 U.S.C. 1028

16 . 18 U.S.C. 1030

17 . Eric J. Sinrod and William P. Reilly, *Cyber crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 Computer & High Tech. L.J. 210 (May, 2000)

18 . Id.

19 . Id.

20 . Ga Code Ann. § 16-9-121 (2001)

21 www.ftc.gov

22 . United States v. Callihan, 666 F.2d 422 (9th. Cir. 1982).

23 . United States v. Bice-Bey, 701 F.2d 1086 (4th. Cir. 1983).

24 . Eric J. Sinrod and William P. Reilly, *Cyber crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 Computer & High Tech. L.J. 213 (May, 2000)

25 . 18 U.S.C. 1029 (a)(3) (2001)

26 . 18 U.S.C. 1029 (e)(1) (2001)

27 . 18 U.S.C. 1029 (a)(2)(2001)

28 . Eric J. Sinrod and William P. Reilly, *Cyber crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 Computer & High Tech. L.J. 213 (May, 2000)

29 . Id.

30 . Id 214.

31 . **Id.**

32 . **Id 215.**

33 . www.ftc.gov

34 . J.D. Candidate, *Univerrsal Health Identifier: Invasion of Privacy or medical advancement?.* 26 Rutgers Computer & Tech. L.J. 331 (2000).

35 . www.ftc.gov

36 . Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace.* 16 Berkeley Tech. L.J. 877 (Summer, 2001).

37 . Winn Schwartau, *Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption.* 88-95. New York: Thunder Mountain Press, 2000

38 . Id.

Bibliography

18 U.S.C. 1028 (2001)

18 U.S.C. 1029 (2001)

18 U.S.C. 1030 (2001)

Bill Husted, *Lack of Wireless Security an Invitation to the Hackers,* Atlanta Journal Constitution, Sept. 18, 2002 .
Bogus E-mail Picks Up Ccredit Card Numbers, CNN.com, Oct. 18, 2002.
Eric J. Sinrod and William P. Reilly, *Cyber crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 Computer & High Tech. L.J. 213 (May, 2000).

Ex-Employee faces charges Massive Identity Theft, Atlanta Journal Constitution, November 26, 2002.

Ga. Code Ann. § 16-9-121 (2001).
Internet Watchdog Warns of Fake eBay Web Site, The Mercury News, December 11, 2002.

J.D. Candidate, *Univerrsal Health Identifier: Invasion of Privacy or medical advancement?*. 26 Rutgers Computer & Tech. L.J. 331 (2000).

Joe Wilcox, *Credit card theft feared in windows flaw* . CNET News.com; 9-6-02.
Outside the Lines Weekly : Identity Theft and Athletes, ESPN, November 2002.
Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace.* 16 Berkeley Tech. L.J. 877 (Summer, 2001).
United States v. Bice-Bey, 701 F.2d 1086 (4th. Cir. 1983).

United States v. Callihan, 666 F.2d 422 (9th. Cir. 1982).

Winn Schwartau, *Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption.* 88-95. New York: Thunder Mountain Press, 2000
www.ftc.gov