

Identity Theft - Is It A Cryptographic Problem?

An Interactive Qualifying Project report

submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

by

Patrick J. Bonneau

John W. Hajeski

Date: March 14, 2005

Approved:

Professor Berk Sunar, Major Advisor

1. identity theft
2. personal security
3. public policy

Professor William Martin, Co-Advisor

Abstract

Identity theft occurs when a person uses the means of identification of another individual to commit criminal activity. Americans of all demographics are potential victims of this crime. After looking at the details of this problem, it is apparent that the growth of identity theft can be attributed to various factors. Hence, a singular source is not to blame for the increasing problem. In particular, identity theft is not only a cryptographic problem, but an educational problem as well.

Acknowledgements

The authors wish to thank their advisors, Professor Sunar and Professor Martin, for their personal work towards the advancement and completion of this project. They also wish to recognize Officer Cornelius Spellman and Master Sergeant John Veals for their invaluable commentary and support.

Contents

1	Introduction	1
2	What Is Identity Theft?	2
2.1	A Victim’s Story	2
2.2	Defining Identity Theft	4
3	How Is Identity Theft Committed?	6
3.1	Stealing Mail	7
3.2	Dumpster Diving	8
3.3	Lost or Stolen Purse or Wallet	9
3.4	Inside Jobs	9
3.5	Social Engineering	10
3.6	Computer and Internet Attacks	11
3.6.1	Viruses, Trojan Horses and Hacking, Oh My	12
3.6.2	Phishing: Where You Are The Fish	12
3.7	Skimmers	13
3.8	The Moral of the Story	14
4	What Is Done With My Information?	14
5	Who Commits Identity Theft?	16
5.1	Family and Friends	17
5.2	Employees	18
5.3	Organized Groups	19
5.4	Criminals: Getting Away With Other Crimes	20
5.5	Illegal Immigrants	20
5.6	The Straight Facts	21
6	Who Are The Victims?	22
6.1	Victim Statistics	23
6.2	Not Safe Even When You’re Dead?	25
7	Effects On Victims	25
7.1	Financial Effects	26
7.2	Emotional Effects	27
7.3	Time Is Not On My Side	28
7.4	So, Can Somebody Help Me?	29
7.5	Police Are Ill-Equipped To Handle The Problem	30
7.6	Psychological Ramifications	31
7.7	WPI Community Example	31

8	Problems With The Current System	34
8.1	Lack of Authentication	34
8.2	Aren't Businesses Losing Money?	36
8.3	Are Companies Preying On Fear?	37
8.4	What Is The Government Doing To Protect Consumers?	38
8.4.1	Laws That Address Identity Theft	39
8.4.2	Prosecution Difficulty	40
8.5	A Need For Education	41
9	Looking For A Solution	42
9.1	Problems Within The Current System	42
9.2	The "Central Authority" Solution	43
10	NIST Solution: The Big Picture	44
10.1	What Are These Four Levels?	46
11	The OMB Standard	47
11.1	Is This Assessment Really Sufficient?	49
11.2	Why Identities Must Be Guarded By A Level Four System	50
11.3	Why Identities Do Not Have to Be Guarded By a Level Four System	51
11.4	Final Thought on Evaluations	51
12	Registration	51
12.1	Remote Registration: Simplicity Versus Risk	52
12.2	Telephone Manipulation	54
12.3	Our Decision	54
12.4	Final Thought on Registration	55
13	Tokens - Definitions	55
13.1	Hard Tokens	56
13.2	Soft Tokens	57
13.3	One-Time Password Device Tokens	57
13.4	Password Tokens	58
14	Tokens - An In-Depth Look	59
14.1	A Locked Key: What's Inside of a Token?	60
14.2	Manipulating Hardware Tokens	60
14.3	Unlocking a Hardware Token	63
14.4	Soft Token: Eve's Objective	64
14.5	Supplementation: The Difference Between Level Two and Three	64
14.6	Hijacking: Open the Door, Then I Knock You Out	66

15 Authorization - Putting Registration to Use	66
15.1 Generic Process at Each Level	66
15.2 The Expectations of Registration	67
16 Putting NIST To Work: An Application	68
16.1 The Wallet of the Future	69
16.2 How Is This Wallet Being Used?	70
16.3 Benefits of This New Wallet	71
16.4 Security Risks of the Wallet	71
17 Concluding Statements	72

List of Figures

1	Number of Identity Theft Victims Per Year from 1998-2003	23
2	Amount of Money That All Victims Contacted By The FTC Had To Pay As A Result Of The Crime	27
3	Amount of Time That All Victims Contacted By The FTC Had To Spend Resolving Their Problem	29

List of Tables

1	Breakdown of How Personal Information Was Obtained By Victims in 2004 . .	7
2	Percentage of Victims Having Existing Account Misuse Prior to 2003	15
3	Percentage of Total Victims Prior To 2003 Open New Accounts	15
4	Percentage of Victims Prior to 2003 that Have Had Non Financial Fraud	16
5	Percentage of the Population Who Were Victims of Identity Theft Based on Level of Education	24
6	Maximum Potential Impact for Each Assurance Level	48

1 Introduction

Identity theft has been classified as the crime of the 21st century. With the amount of victims reaching nearly ten million Americans in 2003 and growing at an exponential rate, it is hard to argue against the severity of the problem. These millions of Americans that become victims are not only financially affected by this crime but are often emotionally damaged as well. The reason for the startling growth of this crime is that it is easy for any crook to commit it. One must merely acquire the personal information of a victim. There are a variety of methods available to obtain this sensitive information that range from the highly technical to the ridiculously simplistic. One does not have to break into a company database to acquire personal information, but can merely steal somebody's mail or even their trash.

It is apparent that industry is moving toward using the NIST recommendations as an authentication solution. While a system based on the NIST proposal contains flaws, such as in its remote registration procedures, evidence will be presented that suggests that this new system can provide consumers with a lower risk of being identity theft victims. Moreover, strong cryptography can be used in this new system to even further reduce the possibility that consumers can become victims. However, even under the NIST solution, the possibility still exists for an individual to become an identity theft victim. In particular, without proper education, many Americans can still be duped into being victimized. As will be shown, while identity theft is partially a cryptographic problem, other components, such as consumer education, can be attributed to the recent growth of the crime.

A system that uses some of the recommendations made from both the central authority model and NIST Special Publication 800-63 could prove to be the most effective in combating identity theft. It is apparent that electronic wallets are being introduced as possible deterrents to identity theft. A system that effectively safeguards the electronic wallet with cryptography and eliminates paper mail containing sensitive information can significantly decrease the identity theft problem. However, like all crimes, identity theft might never be fully stopped and, even under a system using electronic wallets, consumers must be properly educated about how

to properly safeguard the new technology. Thus, with an increase in education and the development of better authentication protocols that incorporate cryptography, the growing epidemic can be hindered.

2 What Is Identity Theft?

It seems that almost every day there is either an article in the newspaper, a segment on a television program or a commercial that deals with identity theft. While identity theft seems to be the popular crime to discuss, it is rather difficult to determine what actually constitutes identity theft. In order to grasp an understanding of what identity theft is, it would prove beneficial to look at the misfortune of one of the many victims across the country.

2.1 A Victim's Story

California native Joe Zicaro is one of the many Americans who has been a victim of identity theft. Zicaro first learned that he was a victim of this crime on July 16, 1999. On this fateful day Joe was contacted by a Sears retail store because a man attempted to obtain a duplicate of his store account card. As a result of this attempted account takeover, Zicaro contacted the three major credit bureaus (Experian, Equifax and TransUnion) to investigate any possible damage to his credit by this thief. After learning that a criminal had applied for a cellular phone in his name, Zicaro decided to place a fraud alert on his report. This fraud alert, in theory, calls for the credit bureaus to contact him whenever a new account is applied for using his information. As a result of this service, Zicaro can then stop fraud from taking place although a thief has his personal information [38].

However, this fraud alert was not placed on Zicaro's credit report immediately. Joe was unable to talk to anybody at Experian and was left to file his request for a fraud alert on their automated system. After various letters and faxes, Experian eventually placed the alert on Zicaro's credit report over a month after his initial request. Moreover, while a fraud alert was

placed on his report by TransUnion and Equifax, all creditors did not take the appropriate actions and normally processed transactions involving Zicaro's information. The thief, even with this service that Zicaro utilized, was still able to commit identity theft as a result of the improper actions of the credit industry [38].

While Zicaro learned that unauthorized accounts were opened in his name, the extent of the damage done to his credit was truly devastating. A thief purchased various items and paid various bills using a checking account opened using Zicaro's information. Zicaro later determined that the imposter had written approximately 200 checks on that account when those checks began to show up in his credit files as collection accounts. Adding up the amounts of the bad checks with the charges on other fraudulent accounts, the total amount of money that the thief was able to steal from Joe was more than \$44,000 [38].

If the financial damage done to Zicaro was not severe enough, the emotional impact of the crime was just as devastating. For instance, Zicaro found little help with law enforcement. Joe first turned to Sacramento law enforcement for help but they stated that they could not do anything because the crimes were being committed in Los Angeles. Then, when Zicaro turned to Los Angeles authorities for help, they again did not want to help him because he lived in Sacramento. Furthermore, when Joe turned to the FBI for help, they simply stated "...our investigative guidelines... do not allow us to investigate allegations of criminal activity where the loss is less than \$50K." Also, despite proving that he has been a victim of identity theft, Joe still finds himself spending countless hours trying to fix his credit report and proving to various agencies that he is innocent of assorted fraudulent activities that the thief committed [38].

The ordeal that Joe Zicaro went through is just one of the many examples of identity theft. Sadly, there are even more severe cases of this illegal activity that involve greater monetary costs and even false imprisonments. While Zicaro's example serves as a good case study of what identity theft is, it is important to actually define the crime.

2.2 Defining Identity Theft

Identity theft is a crime that has recently garnered great public attention. News and television magazine programs have reported many identity theft horror stories. Also several commercials have aired on television stations that involve identity theft. These commercials range from warning Americans to buy a shredder, lest they will face the perils of identity theft, to telling consumers that they can receive a free copy of their credit report once a year. There has even been a movie made about identity theft; The Lifetime movie “Identity Theft: The Michelle Brown Story,” details how easily an individual’s identity can be stolen and the financial and emotional effects that a victim experiences as a result of such a crime.

While identity theft has been discussed in numerous forms, no clear definition of what actually constitutes identity theft is present. Perhaps the most acceptable definition of identity theft can be found in one of the laws that deal with this growing subject. According to the Federal Identity Theft and Assumption Deterrence Act, identity theft constitutes:

“...knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law [17].”

While this law gives a broad definition of identity theft (proving that such a “transfer” has criminal intent attached could be difficult), identity theft crimes can typically be divided into three subcategories.

Financial Identity Theft

Dustin Johnson realized he was missing his wallet when he got home one night last July (2004). He thought it was at work, but when it wasn’t there the next morning, he retraced his steps in his mind and realized he must have dropped it at the gas station the night before. Like most people, his first reaction was to cancel his debit and credit cards. Johnson thought that was the end. But the personal information in his wallet – including his Social Security card – made him a target for identity theft. A \$6,000 credit card bill from Bank of America arrived in the mail about two weeks after his wallet was stolen [10].

The sad story of Mr. Johnson is an illustration of the first subcategory of identity theft: financial identity theft. Financial identity theft entails the perpetrator using personal identifying information to open new lines of credit (accounts that depend on the user's credit history, such as credit cards, loans, etc.) in the name of the victim. Examples of this type of identity theft involve the application for utilities, loans or credit cards in the name of the victim.

Criminal Identity Theft

Al Lopez, a truck mechanic from Orlando, logs his every move now. Someone stole his identity and made a fake commercial driver's license. "I have to write on the calendar if I was at home or at work because if someone is pulled over, I have to prove where I was when something happens," he said [36].

Mr. Lopez lives in constant fear that one day he will be accused of committing a crime that he did not commit. This type of situation manifests the second subcategory of identity theft: criminal identity theft. Criminal identity theft refers to the situation in which a criminal gives another person's private identifying information in place of his own to law enforcement. For example, this type of identity theft would occur if a person was pulled over by the police for some motor vehicle infraction and gave the information of Mr. Lopez instead of his own.

Identity Cloning

Mary Frank, a licensed attorney and identity theft expert, became interested in identity theft as a result of becoming a victim of the crime. Frank had over \$50,000 in credit stolen from her. While this financially loss would seem bad enough, ever more devastating the assailant started to actually live as Mary Frank. More specifically, the criminal began to practice law using the information of Frank [12].

The ordeal that Mary Frank was put through serves as an example of the final subcategory of identity theft: identity cloning. Identity cloning occurs when the perpetrator uses the victim's personal information to establish a new identity. Identity cloning refers to the situation in which a criminal actually lives as the victim [20].

3 How Is Identity Theft Committed?

Identity theft occurs when a thief obtains a piece of personal information about an individual which then can be used to commit a form of fraud in the victim's name. A thief can use several methods in order to procure the sensitive information that can lead to eventual identity theft. These methods range from the highly technical, such as hacking into a database, to the highly simple, such as stealing an individual's mail. Table 1 contains the latest breakdown on how personal information was obtained from victims in 2004.

How Personal Information Was Obtained From Victims in 2004	Percentage of Victims
Lost/Stolen wallet, checkbook or credit card	28.8%
Accessed as part of a transaction	12.9%
Friends/Relatives/Acquaintances	11.4%
Corrupt Employee	8.7%
Stolen Paper Mail/Fraudulent Change of Address	8.0%
Computer Spyware	5.2%
Dumpster Diving	2.6%
Computer Virus/Hackers	2.2%
Phishing	1.7%
Other Methods	7.4%
Unknown	11.1%

Table 1: Breakdown of How Personal Information Was Obtained By Victims in 2004 [21]

3.1 Stealing Mail

The United States Postal System has been instrumental in uniting citizens across the country and the world. However, this system that has done so much good is now a chief source of personal information that thieves can use to commit identity theft. Often, mailboxes are not properly locked or secured. Hence, anyone walking down the street can simply open a mailbox and take its contents without the proper owner of the mail being aware. A thief can easily look through an unsecured mailbox for pre-approved credit cards, bills and bank statements and use the information to commit identity theft. In particular, the amount of credit card offers that Americans receive is staggering. On average, each household receives eight credit card offers a month [22]. Each of these various offers can serve as the key that a thief needs to commit his next crime. Also, a thief can fill out a fraudulent change-of-address form at the post office or at credit card and utility companies to get mail and bills redirected to the thief's address or mail drop off point. Of all identity theft victims in 2004, 8% had their personal information obtained via mail fraud.

3.2 Dumpster Diving

Information containing bank account numbers, social security numbers and other such sensitive information is recorded and transferred on paper continuously. Not only do individuals possess vulnerable paper documents of their own sensitive information, but countless credit agencies and corporations have control over paper documents containing sensitive consumer information. The problem with these paper documents is that, once they are no longer needed, they are improperly discarded. Instead of shredding or using some other means to destroy these documents, people merely throw them into the trash. This leaves individuals vulnerable to what we call “dumpster diving”. Dumpster diving refers to the act of a thief looking through trash receptacles to find documents that can be used to commit theft. One might think it is illegal to look through somebody’s garbage but, as long as an individual is not trespassing onto private property, dumpster diving is perfectly legal. This notion was confirmed in the 1988 Supreme Court Case *California vs. Greenwood*. Police, by looking through the trash of Greenwood, a notorious drug dealer, obtained information about his illegal ventures. Even though the police did not have a search warrant, it was determined that anyone can obtain items from trash receptacles that are in public areas. The personal information of approximately 2.6% of all identity theft victims in 2004 was stolen by means of dumpster diving.

The problem of dumpster diving has caused for a provision to be included in federal legislation that deals with the destruction of documents. In the 2003 federal Fair and Accurate Credit Transactions Act (FACTA), there is a stipulation that states that documents containing personal information of consumers must be destroyed properly using a shredder before they are discarded. Moreover, the states of Wisconsin, California and Georgia have individual document destruction laws as a result of the growing problem [19].

3.3 Lost or Stolen Purse or Wallet

Stealing a man's wallet or a woman's purse in order to acquire their money and possibly use their credit cards is not a new phenomenon. What is a developing issue is that thieves are now stealing wallets and purses to acquire information to commit identity theft. Individuals often keep ATM cards with their respective PIN numbers, multiple credit cards, social security cards, driver's licenses, health insurance cards and other sensitive information on their person, because it is believed that these documents might be necessary safeguards for some unforeseen situation. Clearly, when a thief acquires another individual's purse or wallet, he has an abundance of personal information available to him. While one would typically believe that computer misuse would lead to the most incidents of identity theft, statistics show that the old-fashioned method of simply stealing someone's wallet is the method that thieves used the most to acquire someone's personal information. Almost 30% of identity theft victims in 2004 had their information obtained as a result of losing control of their wallet, checkbook or credit card.

3.4 Inside Jobs

Businesses collect personal information from individuals for legitimate reasons. However, employees can illegally obtain this information and use it to commit identity theft themselves or sell the information to someone else who will then commit identity theft. As we have seen, 8.7% of identity theft victims in 2004 had their personal information stolen by an employee.

As an example of an inside job scenario, forty people who banked with the Philadelphia Federal Credit Union had discovered that their credit histories had been stolen. Then, local criminals purchased more than 60 cars, worth almost \$2 million, using the credit of those who had their credit reports stolen. A certain Darryl Brown paid \$10,000 to a part time clerk at the bank, named Marpessa McNeil, to steal personal information of bank employees. The crimes that followed did not involve McNeil at all. It should be noted that McNeil was not

a professional thief who made a living selling the credit information of consumers. Rather, McNeil was a recent college graduate, with a degree in criminal justice, who simply felt that she was not making enough money [30].

3.5 Social Engineering

Yet another way to commit identity theft is via social engineering. Social engineering here refers to the practice of conning people into revealing sensitive data. Well-known hacker Kevin Mitnick shows in his book, *The Art of Deception*, that it is common for identity thieves to simply pretend to be someone that they are not and acquire information from unsuspecting victims. Often people are unaware of just how valuable the information that they possess is and are too willing to divulge that information to people. As an example of a social engineering scheme, Mitnick tells the story of an individual pretending to be a manager of a particular store in a video rental chain. The imposter contacted another store in the chain, claiming he was having difficulty verifying an account holder and asked the employee who answered the phone to reveal the holder's personal information. As easy as that request was, the thief was able to acquire the personal information that he needed to commit identity theft [25].

A more severe case of social engineering took place in February 2005. ChoicePoint, a Georgia based company, maintains personal profiles of nearly every American consumer. It then sells these profiles to employers, landlords, marketing companies, and even government agencies. Criminals posing as legitimate businesses were able to garner some of these private reports. Not all consumers affected by the breach of privacy have been notified. California is the only state that requires companies to notify individuals of such security breaches. As a result, ChoicePoint sent between 30,000 and 35,000 messages to California residents advising them to check their credit reports for potential fraud activities as a result of the breach [8]. As this case illustrates, while companies may implement great technological tools to safeguard databases containing personal information, thieves can still gain access to this information by manipulating the humans who are in charge of dispersing the confidential data.

Another variation of social engineering takes place frequently via the mail as criminals will send letters to dupe individuals into divulging their information. For instance, thieves may send letters claiming that a person has won a cash prize or that they are needed to make a donation to a charity. No matter the content of the letter, the aim of the criminal is to use any means necessary to garner the information that they desire. One of the more popular cons is the “Nigerian Scam.” The following is a description of the scam presented by the Federal Trade Commission:

“Claiming to be Nigerian officials, businesspersons or the surviving spouses of former government honchos, con artists offer to transfer millions of dollars into your bank account in exchange for a small fee. If you respond to the initial offer, you may receive “official looking” documents. Typically, you’re then asked to provide blank letterhead and your bank account numbers, as well as some money to cover transaction and transfer costs and attorney’s fees. You may even be encouraged to travel to Nigeria or a border country to complete the transaction. Sometimes, the fraudsters will produce trunks of dyed or stamped money to verify their claims. Inevitably, though, emergencies come up, requiring more of your money and delaying the “transfer” of funds to your account; in the end, there aren’t any profits for you to share, and the scam artist has vanished with your money [17].”

Thus, the aim of social engineers is to use any means necessary to garner the information that they desire. Whether it entails using the telephone or a mere mail scam does not matter as long as the desired results are obtained.

3.6 Computer and Internet Attacks

Initially, when one thinks of how personal information is obtained, attacks involving computers are generally believed to be the primary methods used by thieves. However only 9.1% of identity theft victims had their personal information obtained via computer-related activity in 2004 [3]. While computer related breaches are not as common as one would initially believe, it is still important to understand the methods that thieves can use to acquire personal information via the use of a computer.

3.6.1 Viruses, Trojan Horses and Hacking, Oh My

Most internet users have been given a lecture regarding computer safety, vis-à-vis the compromise of sensitive information, in some shape or form (even if it is in the weak form of a “usage policy” they agree to when signing up). While internet users are warned of the dangers of downloading unsolicited material or visiting unheard of sites, users still practice unsafe computer behavior. As Kevin Mitnick states,

“All of these actions-downloading software you learned about from an advertised email, clicking on a link that takes you to a site you haven’t heard before, opening an attachment from someone you don’t really know, are invitations to trouble. Sure, more of the time what you get is exactly what you expected, or at worst something disappointing or offensive, but harmless. But sometimes what you get is the handiwork of a vandal [25].”

The handiwork that Mitnick is referring to is either a computer virus or a Trojan Horse. A Trojan Horse, in terms of computers, is an otherwise useful or entertaining program that contains malicious code that is designed to damage a victim’s computer. In particular, some Trojan Horse programs are designed to hide in the operating system of a computer and spy on every key stroke and function that the computer implements. As a result of such harmful programs, thieves can essentially spy on infected computers and obtain the personal information that is necessary to commit identity theft. Moreover, there are some instances where a perpetrator can gain total control of an individual’s computer or even “hack” into a company database that contains a cache of personal information of various consumers.

3.6.2 Phishing: Where You Are The Fish

Thieves often portray themselves as popular companies such as eBay, PayPal or banks and send out fake email messages to various consumers. In these email messages, customers may be told that their account has expired or needs to be verified, that a security breach has happened in the company or even that they can claim some exclusive member’s benefits. In all of these various instances the email directs the consumer to a fake web page that asks customers to provide sensitive information. Once consumers enter their information, it gets

sent to a criminal and the result is all too familiar.

This type of internet scam is referred to as phishing because, like real fishing, thieves continuously send out waves of these messages knowing that someone will eventually take the bait. According to a study by Gartner Inc., a Connecticut-based research and analysis company, more than 57 million Americans received phishing e-mails last year. Also, almost 2 million Americans actually fell for the scam and gave away their sensitive information [6].

3.7 Skimmers

Criminals may also possess a device referred to as a skimmer and use it to collect sensitive data. A skimmer is a device that resembles a pager or a cellular phone in size. A skimmer will store the data on the magnetic strip on the back of a credit or ATM card when a card is swiped through it. The information that is stored on the skimmer can then be downloaded onto a computer or even transferred onto a blank card. The restaurant industry is especially vulnerable to skimming. The reason for this vulnerability is that the restaurant sector is one of the very few places where customers are separated from their credit card when payment occurs.

The manner in which a skimming scam typically works at either a restaurant or retail store is that a thief who possesses a skimmer will first approach an employee. Restaurant and retail workers generally feel that they are underpaid. As a result, a thief will offer usually between \$20 to \$50 to an employee for each card that they swipe through then skimmer. Then, criminals will use the information from the skimmer to commit identity theft and move on to another community to start the scam again.

Skimming scams are not merely limited to the restaurant business. For instance, in July 2002, Benjamin Driscoll of Delray Beach Florida accidentally uncovered a skimming scam. Driscoll travelled to his local bank and proceeded to make use of their ATM machine. Upon swiping his card and entering his PIN, the message on the machine stated that his transaction could not be processed. Driscoll tried again and received the same message. However, Driscoll noticed that there was something peculiar about the way the ATM machine looked. Driscoll

tugged on the machine and a skimming device fell into his hand. The device was merely attached, with Velcro, over the normal ATM slot [30].

3.8 The Moral of the Story

There are countless ways that thieves can obtain the personal information of individuals in order to carry out their devious crimes. However, it is widely reported in media outlets and commonly believed by consumers that computers are the cause of the recent surge in identity theft. It is believed that online banking, shopping and other such computer transactions are easily vulnerable to attacks by thieves. Statistics show, however, that of identity theft cases in 2004, 68.2% of victims had their information obtained offline while just 11.6% of victims had their information obtained online. Thus, computers are more secure at safeguarding personal information than one would initially suspect [21]. While computers are not the chief resource that a thief uses for acquiring the personal information of victims, they play a very important role in the identity theft problem. Thieves are able to acquire new accounts, in the name of victims, over the internet. It is already readily apparent that a partial reason why identity theft is such a severe problem is a result of the ease that the personal information of Americans can be obtained.

4 What Is Done With My Information?

New scams and techniques are continuously being devised to steal information of Americans. With personal information obtained in one or more of the previously described ways, a thief is able to commit fraud in the victim's name, and start to do the real damage. An avenue often taken at this point is to use what structures are in place already: the thief misuses one or more of the existing accounts of a victim. For instance, a criminal could take over the existing credit card of a victim or even use a victim's telephone service. This type of fraud was reported by 85% of all identity theft victims. The percentages of all victims that have had

Existing Account Misused	Percentage of All Victims (Prior to 2003)
Existing Credit Card	67%
Checking/Savings Account	19%
Telephone Service	9%
Internet	3%
Insurance	2%

Table 2: Percentage of Victims Having Existing Account Misuse Prior to 2003
[33]

Type of Account Opened	Percentage of All Victims (Prior to 2003)
Credit Cards	8%
Loans	5%
Telephone Services	5%
Checking/Savings Account	3%
Internet	2%
Insurance	1%
Other Accounts	1%

Table 3: Percentage of Total Victims Prior To 2003 Open New Accounts
[33]

various existing account misuse is conveyed within Table 2. The Federal Trade Commission compiled these results within a report issued in 2003. As well, an identity thief can use the personal information of a victim to open a new account in the victim's name. For instance, the personal information of a victim can be used by thieves to open credit card, utility and even loan accounts in the name of victims. Among all identity theft victims, 17% said that a thief has used their information to establish a new account in their own name. Table 3 shows a breakdown of the percentage of victims that have had one of the various accounts opened in their name. Again, these statistics were obtained from a 2003 FTC report. While it is common for an identity thief to use the personal information of a victim to commit fraud for monetary gain, there are instances when thieves commit fraud for other reasons. According to the Synovate report, 15% of all identity theft victims reported that the identity thief used their information in nonfinancial ways. This means that a thief could use a victim's information to obtain a driver's license or even employment. Moreover, a thief can even give the information of one of their

Type of Non-Financial Fraud Committed	Percentage of Total Victims (Prior to 2003)
Committing Crimes	4%
Obtaining Government Documents	3%
Rent Housing	2%
Medical Care	2%
Employment	2%
Tax Returns	2%
Other Misuse	7%

Table 4: Percentage of Victims Prior to 2003 that Have Had Non Financial Fraud [33]

victims when they are caught committing a crime. This usage would most likely occur when the criminal is on some form of probation or parole. If their “true selves” were apprehended, the punishment would be far worse than the normal statute. Table 4 gives a breakdown of the percentage of total identity theft victims that have had various forms of non financial fraud committed in their name.

5 Who Commits Identity Theft?

Commonly, identity thieves are perceived to be nameless faces that are well-educated individuals. Like all crimes, motive and opportunity are necessary, as well as criminal intent: that force that enables individuals to disregard the law for personal benefit. This notion of diversity in criminals is even more prevalent in identity theft because identity theft is a low-risk crime. An identity thief can be anyone from a computer savvy teenager to a convicted felon or an organized criminal group or even a coworker or family member. Furthermore, one is not required to have a certain level of intellect to commit identity theft. Computer hacking knowledge or technological devices such as skimmers are not necessary for an identity thief to be successful. Stealing credit information from a mailbox is just as effective as hacking into the credit information of a major bank. Thus, while there is no characteristic type of individual, it can be seen that identity thieves typically fall under one, or more, defined categories, which we will now

describe.

5.1 Family and Friends

Over a three year period, Florida resident Kelli Pasqualetti-Heller began to receive letters from collection agencies demanding payment for numerous outstanding utility bills. Furthermore, she was receiving demand letters from furniture companies and delinquency notices from the IRS for back taxes. However, these demand notices were not addressed to Ms. Pasqualetti-Heller. Rather, they were addressed to her eleven year old son who was suffering from cerebral palsy. After conducting her own inquiries and hiring a private investigator, Pasqualetti-Heller discovered that her son had had his identity stolen by his own father. The young boy's father was using his son's Social Security number to make purchases [30].

As the story of this Florida family shows, identity theft is not just committed by nameless faces that may be sitting behind some distant computer. It is entirely plausible that an identity thief might be a family member. A report issued by the Federal Trade Commission stated that in approximately nine percent of all identity theft cases a family member or relative was the perpetrator. This means that as many as 900,000 individuals were victimized by their own family last year. This trend of family members committing identity theft has become so alarming that the national television show 60 Minutes gave a report, entitled "All in the Family," chronicling the national problem.

The report chronicles the story of Abigail Kelly, who had her identity stolen by her own sister, and "Lynn," a woman who had her identity stolen by her son. Moreover, the report chronicles the emotional effects that family identity theft has on individuals. While identity theft performed by a stranger causes a victim to become less trusting, when the assailant is a family member the emotional effects are even greater. As "Lynn" stated, "When it's a family member, especially a son or a daughter, it's like, 'if you can't trust your kids, who are you gonna trust?' They're a part of you." [9]. Besides family members, similar reports of friends and acquaintances committing identity theft are also prevalent.

5.2 Employees

On September 14, 2004, thirty-five year old Philip Cummings pleaded guilty to committing identity theft. What makes Cummings' story so unique is that he is a part of the largest case of identity theft in US history as a result of he and his fellow accomplices managing to steal over \$50 million. From mid-1999 through August 2000, Cummings worked as a help-desk worker at Teledata Communications, a Long Island-based computer software company that provides banks with computerized access to credit information databases. Cummings agreed to sell other co-conspirators the passwords and codes for downloading consumer credit reports and these co-conspirators, in turn, used the information in the reports to commit identity theft. Over 10,000 reports were stolen and Cummings agreed to sell these reports for approximately thirty dollars each [24].

Philip Cummings is just one example of an employee using secret company information to steal identities. The type of theft that Cummings was involved in is typically referred to as an "inside job", which are usually the starting points for all identity theft cases. In these type of thefts a person working in an industry with useful information will either sell the information to a criminal or use the information themselves to commit an identity theft. What is especially alarming about this type of attack is that an individual does not need to have an upper level position to be privy to information that is beneficial to thieves. For instance, entry level secretaries and receptionists in the bank and health care field have access to sensitive information of customers. Since access to these type of jobs require little education, in some instances organized crime groups have had members take these entry level positions in banks and health offices so that they are privy to this sensitive information.

According to a study by professor Judith Collins of Michigan State University, as much as 70 percent of all identity theft starts with theft of personal data from a company by an employee. Rob Douglas, an identity theft consultant in the banking industry, agrees with the assertion that insider theft is the primary problem. Douglas states

"There is always a lot of concern about hacking but the demonstrable number

of mass hacks pales in comparison to the easy old method of insider theft. It's a crime of opportunity. The information is right there. I always tell banks I talk to, information equals cash [30]."

As Douglas articulates, while attention is focused on individuals behind computers attempting to gain access to a database of beneficial information, it is much easier for an identity thief to co-opt someone with access to the sensitive information to get it for him.

5.3 Organized Groups

As discussed previously, identity thieves are not necessarily a sole computer hacker attempting to break into a database of company information. In most instances identity thieves are members of an organized group. These groups are known to make sophisticated and coordinated attacks and move from one community to the next. The "Collector-Converter-Passer Model" describes the manner in which these groups work. Collectors obtain information and sell it to converters. These collectors may obtain this information by stealing from mailboxes, going through trash or obtaining an entry level position in a field with sensitive information. Collectors can either be paid in cash or drugs for this information. For instance in March, 2004, an identity theft ring was discovered in Port Orchard, Washington, where collectors were instructed to steal mailboxes throughout the community and in return received methamphetamine for their work [31].

Next, converters take the information from collectors and convert the information into cash or other forms of monetary wealth. This is the part of the process where the identity of an individual is actually stolen. In instances where checks must be cashed or goods must be retrieved from stores, converters will have a passer do the work so they will not be put at risk by picking up the illegally obtained items.

5.4 Criminals: Getting Away With Other Crimes

In a small number of instances, criminals will use identity theft to get away with other crimes. According to a survey conducted by the Identity Theft Clearing House in 2000, 12 percent of identity theft victims found themselves burdened with wrongful criminal records [31]. The manner in which this type of identity theft works is that when criminals are arrested they will provide the identity of another person. Thus, the actual criminal will, in theory, be able to get away with his crime while an unsuspecting victim will be asked to appear in court. For instance, a man by the name of “Bryce Roland” was arrested and convicted twice for drunk driving. However, Roland never was in the state where the arrests took place. Roland did have his wallet, which contained his SSN, stolen by Edward Wolsiffer. Wolsiffer used Roland’s identity when he was arrested by the police for driving under the influence of alcohol [30].

Another, more humorous example of a thief attempting to commit crime in the name of a victim can be seen in the case of James Perry. James Perry received four drunken driving arrests in Florida. Since Perry felt it would be entirely too difficult to receive a driver’s license when he moved to Connecticut, he decided to assume the identity of his neighbor, Robert Kowalski. Using Kowalski’s name, Perry was able to receive a driver’s license and various credit cards. What seemed like the perfect plan was foiled when Perry was arrested for disorderly conduct. Upon giving Kowalski’s information, Perry was immediately surprised to learn that police accused him of being a convicted sex offender who do not properly register with the state. Hence, Perry, in the process of trying to hide his prior criminal acts, managed to steal the identity of a sex offender [13].

5.5 Illegal Immigrants

Identity theft is one of many tools that are used by criminals to commit illegal activities. One problem that has plagued America for years is illegal immigration. Whether it is an attempt to start a new life or the opportunity to perform criminal activity, countless foreigners

illegally enter America each year. In 2002, the Census Bureau estimated that 8.7 million people illegally resided in the United States. Of these illegal immigrants the Immigration and Naturalization Service (INS) reports that 40% are visa overstayers while the remaining 60% were never granted legal entry. With all of these illegal immigrants entering the country, many of them turn to identity theft not to steal money, but to obtain the necessary identification to garner employment, housing and other benefits of US citizenship [30].

Linda Trevino, who lives in the Chicago area, was a victim of identity theft at the hands of an illegal immigrant. In 2004, Trevino applied for a job at a local Target department store. Much to Trevino's dismay, she was rejected. The reason for her rejection was that the chain informed her that she already worked at the store. As Trevino later discovered, an illegal immigrant had stolen her social security number and other personal information to garner employment at the store. Even more disheartening, thirty seven additional employees used used Trevino's information to garner employment at various other stores.

Trevino's tale is just one instance of the hundreds of thousands of victims who face this type of fraud annually. What makes illegal immigrants stealing an identity even more damaging to victims is that, like in Trevino's case, multiple illegal immigrants sometimes share the same information. According to James Lee, a chief marketing officer for private data collection firm ChoicePoint, the average victim of immigrant-based identity theft sees their Social Security number shared about 30 times. This sharing of one identity is common for illegal immigrants residing in tight-knit communities. Illegal immigrants can obtain these identities either via the previously described methods or, as in most cases, they will pay for the information for the information, which is readily available from higher-level criminals [32].

5.6 The Straight Facts

Usually, when someone is preached to about potentially being the victim of a crime, their basic instinct is to think that the crime can never happen to them. While it may be comforting to think that identity theft is something that can be dismissed, this is sadly not the case. According

to the National Crime Prevention Council, identity theft is the fastest growing crime in the United States. In the year 2003 alone, 9.91 million Americans were victims of identity theft. This represents 4.6% of the total population of American adults. This means that in a room full of twenty adults, one person will have been the victim of identity theft [33].

Moreover, identity theft is not a crime that has just started taking place in the year 2003. Within the five year period of 1998 to 2003, approximately 27 million American adults have been victims of this growing crime. Figure 1, which contains information from the Federal Trade-Commission Identity Theft Survey, shows the breakdown of how many Americans have been victims of identity theft each year. As the chart shows, the number of identity theft victims has increased every year, with the number of victims rising dramatically in 2003 and 2002. In particular, 26% of all identity theft cases took place in the year 2003. This amount matches the total number of cases that took place prior to 1998. It should be noted that the total number of identity theft victims is based on the results obtained by a FTC report in which surveys of living Americans were taken. Also, the number of incidences that took place in 2003 is nearly three times the amount of incidences that took place in 2001, and nearly 33% greater than the amount of incidences that took place in 2002. It is not unreasonable, therefore, to project exponential growth in this phenomenon barring some dramatic change in practices.

6 Who Are The Victims?

Clearly identity theft is growing at a rampant rate. Common belief indicates that identity theft only affects the extremely wealthy. It is true that several celebrities have had their identity stolen. Robert De Niro had his identity stolen by a man who played his movie double. Warren Buffet, Oprah Winfrey, Stephen Spielberg, Martha Stewart, Paul Allen, Michael Bloomberg and Ted Turner all had their identity stolen by a New York busboy named Abraham Abdallah. Even movie star Will Smith and basketball legend Michael Jordan were victims of this growing crime [30]. While these incidents involving celebrities reinforce the common belief that iden-

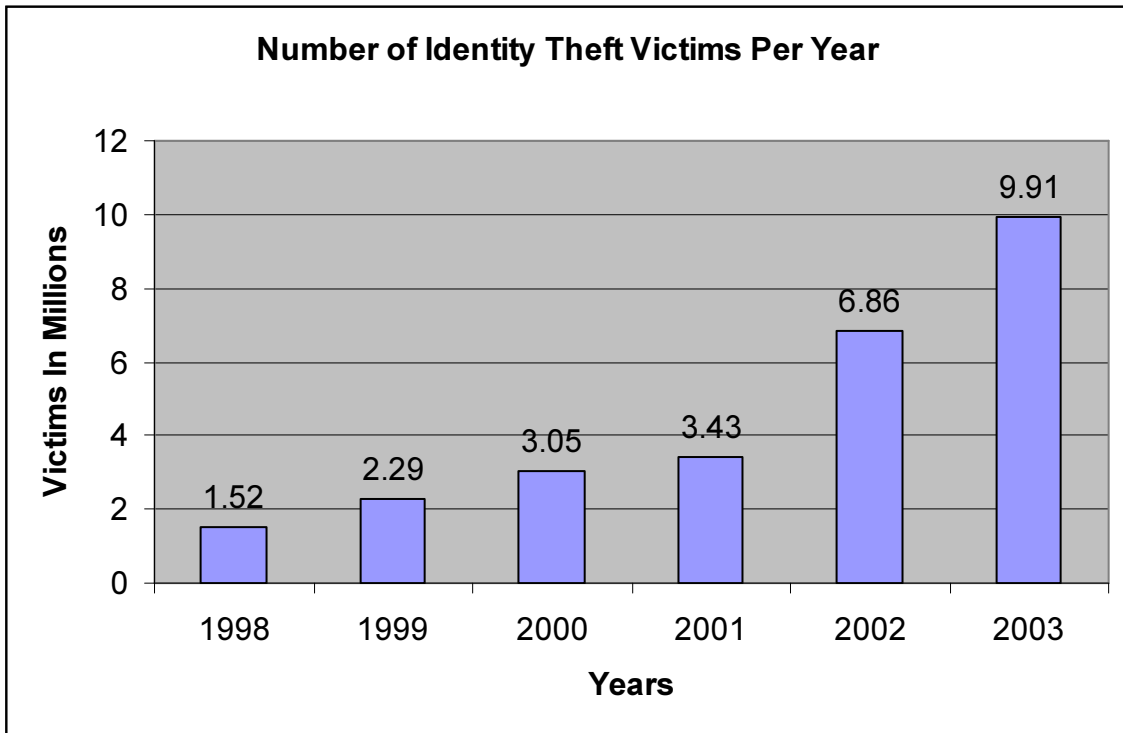


Figure 1: Number of Identity Theft Victims Per Year from 1998-2003
[33]

tity theft is a crime reserved for the wealthy elite, the actual statistics (obtained from a report by the Privacy & American Business in 2003) show that identity theft is a crime that affects people of all ages, of all income groups and of all races.

6.1 Victim Statistics

Identity theft is a crime that impacts adult Americans from all demographic groups. In 2003 an extensive study about the number of identity theft victims in America was conducted by Harris Interactive to prove this idea. According to the study, 33.4 million Americans (or 16% of the population) have been a victim of identity theft. In terms of race, 20% of African Americans, 15% of Caucasians and 22% of Hispanics living in America have been victims of identity theft. While there are slight variations, it is clear that the percentages of cases based on race are relatively close. This idea is further asserted in regards to age. The highest incidences of identity theft were reported in the 30-39 age group at 20%. Of all Americans between 18 and

Level of Education	Percentage of Americans That Were Victims of Identity Theft
High School or Less	12%
College Degree	17%
Post-Graduate Degree	22%

Table 5: Percentage of the Population Who Were Victims of Identity Theft Based on Level of Education

[2]

24, 10% were victims of identity theft. Moreover, 16-17% of Americans between 25 and 29 and adults over 40 were victims. The percentages of victims are very similar for all American adults over 24, again asserting the notion that identity theft affects everyone [2].

American adults are not the only potential target for identity theft. Approximately two percent of identity thefts involve children [30]. This means that approximately 750,000 children have had their identity stolen. For instance, when sixteen year old James Thibodeau went to get his learner's permit, an exciting milestone in the teenager's life was turned into a nightmare. Thibodeau was not allowed to receive his learner's permit because someone already obtained a license in his name. To make matters worse, James was told that he owed over five thousand dollars in back child support for a twelve year old son. It turned out that James had his identity stolen by not one but two criminals. One of those perpetrators was his own father [1]. The correlation between how much money an individual makes and the chances that he will become a victim of identity theft must be examined. Of those making more than \$75K per year, 20% have been victims. On the contrary, 14-16% of individuals in lower income groups were victims. While those who make over \$75K are more susceptible to being identity theft victims than those who make less money, the difference is not as dramatic as one might initially think. Next, the degree of how educated a person who is a victim of identity theft is can be examined. Out of all Americans with post-graduate degrees 22% have been victimized. Of those with college degrees, 17% had their identities stolen and 12% of those with a high school degree or less had their identity stolen [2].

When looking at the victimization statistics that are correlated to race, age, education and income, one can see that there are differences that can be used to determine a profile for a typical identity theft victim. Usually identity theft is believed to be a crime that is reserved for the wealthy elite. While it is true that those who have a higher education and garner a higher income are slightly more likely to be victims of identity theft, the similarity in statistics shows that identity theft is a crime that is likely to happen to any American adult.

6.2 Not Safe Even When You're Dead?

While statistics have been given on who is likely to become a victim of identity theft, it should be noted that thieves will steal the identities of deceased individuals as well. Notably, deceased victims of the terrorist attacks on September 11, 2001, have had their identities stolen. Another such instance took place last year. A woman by the name of Kwezeta Butler would scan the obituaries of newspapers and pay an internet search company to do background checks on the dead. Butler was able to obtain the personal information of eighty people from five different states. Then Butler would sell the information of these dead individuals, for \$600 per identity, to individuals with bad credit. Next, these crooks would list these deceased individuals as co-signers for cars at a dealership in Atlanta. In total one hundred car loans were taken out at this lone Atlanta dealership, with the loans totaling approximately \$1.5 million [34].

7 Effects On Victims

Citibank has recently issued an advertisement campaign directed toward identity theft and the company's policies in regards to the issue. In one of their television commercials, an elderly woman is seen cleaning her swimming pool. Then, when the woman begins to talk, her voice is that of a young man who has stolen her identity. The man begins to state how he has purchased a new truck but he is not worried because he does not have to pay for it [18]. While these Citibank commercials present identity theft in a fairly light manner, the effects that identity

theft has on victims is anything but humorous.

7.1 Financial Effects

The most obvious way that identity theft affects victims is financially. By looking at the FTC statistics of identity theft victims contacted in their extensive survey work, clear trends in the amount of money victims have to pay can be seen. For 63% of all identity theft victims, there was no loss of money out of pocket. The average amount of money that victims of identity theft pay to resolve their issues is \$500. While this is the average amount that all victims of identity theft pay for their out of pocket expenses, it is apparent that there is a distinct correlation between the type of identity theft that occurs and the amount of money that a victim has to pay to recover from the crime.

Figure 2 shows a breakdown of what percentage of identity theft victims had to pay various amounts of money out of pocket. In particular, the graph shows the monetary damages for three subcategories of identity theft: the misuse of existing credit cards, the misuse of other existing accounts and the creation of new accounts and other fraud. As the graph shows, individuals who experience identity theft that did not involve existing credit card accounts paid more money than cases that just involved existing credit cards. The average out-of-pocket expense for those who suffered from “new accounts and other frauds” identity theft was \$1,200. Another factor that relates to the amount of money that a victim has to pay in order to rectify their given predicament is the length of time that elapses before the victim realizes that their identity has actually been stolen. As one would suspect, victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses. No expenses were incurred by 67% of those victims who discovered the misuse less than 6 months after the fraud began. On the other hand, only 40% of victims who took 6 months or longer to discover the misuse were able to avoid incurring expenses [33].

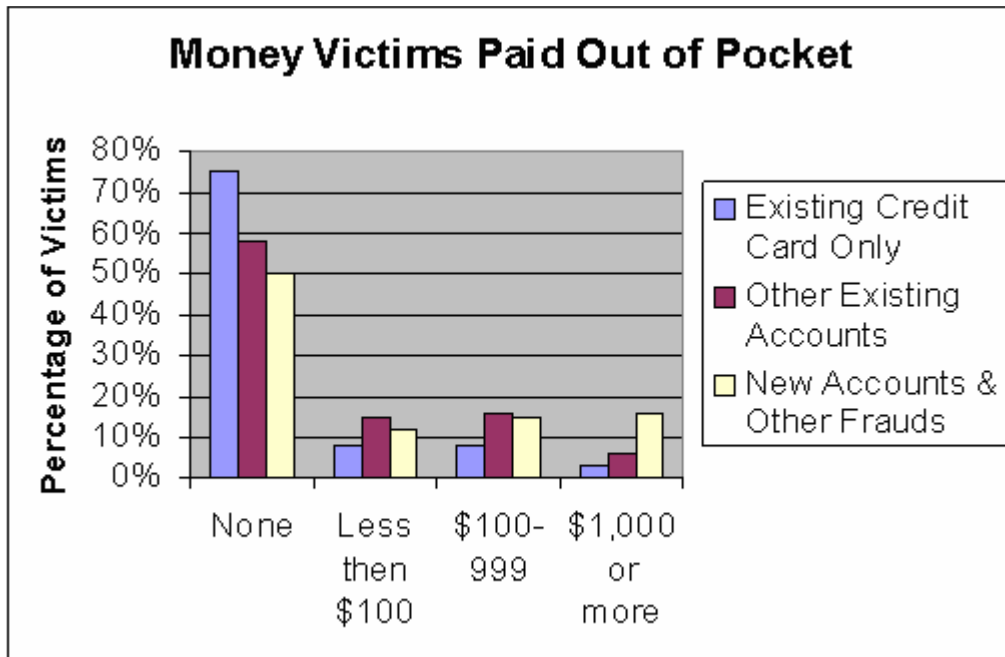


Figure 2: Amount of Money That All Victims Contacted By The FTC Had To Pay As A Result Of The Crime

[33]

7.2 Emotional Effects

The Federal Trade Commission (FTC) gives an easy four step process to follow when someone becomes a victim of identity theft.

- First, the victim is instructed to call the toll-free fraud number of any one of the three major credit bureaus (Equifax, Experian and TransUnion) to place a fraud alert on their credit report.
- Next, a victim is instructed to contact the various creditors with which they do business to close any accounts that have been compromised or opened fraudulently.
- Thirdly, a victim must file a report with their local police department. It is important that victims get a copy of the police report in case the creditors or credit bureaus need proof of the crime.

- Lastly, an identity theft victim is instructed to file a complaint with the FTC. The Identity Theft and Assumption Deterrence Act of 1998 established the FTC as the one central point of contact for victims to report all instances of identity theft. The FTC maintains a database of identity theft cases that can be used by law enforcement agencies for investigative purposes [17].

While the FTC presents resolving an identity theft case as some straightforward algorithm, the truth is that the aftermath of identity theft is an incredibly stressful ordeal. A victim must spend a tremendous amount of their own personal time to resolve the issue. Moreover, victims do not merely make one simple phone call to one organization and then the entire ordeal is over. Rather, several phone calls must be made to various organizations on more than one occasion. Lastly, the seemingly simple task of obtaining a police report is far more complicating than the FTC leads consumers to believe.

7.3 Time Is Not On My Side

While the financial aspects of identity theft are the easiest to quantify, the time and emotional effects of identity theft are just as critical. Figure 3 depicts the amount of time identity theft victims spend resolving their problems. The graph separates identity theft into the same three categories that were used in Figure 3. The average amount of time that a victim of identity theft must spend to resolve their problem is 30 hours. Out of all of the victims of identity theft contacted by the FTC, 35% reported that they were able to resolve all of their problems in one hour or less, 29% required 2 to 9 hours to resolve their problems and 30% of all victims spent more than 10 hours. In what are certainly the most extreme scenarios, 6% of all victims spent over 240 hours of their time working to resolve their problem [33].

However, the amount of time that a victim has to spend resolving their problem exhibits some correlation to the type of identity theft that is committed. It is apparent that those who

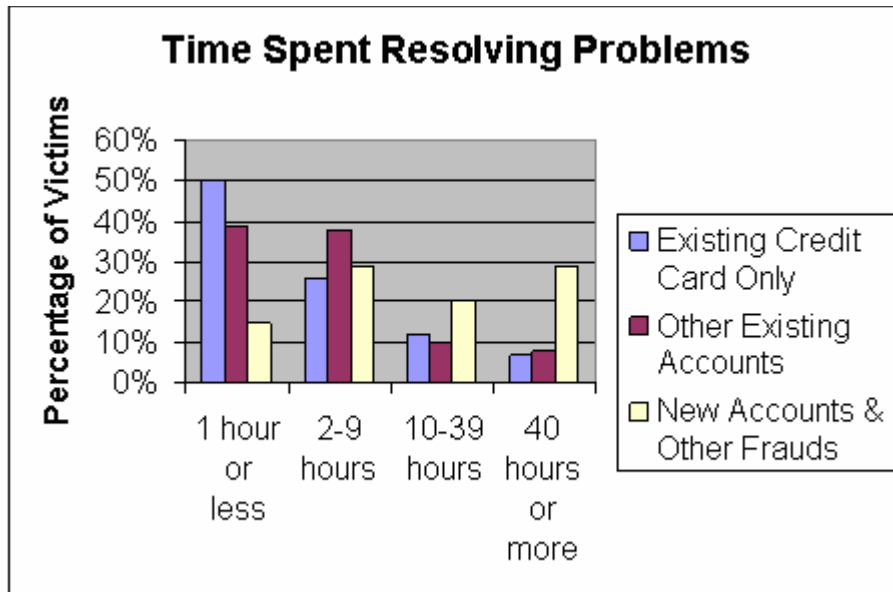


Figure 3: Amount of Time That All Victims Contacted By The FTC Had To Spend Resolving Their Problem

[33]

have an entirely new account opened in their names have to spend a greater amount of time than those who have just had one of their existing accounts tampered with. As Figure 7.2 displays, 49% of all victims that had a new account open in their name spent over ten hours to rectify their problem. To the contrary, only 18-19% of victims that had an existing account tampered with had to spend over ten hours to rectify their problem [33]. Thus, it is apparent that identity theft is not a crime that will be resolved without spending a substantial amount of time. While in some instances one may only need to spend a minimal amount of time to resolve one’s problem, often identity theft involves countless hours of work in order to return to a state of normalcy.

7.4 So, Can Somebody Help Me?

According to the FTC, all one has to do to solve one’s identity theft problem is make a couple of phone calls to credit agencies. As one would suspect, the countless hours of time that victims waste is as result of not being able to successfully contact these agencies. More-

over, consumers are bounced from one agency to another, often waiting on the phone to talk to an actual human. Then, once a victim gets to actually talk to an agency employee, they find that the agencies are not eager to help them but, rather, question the validity of the statements that they are making.

This frustrating process is seen in a 2003 study by the Identity Theft Resource Center (ITRC). According to the study, only 24% of victims were easily able to find contact information for these various agencies. Also, only 14% of victims report that the company representatives that they worked with treated them with respect. Moreover, 45% of victims reported that agencies refused to fix the actions of the identity thief despite the presence of evidence of such a theft. Hence, the easy process of contacting a couple of agencies to rectify the problem is nonexistent. The aftermath of identity theft is a stressful ordeal that involves countless hours of contacting uncooperative companies [20].

7.5 Police Are Ill-Equipped To Handle The Problem

A major source for turmoil for identity theft victims is their interaction with law enforcement. While the FTC says that filing a police report is instrumental in resolving an identity theft case, getting one filed is rather difficult. Since identity theft is such a new crime that transcends numerous jurisdictions, most agencies are unfamiliar with how to proceed with the cases. No more is this seen with statistics from a 2003 report from the ITRC. Of all victims contacted, 54% had to contact more than one police department to garner a report. Moreover, only 51% of victims received a police report on their first contact while a total of 26% of victims never received a report. Even more discouraging, 56% of victims contacted felt that they were bounced from one agency to another with no one willing to help them. This notion is further enforced by the notion that only 39% of victims ever had a detective assigned to their case. Clearly, police departments are ill equipped to deal with the identity theft epidemic [20].

7.6 Psychological Ramifications

Any victim of a crime has some form of psychological damage done to them as a result of the unfortunate incident. Similarly, the emotional turmoil that identity theft victims go through should not be made light. According to reports by the ITRC, 76% of victims are left with deep fears regarding personal financial security and a sense of helplessness as a result of the crime. Approximately 89% of victims were left in a state of rage and 54% of victims had trouble sleeping as a result of their ordeal. While these feelings diminished over time, it is clear that identity theft is not merely a crime that affects the credit score of an individual. Identity theft is a crime that changes the emotional dynamics of victims for the worse [20].

7.7 WPI Community Example

By examining a case study of a victim from WPI, the financial and emotional effects of identity theft can be seen. Master Sergeant John Veals, Jr. was the victim of identity theft during August of 2001. He believes that this was achieved by the loss of a credit card and other sensitive information from his wallet. The wallet, which was in his clothing, had been left in a gym locker room. Several days later, he discovered his credit card had been missing, at which point he called the credit company to cancel the card and see if there had been any fraudulent charges added. He also made sure to contact the owners of the establishment where the card was stolen and the police department.

MSG Veals found that there had been approximately \$4,000 in fraudulent charges issued on his credit card. Only 1.25% of these charges (\$50) were ever refunded. During the interrogation process (where authorities were collecting general information), he sensed that the police, for whatever reason, initially treated him as if he had either intentionally lost this piece of identification, or he was an accomplice to someone's plot to fraudulently use his identity. Regardless of this, John Veals was finally referred to an investigator proficient in scam artist cases, the best bureau at the time to deal with this category of crime. However, the slow pace

of the investigation was a disadvantage. After the interrogation, the authorities told him they would 'get right back to him'. While contacting his lawyer, it became necessary to acquire a copy of the police report, during which he was told that 'they were still looking into it', and they could not provide him with one. It seems clear for our study that this police department had no prior experience.

Moreover, whoever acquired John's credit card had tried to use his information to acquire new sources of credit. Fortunately for John, the criminal failed in accomplishing this since John had contacted the appropriate sources to place a fraud alert on his credit report. According to Veals, there are several features in place to try and apprehend these thieves. For instance, there are surveillance cameras hidden within establishments and there are faster credit checks that companies can choose to utilize. While these features are in place, they still do little to help apprehend suspects. For instance, while a store camera could have taped Veals' culprit, most stores only keep archives of their tapes for 72 hours. Consequently, these tapes that could have potentially depicted Veals' culprit were gone by the time police began their investigation. Unfortunately, the person who stole Veals' identity was never arrested.

Once the criminal investigation was in the hands of law enforcement, John was faced with the logistical and financial aftermath of the crime. Veals had to go through the process of changing his social security number since it was compromised by the thief. This required that he retain a lawyer, costing him eventually \$5,600. Just like the scam artist detective, this lawyer seemed new to the territory yet proficient in the realm of identity theft; he knew the exact channels and proper procedure for this complicated but necessary task. Veals and his lawyer contacted the Social Security Administration, with police investigation report and credit union paperwork in hand. This information was necessary to prove that this change needed to take place. Also, Veals had to go through the process of notifying the military administration, since bases still use SSNs heavily for internal identification. Everything in his life linked to the Social Security Number had to be reviewed or altered. Like the police, the lawyer had no direct experience with this crime, but he was good at getting things done inside the credit bureaus and Social

Security Administration. After this ordeal, his lawyer hoped ‘this would never happen to me’ as a result of seeing the hassle of what needed to be done to rectify an identity theft case.

To this day, Major Sergeant John Veals is very cautious when it comes to his identifiers. A credit report cannot be obtained in his name by anyone, such as banks and home brokers, without his written notification. This service was recently triggered when his daughter, taking residence in Boston to attend Northeastern university, required her parents as co-signers on a lease. As a result of this crime, Veals only carries a credit card when he knows that he will be using it. Furthermore, anytime he needs a credit card he brings only one, not four like he used to. Moreover, Veals has written a “See I.D.” notification on the reverse side of all credit cards that he owns. Anyone accepting a credit card as a form of payment is expected to check that it is signed, and that the signature on the card matches the one given on the receipt. Since his ordeal, Veals says he and his wife scold any cashiers or businesses who accept the credit card without checking the reverse, and then subsequently request a form of identification to report the cashier for improper actions. Veals told us that he bought each of his college-aged children paper shredders as birthday gifts and insists they destroy all important paperwork when it is discarded. He himself collects the pre-approved credit cards he receives in the mail, and then posts them “Return To Sender” when he has amassed enough. Usually, after having to pay postage twice, the company no longer sends this risky mail.¹

Master Sergeant John Veals, Jr. says that total man-hours spent on this were 4 hours per day, 5 days per week, for the course of three months, totaling 240 hours. Veals felt that the inconvenience of the ordeal was most painful (although in his case, repaying the fraudulent charges and retaining a lawyer were costly consequences as well.) He said, “The process is really frustrating.”, especially the phone interactions. Often he was transferred, re-transferred, and forced to leave voice mail messages at several ends. Clearly, the ordeal of Veals experienced illustrates the notion that identity theft can affect anyone and, while the financial costs

¹This is a slower type of education, but we feel it’s this brand of reinforcement that will eventually get people to realize the importance of verification of in-person forms of payment Furthermore it shows how much Veals and his family have been affected by this ordeal.

of the crime are the most tangible to outsiders, in actuality the emotional ramifications of the crime are perhaps even more devastating.

8 Problems With The Current System

So far we have tried to shed light on the mechanics of ID thefts and its effects on Americans, both statistically and through anecdotes. The typical mechanics are as follows. A thief will first obtain a piece of personal information, in one of several ways, and then use that personal information to perform fraud in the name of the victim. Now, two chief questions remain to be answered. Firstly, why can someone commit identity theft simply by acquiring a piece of information about a person? Secondly, what is currently being done to remedy the problem?

8.1 Lack of Authentication

One reason Americans are so susceptible to identity theft is that companies use insufficient authentication techniques. Authentication refers to a protocol that a business follows to confirm that a person is who they actually say they are. There are several generic classifications of authentication technologies. First, there is the notion of shared secret authenticators. “Shared secret authenticators” is a rather fancy name that refers to the conventional username and associated password practice. Next, there is the potential use of hardware or random password tokens. These are physical, hardware devices that a user must have possession of in order to be authenticated. Hardware and password tokens will be discussed in more detail later in the document. Third, biometrics can be used as a form of authentication. Biometric technologies identify individuals by some unique physical characteristic. For instance facial features, fingerprints or even the sound of someone’s voice can be used to authenticate the identity of an individual. It should be noted that the use of biometrics is a controversial subject that evokes privacy issues that are far beyond the scope of this project [3].

While these various forms of authentication exist, creditors seem currently to assume that

the person applying for a new account is the same person whose name and personal information are used in the application. The way that a creditor authenticates an applicant for credit is by matching personal information provided in the application to information contained in a credit report. The information that is matched includes such items as a consumer's name, social security number, date of birth and address. If there is a match on at least a few items of information, it is assumed that the person is sufficiently authenticated [28].

Under the current system, it is easy to be authenticated for any transaction. The obvious drawback to such a system is that consumers are more susceptible to identity theft with such lax procedures. On the other hand, there are benefits for consumers under the way that the current system is structured. Consumers are able to obtain new credit cards, mortgages and bank accounts without having to provide an array of documentation or tokens to prove their identity. Americans are constantly busy and generally do not want to go through the hassle of proving their identity for what they perceive to be mundane items. Therefore, the ease that Americans crave when applying for new credit is also a partial source for the identity theft problem. For 95% of American adults, this systems nature is truly convenient. However, for the 5% of Americans who were identity theft victims in 2003, it is apparent that these lax procedures are not sufficient.

This notion of inadequate authentication procedures by businesses is further emphasized in an interview that was conducted with Jordana Beebe, Communications Director of the Privacy Rights Clearinghouse (PRC). The PRC is an organization that works to raise awareness of identity theft, provide assistance to victims and lobbies for consumer protection. Beebe issued the following statement on behalf of the PRC,

“In our opinion, the credit industry has not taken very simple steps that we feel would stop identity theft in its tracks. For instance, rather than simply giving out credit cards like candy, we think they should verify personal information on a credit application by comparing it with information contained on the person's credit report. At this point, the only thing that's looked at is the person's Soc. Security number (SSN) and credit score, but none of the other information is verified. We've heard from victims of identity theft where the only piece of information that was accurate on a credit application was their SSN. Their name is misspelled, date

of birth is wrong and of course the thief will put a different address.”

Thus the authentication processes that companies are practicing are at times so lax that it makes identity theft an easily committable crime.

8.2 Aren't Businesses Losing Money?

One would think that identity theft must affect businesses financially and, as result, they would want to implement more stringent authentication techniques to contain the growing crime. It has even been reported that companies lost \$47.6 billion in 2003 [33]. While companies are reported to be losing such a great amount of money, it is apparent that companies are not in danger of going bankrupt as a result of the problem. The assessment of how much damage is actually being done to the business sector is explored in George May's work *Stop Thief!*, May states,

“While credit issuers report billions of dollars in fraud ‘losses’ each year they really do not suffer much. Through higher interest rates and fees they pass most of this loss along to consumers. Basically they make the business decision that it is easier and more efficient to burden honest consumers with these losses than it is to prevent, or pursue, identity thieves” [23].

While May portrays the credit bureaus as amoral organizations who take pleasure in causing financial hardships to consumers, the truth is that this is how all businesses operate. Businesses must frequently perform a cost-benefit analysis of components of their organization. For instance, there are numerous nuclear power plants all over the world. There is a small probability that this facility can experience a meltdown that could kill numerous individuals. A potential solution is to build a very expensive container of some kind around all plants to stop this hypothetical waste from spreading. Businesses must make the decision if this type of expensive solution to solve a potential low-risk problem is necessary. Similarly, businesses have performed a cost-benefit analysis that has shown that while a percentage of Americans may become identity theft victims and have to have their losses reimbursed, implementing a more complex authentication system would not be profitable. Identity theft is not causing for

businesses to go bankrupt because, of it were, companies would spend a substantial amount of money and time to develop a new authentication system.

This notion that identity theft is not a crime that is causing crippling damage to the financial sector is even expressed on the website of Experian. As the website states,

“In a country where consumers owe more than \$1 trillion on their credit cards, estimates of \$2 billion to \$3 billion in credit card fraud losses may not seem all that terrible. That comes out to just two to three one-thousandths of one percent. But it is terrible to victims of fraud. Though they may be protected financially, they are forced to endure major inconvenience. Additionally, we all pay for the costs of fraud in the form of higher prices, higher interest rates and increased inconvenience [16].”

We find it striking that one of the three major credit bureaus blatantly admits that identity theft is not a problem for the credit industry. Significantly, instead of losing money some companies are gaining money from identity theft as a result of the market of identity theft protection products.

8.3 Are Companies Preying On Fear?

The effects of identity theft are truly devastating to consumers and it is apparent that the businesses in America are not practicing the proper authentication techniques to squelch the problem. What is even more disheartening is that financial institutions are not only not taking the proper steps to protect victims, but they are also capitalizing on the fears of victims by offering identity theft protection products. For instance Experian, TransUnion and Equifax, the three major credit bureaus, are not directly affected by identity theft because they do not actually issue credit. However, these credit bureaus each offer an identity theft protection product. For an annual fee, the companies will send a quarterly credit report, notify consumers if there is a change in their report and provide some form of insurance. For instance, Equifax Credit Watch Gold is a service that provides \$20,000 in identity theft insurance for \$99.95 a year [15].

So companies are able to prey on the fears of consumers to make a profit off of a grow-

ing crime. Sadly, consumers have eagerly purchased these products. In 2003, 33.4 million Americans bought a product to protect their privacy [2]. Such products not only included the previously discussed identity theft insurance but also software that is supposed to enable an individual to shop on the internet in complete anonymity. One would think that these miracle products would be highly beneficial. Again, the idea of companies using potential inadequacies in their own system to hopefully garner larger revenues is nothing new. For instance, Microsoft operating systems are vulnerable to various computer viruses. While Microsoft offers minor upgrades to their system to strengthen these vulnerabilities, Microsoft also makes virus protection software to potentially garner a larger profit.

Not surprisingly, at least one manufacturer of paper shredding is also preying on the fears of Americans in the hope of making a larger profit. Fellowes, an office supplies company, has passed a television advertisement campaign for one of its shredding products. The commercial depicts an identity thief snooping through a trash receptacle. The thief gives the warning that unless you buy a shredder, he can steal your information and commit identity theft. Instead of trying to take measures to stop the identity theft problem, it is apparent that various companies are using the fears of Americans to garner a larger profit.

8.4 What Is The Government Doing To Protect Consumers?

In response to the growth of identity theft, the government has issued an array of laws dealing with the new crime. While there are several laws present on the subject of identity theft, we claim that they fail to address the true problem that is plaguing America. All current laws deal with either the punishment of criminals or the rights of consumers after they have become victims. While such legislation is important, none of the laws currently in existence place regulations on the type of authentication protocols that businesses must implement to keep the crime from happening.

8.4.1 Laws That Address Identity Theft

The first major law directed toward identity theft was signed by President Clinton. The Identity Theft and Assumption Act of 1998 for the very first time defined the victim of identity theft as the person who actually has their identity stolen. Previously, the victims of identity theft were classified as the businesses who issued the lines of credit to the perpetrator. Also, under this law, the Federal Trade Commission is assigned the responsibility for being a centralized complaint and education point for consumers. Moreover, this government organization has the responsibility to inform local and federal law enforcement agencies and the major credit bureaus of complaints. Although informed, police and credit agencies are not required to do anything about the complaints. In particular, Federal law enforcement agencies typically ignore cases involving less than \$200,000 since no funding is provided in the legislation to prosecute perpetrators [18]. This law, therefore, merely addresses what happens once an individual becomes a victim of identity theft and does not provide means to actually stop the crime from happening.

Next, the Fair Credit and Reporting Act (FCRA) is another law created that is helpful to victims of identity theft. Under this law credit issuers and bureaus are ordered to use procedures to make sure that the information that is kept and disseminated about consumers is accurate and current. Thus, this law is applicable to victims who have difficulty in getting their credit report fixed after contacting the applicable agencies. Even with this law, it is still difficult for a consumer to receive monetary damages as a result of a credit file not being updated properly. A victim has to prove damages caused by the mishap and show that the particular company was negligent in handling the claim. Thus actually being awarded damages based on a violation of the FCRA is nearly impossible. Also, starting in December 2004, consumers will be able to order a free credit report from each of the credit reporting agencies every twelve months as a result of the FCRA. Again, the FCRA is a law that deals with events that take place after a consumer has become a victim of identity theft and does nothing to actually stop the crime from taking place. This notion is further manifested with the Fair Credit Billing Act (FCBA).

The FCBA establishes procedures for consumers to resolve disputes with credit issuers [18]. Again, this is a law that only applies to victims of identity theft and does nothing to protect people from becoming victims.

Within the past year, two new laws have been introduced dealing with the growing crime. First, the Identity Theft Penalty Enhancement Act increases the amount of jail time that an identity thief, who commits a felony, will face. Felons will have two years added to their sentence for committing identity theft and five years added to their sentence if the crime is linked to some terrorist activity. Lastly, the Fair and Accurate Credit Transactions (FACT) Act gives victims the right to obtain records from businesses where a thief opened accounts in their name. Previously, victims were not given access to such documents because businesses claimed that victims had no right to the documents. The FACT Act does have one provision that is supposed to deter identity theft from happening [15]. Under the law only the last five digits of a credit card numbers are allowed on cash register receipts. Certainly, such an undertaking does little to stop identity theft as there are a myriad of methods to obtain personal information. Authentication, one of the chief problems facing America, is again not addressed in any of these laws.

8.4.2 Prosecution Difficulty

Hence these laws mostly deal with the aftermath of identity theft. While most of the laws serve to merely define the punishment that criminals will face, these punishments are rarely applied. Only approximately one out of every one hundred identity thieves is ever caught. Then, if the thief is caught, convicting him is extremely difficult. Often identity theft cases cross multiple jurisdictions and, as a result, are extremely difficult to prosecute. This problem was recently articulated by Attorney General Thomas F. Reilly in response to the difficulty in prosecuting a woman from Philadelphia who stole the identity of eight Massachusetts residents. Massachusetts initially passed on the case because the alleged perpetrator resided in Philadelphia.

Meanwhile, police in Philadelphia showed no interest in the case because a successful prosecution would have been difficult with all the victims located out of state. As a result, Reilly has proposed legislation that would allow authorities in Massachusetts to prosecute identity thieves in either the county where the thief acts or the county where the victim resides. Moreover, the proposed legislation would allow the prosecution of identity thieves from Massachusetts without requiring victims to be flown from out of state to testify [37].

The laws currently in existence that are applicable to identity theft deal with the punishment of criminals and the rights of victims. Moreover, due to lack of funding and jurisdictional issues, in the rare cases when a thief is caught the likelihood of successful prosecution is slim. Most importantly, the lax authentication techniques used by businesses are the chief reason why identity theft takes place and no law regulates the authentication practices of businesses. Clearly, laws and funding must be developed by the government to address the reasons why identity theft happens and actually enforce the laws currently in place.

8.5 A Need For Education

We have so far argued that identity theft is a major problem that is not being properly addressed. The glaring question now present is what exactly needs to be done to stop the identity theft epidemic. One thing that is readily apparent is that Americans need to be educated regarding what exactly identity theft is and how they can better protect themselves. It was found in 2003 that 49% of Americans, or 98 million adults, felt that they did not know how to protect themselves against identity theft. This sentiment is further revealed by demographic as the youth, poor and less educated Americans are far less likely to know how to protect themselves from the crime. For instance, 56% of Americans in the lowest income group do not know how to protect themselves. Furthermore, only 44% and 45% of Americans who are between 18-34 and those who have a high school education or less respectively knew how to protect themselves [2].

Clearly, there is a glaring need for educating the masses. Through education, victims

would less likely fall for social engineering scams and would have a deeper knowledge about how they should safeguard their information. One individual who realizes this education laps is WPI campus police officer Cornelius Spellman. Officer Spellman has worked on anti-fraud task forces and, through his investigative work, has frequently used social engineering techniques to obtain information. According to Officer Spellman, obtaining information from citizens is simply too easy due to a general lack of awareness and education.

As a result, in November 2004 Officer Spellman held a seminar at WPI educating faculty and staff members about the problem. Besides making individuals aware of the growing problem, Spellman offered helpful tips to all in attendance. For instance, Spellman explained that it is imperative to only carry documents, such as a Social Security card, when it absolutely necessary and he also gave the necessary contact information in case someone ever does become a victim of identity theft. Seminars like the one that Officer Spellman has conducted are imperative in the fight against identity theft. While the FTC offers some educational workshops throughout the country, local law enforcement outreaching to the community in a free public forum allows for the danger of the crime to be heard by more people. While it is true that some people, no matter how much they are lectured to, will never change their ways, an educational outreach program conducted by law enforcement can only serve to help those who attend it.

9 Looking For A Solution

9.1 Problems Within The Current System

The current manner in which American commerce operates allows identity theft to take place at a rampant rate. As shown previously, the existent laws do little to stem the problem. The financial industry's efforts to truly authenticate consumers and ensure that they are who they say they are leave something to be desired. In addition, consumers do not take enough actions to safeguard their personal information from potential thieves.

Because of this, there is a need to make a change in the way that consumers and industry

interact with each other if the identity theft problem is ever to be resolved. In particular, there must be a method created to ensure that consumers can be authenticated in a manner that is affordable and that instill confidence in users. If and when a consumer's personal information is stolen by a thief, the criminal should not be able to be authenticated in the name of the victim.

9.2 The “Central Authority” Solution

In theory, the best approach to solving the identity theft problem is the concept of a “central authority”: a single, benevolent, empowered entity that would oversee all transactions of information, and ensure that it always remains in the right hands. Under this type of model, a unified federal agency would be contacted whenever the identity of a citizen needs to be authenticated. For instance, if an individual wants to apply for a new credit card, that person would first contact the credit agency to make a request. Next, the credit agency will contact the government authentication agency. Then, the government authenticator would perform a protocol to verify that the consumer, whose name was given by the credit agency, actually wants to have a new credit card. Finally, if the agency can confirm the identity of the consumer, a new card will be issued. If it is determined through the authentication protocol that the consumer never actually wanted the credit card and someone else stole his identity in an attempt to obtain a fraudulent card, the transaction will be aborted.

An application of the “Central Authority” archetype exists within in Robert Pinheiro's work, “Proving Identity Theft Using Trusted Authenticators.” Pinheiro explains a system developed by Professor Lynn LoPucki of the UCLA School of Law, called the Public Identity System (PIDS). PIDS would create a list of individuals who voluntarily consent to be contacted for verification when someone applies for credit in their name. This system is best described in the following passage from Pinheiro's work,

“An individual would voluntarily provide his/her personal information to the list, including name, SSN, and perhaps other identifying information. A thorough authentication process would ensure that new members of the list are truly the per-

sons they claim to be. A personal appearance before the government agency that maintains the list would be required. Individuals participating in PIDS would specify one or more standardized ways that a creditor should contact them when the creditor has received a new account application in their name. Contact methods would likely be limited to a phone call, e-mail (encrypted or unencrypted), or US Mail [28].”

Furthermore, both LoPucki and Pinheiro state that, if such a system were to be developed, federal laws should be modified that would punish agencies if a PIDS participant becomes a victim of identity theft due to the agency not performing the authentication process for a member that requests it. There are some variations to the PIDS system. Pinheiro offers one in which the trusted authority is not a central government agency, but rather the banks of consumers.

While such a central authority system is the most common model proposed by experts to solve the identity theft problem, it is faulty on at least one glaring level. These systems lack actual detail on how the authentication process will take place. While many theorize that password, email or telephone authentication could be used, it does not specify under which circumstances each authentication method would be appropriate. Moreover, these proposed systems fail to articulate how registration will take place as well. No details are given that suggest how many forms or what type of identification is needed for registration. In short, “central authority solutions” are often vague proposals that suggest means which are difficult or impossible to implement within the near future.

10 NIST Solution: The Big Picture

Whereas the central authority models are presented as standardized, perfect ideals that will forever end the identity theft problem in America, another model recently emerged that takes a more realistic approach to this enormous problem. The National Institute of Standards and Technology (NIST) offers a guideline for electronic authentication within NIST Special Publication 800-63. Although the document is tailored to offer authentication recommendations for

federal agencies, the guideline may be used by nongovernmental agencies on a voluntary basis as well. The general authentication process is described as follows by the NIST document:

“E-authentication begins with registration. An applicant applies to a Registration Authority (RA) to become a subscriber of a Credential Service Provider (CSP) and, as a subscriber, is issued or registers a secret, called a token, and a credential that binds the token to a name and possibly other attributes that the RA has verified [7].”

These basic logistics are not often absent from the identity theft problem, since the procedure is similar enough to the way that American society operates currently, when applying for and using these kinds of “identifiers”. In contrast to today’s practices, however, the NIST proposal provides a uniformed layout of what specific procedures should be followed for registration and authentication.

The NIST authentication guideline is a supplement to the Office of Management and Budget guideline “E-Authentication Guidance for Federal Agencies” (OMB 04-04). Under OMB 04-04, four levels, ranging from Level One to Level Four, of identity authentication assurance are defined. Each tier corresponds to a credible agency’s degree of certainty that the user has presented an identifier. For example, Level One refers to the situation when the agency has little or no confidence in the validity of the identity present, and Level Four is intended to instill absolute confidence in the end-user [7].

Now, with all four authentication levels defined, a company, through a series of personal assessment activities, will be able to determine the appropriate level of authentication required for any particular application. With an appropriate level of security identified, one is able to consult the NIST document and apply the required registration procedures that pertain to that level. NIST documents the in-person and remote registration procedures that can be used at each level. Higher levels require more stringent registration procedures; remote registration is not even an option at Level Four.

Hence, this NIST proposal is a solution for identity theft that, unlike previously proposed solutions, possesses enough detail and specification to actually be adopted, in our view. Indeed

this guideline is already being cited in the authentication products of privately owned companies. For instance, in the white paper *Trusted Federated Identity Solution Architecture*, Verisign Corp. and IBM detail the couplings of their products that could form an identity management architecture based on the Registration Authority and Credential Service Provider model detailed above. More importantly, the document states that all companies that are members of the proposed federation group need to agree on what minimum registration and authentication protocols will be carried out. In particular, the document cites the NIST recommendations as a viable option for determining such requirements. Therefore, the recommendations made by NIST are not simply vague proposals but, rather, a document with enough detail that can already be critiqued, applied and adopted by companies [35].

10.1 What Are These Four Levels?

Before going into detail about the inner workings of the system, it is essential to first analyze how the NIST standard has defined these four levels of security. It was previously mentioned that increasing levels are proportional to the confidence in the end-users, therefore each level must have tighter security surrounding it than all those below. The contingencies implied by registering and authenticating under these four levels will be detailed further within the upcoming, respective sections. For now, a few examples are presented to demonstrate proper implementation of each tier.

Level One refers to the situation where an agency has little to no confidence in the identity of the client. This would include electronic form submission (one-way transfer), discussion board participation, and registering a username or password for a government website. In a Level Two scenario, there is some confidence that the asserted identity is accurate, such as online learning centers, change of address within the Social Security Office, and bank account interactions. When an individual gets their address of record changed, a notification is sent to the previous address of record to confirm this new change. While there is the possibility that information can be intercepted through mail fraud, it is not deemed severe enough to warrant a

higher level of security.

Level Three, designed “for transactions needing high confidence in the asserted identity’s accuracy”, is adequate for legal paperwork submission (such as a patent office), expense account maintenance, and disaster reporting (such as the First Response service). There is great possibility of substantial financial loss if improper authentication takes place, yet the losses are not severe enough to necessitate the greatest level of security.

Finally, Level Four is defined for the highest authentication assurance. In particular, this level is reserved for the need for very high confidence in the accuracy of the identity of the user. Level Four would protect such highly sensitive information as criminal record databases, medical records, and any such transfer of secretive, personal information. If someone accessed this database without authorization, the privacy of citizens would be violated, and law enforcement investigations could be compromised. This type of transaction would certainly require the highest level of security.

It seems as if Level One and Level Two are simplistic functions that are often performed on the internet several thousand times daily: registering a free email account, signing up for a bulletin board, sending a facsimile and online banking. The standard 128-bit web encryption is more than enough for these functions, but those that would take place within Level Three and Four require a bit more protection, as history has shown us. Surely, only these two lower echelons could possibly be candidates for the transfer of personal information over open networks.

11 The OMB Standard

In order to determine which of these four levels is appropriate for a given situation, a company must first perform a risk assessment evaluation. In this process, a company must take into account the likelihood of improper authentication occurring and what possible damages could arise if improper authentication takes place. The company is then asked to classify the

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Civil or Criminal violations	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High

Table 6: Maximum Potential Impact for Each Assurance Level

possible impact that improper authentication would cause in a variety of areas. This type of evaluation is further detailed in Federal Information Processing Standard 199. Then, according to OMB 04-04, once this risk assessment is complete, the company must then find the lowest level whose impact profile meets or exceeds the potential impact determined for every category analyzed in the risk assessment, and use that to determine the required assurance level. Table 6 displays the rubric which a company would use to make this described comparison. Also within OMB 04-04, the five key issues of assessment are described: Agencies should determine assurance levels using the following steps, described in Section 2.3 of the OMB document:

1. Conduct a risk assessment of the e-government system.
2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

The two schematics (NIST and OMB) intermesh quite well; they both have four levels of safety, each built upon the last, with increasing complexity. The crux of the assessment lies in the potential for certain threats, and the potential impact these threats would create. For example, “Unauthorized release of sensitive information” is considered low-risk at Level Two, moderately risky at Level Three, and high-risk at Level Four. Therefore, if an information leak would be devastating to your business or personal interest, Level Four would be highly

recommended [5]. The goal is balance convenience against risk and their model does this by carefully considering these four gradations.

11.1 Is This Assessment Really Sufficient?

While OMB 04-04 recommends a self-evaluation, it is apparent that this form of assessment is not sufficient enough in determining security levels for a given application. If a company is to formulate its own opinion as to what level satisfies existing needs, one wonders if companies would just refer to the lowest authentication levels that require the least amount of money to maintain and offer maximum convenience to the paying customer. As shown in previous chapters, credit companies currently use lax procedures in their authentication protocols. It has been revealed that these companies merely match pieces of personal information to a database that they maintain. In many instances, there is information that is mismatched yet authentication still takes place, thus furthering identity theft's growth as a rampant problem.

Additionally, if companies have been unwilling to adopt secure policies on their own up until now, why should it be expected that these same companies will adopt secure policies in the future, if they remain the ones making the determination? In order for these authentication levels to be assigned effectively, concrete legislation would have to be developed that describe specifically what type of activity should fall under what type of authentication level. In particular, the legislation should also classify each level based upon concrete dollar amounts that are involved within the particular activity. Hence, if an activity holds contingencies less than X dollars, it would qualify for Level One authentication, if it involves between X and Y dollars it should qualify as Level Two authentication, and so on in this manner. Only with enforcement would companies be fully (or near fully) accountable for the needs of their customers, when performing this evaluation.

Due to the scope of our analysis, we are not particularly concerned with federal procedures or necessities, but rather with the context of these proposals on a civilian level. Whereas NIST implies that this system eventually will be scaled or adapted for widespread use, the OMB

rhetoric does not take into consideration the differing needs of the public. These facts lead to a schism of thought, based upon the merging of these two documents and our goal to secure personal identities. In our context, the following question immediately arises: “Is it absolutely necessary to ensure that Level Four of the NIST standard be employed at all times when identity information is involved? Facts and arguments pertaining to this question are presented in the following two section. There are no specific tasks stated that absolutely require specific levels of authentication power. There are implications throughout the document, and some examples, but somebody has to enforce a standard of practice. It is too crucial of a concern to be left in the hands of the self-interested end-user.

What it comes down to is that there is no specified

11.2 Why Identities Must Be Guarded By A Level Four System

According to this OMB memorandum, the major types of impacts created by the compromise of an information system are

- “Financial loss or agency liability”,
- “Inconvenience, distress or damage to standing or reputation”,
- “Harm to agency programs or public interests”,
- and “Unauthorized release of sensitive information”.

As we have found, all of these are also the most common results of the work of an identity thief, most specifically the damage to a person’s reputation. Level Three is only certified in situations where the dispersal of this information is only of “moderate” threat in this regard. If one truly feels that identity deserves to be placed behind the strongest of locks, then anything less than Level Four would be a compromise. The OMB document suggests Level Four for such activities as medical and criminal record access, very secure and personal information. Why stop there, and not include all sensitive facts about an individual, such as social security

numbers and dates of birth?

11.3 Why Identities Do Not Have to Be Guarded By a Level Four System

The existence of this highest-level of security gives us the inclination to use it for all purposes we feel are worthy of it. The natural question: if personal identity is not important enough for Level Four, then what is? Would we assign the same level of security to people's identities that we would feel inclined to give such applications as remote nuclear launch codes, lists of undercover agents, and other sensitive information that, in the wrong hands, would most certainly lead to death? We must not forget that the mass propagation of these hardware tokens, given a world in which every person held one that was bound to their identity, would increase the likelihood that they might become decipherable. This would compromise the keystone of Level Four security, and all that is held behind it (at the very least, it would be severely weakened). We are not saying that people's livelihoods are not worth it, we are saying that people's lives most certainly are.

11.4 Final Thought on Evaluations

It will be up to debates and discussions on many more than the few points raised in the preceding sections to determine whether Level Three or Level Four will be the best protection for people's identities. Our purpose here was to point out that it's not a trivial decision, and that more specificity is needed from the rule-makers (NIST and OMB) on the implications directly created by attaching personal information to tokens and databases.

12 Registration

Before a person is allowed within the open network, they must first pass a background check of sorts, during the process known as "registration". NIST Special Publication 800-63

provides guidelines as to level-specific registration requirements. This process does not take place for Level One; the issuance of a password does not require that an identity be aligned with its possession, since all names on Level One are assumed to be pseudonyms [7].

Depending on which of the remaining three levels of the hierarchy are to be entered, the applicant must supply documentation of increasing complexity. For Level Two, a driver's license or passport suffices; it must be "a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality." The Registration Authority, or RA, then compares the picture to the applicant, and records the pertinent personal data, such as address, date of birth, and identification number. If all is clear, the applicant is granted access. The applicant is issued authentication credentials and notice is sent to their address of record.

The process works similarly for Levels Three and Four, except that the 'Government Picture ID' is subject to more scrutiny than a simple on-sight comparison; it is suggested that the identification be cross-checked through a government agency or credit union, to verify the information given is accurate. Also, at Level Four, an additional piece of identification is required, plus the recording of a biometric, which is to be linked to the granted tokens.

12.1 Remote Registration: Simplicity Versus Risk

The most controversial feature, in regard to this registration process, is the allowance for a remote method for Levels Two and Three. Despite the heightened complexity, which now requires the possession of a banking account number in addition to the original government ID, there is still an allowance for fraud within this situation. An identity thief can easily obtain the required information to register for a service using another individual's identity. One must merely obtain a government ID number, such as a social security number, and a financial account number, such as a credit card number, in order to register remotely for a service at Level One through Three. This information, along with other basic identifying information, can be obtained by a thief who uses social engineering. Social engineering, as detailed in Kevin Mitnick's book, *The Art of Deception*, refers to the art of a thief tricking individuals into revealing

their personal information or other critical information that can be used to commit identity theft [25].

For instance, in September of 2004, in the wake of Hurricane Francis, four men posed as officials from the Federal Emergency Management Agency at New St. John's Baptist Church in Northwest Ocala Florida. These impostors stole bank information, social security numbers and other such personal information from hurricane victims, by lying about needing this data to process the paperwork for disaster relief. Similarly, during this year's election season, a voter scam took place in northeast Ohio. Imposters, claiming to work for the Ohio Board of Elections, called several individuals claiming that they needed information to confirm the individual's voter registration status. The crooks obtained the social security numbers and credit card number of several voters. Under the guidelines for registration under different security levels, these imposter situations would not be prevented inside of Level One through Three remote registration processes.

Clearly, there are several types of techniques that can cause for a crook to obtain the personal information of an individual. A crook can even "dumpster dive" to acquire information. Frequently, individuals discard documents that contain sensitive information without properly destroying them. By simply going through a trash receptacle, a thief will have the required information to perform remote registration. The direct approach, stealing information from an individual's mailbox, is also commonplace. Sensitive information is sent through standard mail on a daily basis. However, most mailboxes are not properly secured, and a thief can easily steal the contents of a mailbox. For instance in March 2004, an identity theft ring was discovered in Port Orchard, Washington. For instance, we already mentioned the March 2004 case where individuals were instructed to steal from mailboxes throughout the community; the contents were then used to commit identity theft.

12.2 Telephone Manipulation

In addition to knowing the information to perform a registration, a thief must also be able to intercept the confirmation message the RA sends out afterward. Again, this can easily be done. In the first three levels, a confirmation message can be sent through mail. By simply filing paperwork at the post office, a thief can have a victim's mail forwarded to a different address. If the change-of-address process happens to be made more secure, a thief can simply steal the confirmation letter from the mailbox of the victim. It is again possible, but more difficult, to intercept email and telephone transactions. For instance, Kevin Mitnick describes how to force telephone companies to forward calls to different numbers. Similarly, one can conceivably intercept the authentication required to gain access to a victim's email account.

Level Three, however, also might require telephone confirmation with voice recognition. This type of confirmation method is substantially more difficult to overcome, assuming that the system works properly. It seems the thief would have to physically force the victim to speak in the phone. However, there exist devices that could emulate frequency and sound of the victim's voice. The address confirmation process specified by NIST can make the process of identity theft difficult but it is very possible to circumvent these problems.

12.3 Our Decision

It is thus the position of the authors that, in a world where people wait for hours on end at the Department of Social Security for the office to issue a single critical piece of identification, and a world where people do not lock their mailboxes and throw junk mail away that may contain vital information, that complicating this registration process, by eliminating the possibility of remote interaction, is not being "too safe". The creators of this framework banned remote registration for Level Four, perhaps because remote recording of biometrics would be complex, but also perhaps because they decided that the risks outweighed the benefits in this very critical, highest-level point. To allow remote registration at Level Two and Three was probably a

vote in favor of simplifying what would be a massive amount of paperwork and labor for these Registration Authorities; trying to prevent the aforementioned crowded Social Security waiting room image.

12.4 Final Thought on Registration

Considering all that has been studied throughout this project, the attachment of an ounce of importance to these implements obtained from these RAs may deter their loss or risk of being stolen. That is, if Social Security or the Department of Motor Vehicles makes you wait hours for the issuance of documentation (SS cards or driver's licenses), people tend not to lose them because, in the back of their minds, they know the hoops they will have to jump through in order to get replacements. If we presume NIST allowed remote registration motivated by simplicity, we wish to repeal it, motivated by want of added security. This is a subtle yet effective way of turning the current lack of care for paper documentation around, in hopes of maybe attaching that same regard to these "tokens", one day hoping that hard tokens are worthy of putting in that fireproof locked strongbox, right next to birth certificates and other irreplaceable items.

13 Tokens - Definitions

According to the document, there are four types of tokens that can be used inside of the NIST system: hardware tokens, software tokens, one-time password device tokens and password tokens. Each of these tokens is coordinated with a certain level of security. Hence, only certain types of tokens are permitted in a particular level of security. This breakdown of which token is acceptable for each level of security is illustrated as follows:

“Password tokens can satisfy the assurance requirements for Levels 1 and 2. Soft cryptographic tokens may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3. One-time

password devices are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3. Hard tokens that are activated by a password or biometric can satisfy assurance requirements for Levels 1 through 4 [7].”

While these are four general tokens that have been mentioned previously, NIST has special requirements for each type of the different tokens in order for them to be used effectively in their system.

13.1 Hard Tokens

By definition, a hardware token is a physical device that contains a protected cryptographic key. One may prove authentication only by having possession of the token and control of the secret key. In order to be qualified for use in the NIST system, hardware tokens are required to be activated by either a password or biometric. Moreover, the cryptographic authentication key must be impossible to extract from the device. Lastly, the token must meet certain Federal Information Processing Standards detailed in FIPS Publication 140-2. Firstly the token must have Level Three or higher ratings in physical security. This type of rating is specified in the following excerpt from FIPS 140-2:

“Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened [7].”

Besides the physical security described above, the device must have an overall validation of Level Two or higher. This means that cryptographic keys used must meet a certain stringent standards specified in the document. By meeting all of these standards, a hardware token can be used for NIST Levels One through Four.

Consequently, the type of hardware tokens that NIST requires are not simple devices that can be easily broken into by anyone and taken apart to reverse engineer the inner workings.

Rather, the FIPS 140-2 standards place very strict requirements on how well the device must be protected. For instance, it requires that if anyone attempts to open the physical casing of the device that a warning message of some form is sent to the RA so they can immediately disable the token. Moreover, there are rigorous cryptographic standards placed on the device guaranteeing a high level of security.

13.2 Soft Tokens

From the NIST documentation:

“...a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token key shall be encrypted under a key derived from some activation data. Typically, this activation data will be a password known only to the user, so a password is required to activate the token. For soft tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher, and may be either a hardware device or a software module. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication [7].”

This is very similar to a web browser cookie or encryption keys, in the sense that our data is generally public, but possessing this item alone will not tell you enough about the transactions taking place to extract any valuable information. Notice that the key is a device of sorts: you input a password, and it outputs the private, vital segment of itself. Also note this is not congruent to simply having a user input a password; the user downloads the token (again, “Eve” can have this entire module if she wants), then that user activates it on their own side with a password, which is never transferred over a network. Therefore, because ‘anybody’ can have this token, the password must be a strong one, and the ever-present prospect of a password attack must be addressed.

13.3 One-Time Password Device Tokens

“...a personal hardware device that generates “one time” passwords for use in authentication. The device may or may not have some kind of integral entry pad,

an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by using an Approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, a counter generated on the device, or a challenge from the verifier (if the device has an entry capability). The onetime password typically is displayed on the device and manually input to the verifier as a password (direct electronic input from the device to a computer is also allowed). The one-time password must have a limited lifetime, on the order of minutes, although the shorter the better [7].”

This is essentially a more complex version of the hard token above, where “proof of possession” is specifically defined: enter a number or a fingerprint, and then use whatever is outputted as the verifier. The key difference is that this device must be adaptive: it does not always have the same output, as is implied by the hard token design. For example, I use a hard token to access a secure network, and I do this by plugging it into the USB port of my PC. The same encryption key is sent across the wire each and every time. Even though this key is secure (our method should be top-notch), “Eve” is going to get many opportunities to see the same message encrypted different ways, and there may be a chance she can decode the message after enough of these (on the order of thousands of captures). Now, to go through the same example, this time with a one-time password device. A new message is sent, use only on a temporary basis, and transformed by the same encryption method. There is no repetition, therefore “Eve” will have increasing difficulty of decrypting our messages. The one-time password token is superior, but definitely more expensive to produce and maintain on a large-scale, public consumer basis.

13.4 Password Tokens

“...a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however some systems use a number of images that the subscriber memorizes and must identify when presented along with other similar images.”

The most simple of verification methods, but here it is often used in conjunction with one of the three implements listed above. NIST knows fully well several people still write passwords

down when they should not, and the wrong people occasionally find these notes. Therefore, password tokens play only a small role in proving one's identity, but their exact structure must be defined here all the same.

14 Tokens - An In-Depth Look

As seen within these definitions, the justification, or rather the presumptions, of the dependency placed upon tokens, is two-fold:

- 1.) The creation and possession of such tokens implies that the possessor has registered under a trusted authority, and that registration included the supplementation of critical documentation, that which is believed only to be in the possession of the person who matches the identity given (i.e. they are who they say they are). These tokens are only created for a person after having proven to be trusted in this manner.

- 2.) These tokens are well-protected, irreplaceable or unforgeable, and unique in construction and usage. The token or tokens become almost bound to the person. As long as they are not shared, stolen, or otherwise acquired by another user, the acting user on the open network can and must be trusted.

Any flaws within the NIST schema, in regards to token usage, will occur as a violation of either of these provisos. The NIST paper goes to great lengths to advocate both as strengths behind Level Three and Level Four interactions, and while it does not imply by any means that these are foolproof, the purpose of this section is to bring to light some of the more creative, if not realistic means of spoiling the trust attached to these hard and soft tokens. In fact, one section is devoted to possible means of preventing the obfuscation of tokens by third parties, suggestive albeit vague.

14.1 A Locked Key: What's Inside of a Token?

The NIST booklet acknowledges that a token created based upon identification information must also contain this information, albeit encrypted and protected. However, the lock on this key is not fail-safe:

“Hardware tokens prevent malicious software from extracting and copying the authentication secret token from the token. However, malicious code may still misuse the token, particularly if activation data is presented to the token via the computer. Similarly, the cryptographic tokens at least make it difficult to trick a user into verbally giving away his authentication secret, making social engineering more difficult, while many kinds of passwords are readily expressed over the telephone.”

Cracking the code is difficult, but not entirely impossible. Consequently, the safeguarding of tokens is highly advocated:

“However, when using either public key pairs or shared secrets, the subscriber has a duty to maintain exclusive control of his token, since possession and control of the token is used to authenticate the subscriber's identity [7].”

This is critical, since, if a person possessed either token, with the right means, they could decrypt the stored information, and use this to their advantage; basically, all of the 'detective work' of identity theft would already be complete. Also, the tokens could then be used to access the original intended system, immediately. Both of these possibilities are difficult, for differing reasons.

14.2 Manipulating Hardware Tokens

While the hardware tokens described by NIST seem to be fully secure, they are not entirely immune to compromise. It is still conceivable that somebody with enough time, money and technological background can eventually compromise the security of the device. However, as shown earlier in this report, most identity thieves do not accomplish their crime by great technological methods. Rather, they use simple techniques such as dumpster diving, mail theft and social engineering techniques. This notion is confirmed by the 2003 Federal

Trade Commission-Identity Theft Survey Report. This report, which was prepared by Synovate, states that of all identity theft victims that knew how their personal information was stolen, approximately half of the victims had their information taken via lost or stolen credit cards, check book, social security cards and mail [33]. In order to compromise these tokens, the “solo” identity thief archetype would be virtually eradicated and instead replaced by a more complex identity theft ring.

However, while it would be hard to physically compromise the token and then deduce how the device can function, it is still possible for a common criminal to compromise the device. Hardware tokens are required to be operated by passwords at some security levels. As shown throughout the course of this entire report, obtaining an individual’s password is very simple, and often met with little resistance. Now, in this situation, where a hardware token is present, previously described schemes can be adopted so that the thief can not only steal the password of an individual, but also steal his physical token as well. For example, suppose that a thief, dressing in a fancy suit and tie, comes to an individual’s home claiming to be from their credit card company. The thief could merely tell the unsuspecting victims that all customers are having their tokens upgraded to a safer more secure system. All that they need to do is hand over their token, password and some personal information to the man in the suit, and they will be given a “new, better” token. In fact, to further this con, perhaps he would carry some nice plastic contraptions that resemble tokens, and give them out right away. The victim might be told he has to wait for a period of time before this account is updated and then their new token will be ready to use.

This is merely an adaptation of proven schemes that have been used to commit the crime. For instance, in September 2004, criminals in the Ohio area pretended to be members of the Board of Elections. These individuals called up various people and asked them to give their Social Security numbers, along with other personal information, in order to confirm their voter registration status [27]. Many voters willingly gave out their personal information to these imposter agents. Hence, if people are currently falling for such voter registration scams, it is not

a far-fetched conclusion that these same people could easily give up their hardware token and all of the necessary information to activate it.

As stated previously, it is possible for the hardware token to be deactivated if it is being handled improperly or even if it is stolen or misplaced. However, this presumes that the user notifies the CSP immediately if such an abnormality occurs. Moreover, with password-enabled hardware tokens, there is always the inherent risk of users writing their passwords down somewhere. As Bruce Schneier states in his book, *Secrets & Lies*,

*“The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it’s easy to remember, it’s something nonrandom like “Susan.” And if it’s random, like “r7U2*Qnp,” then it’s not easy to remember [29].”*

Consequently, it is almost to be expected that when a password is required for a certain situation, then a percentage of individuals will write it down. A certain level of care is expected with hardware tokens. A token user is expected to keep the token secure and also keep their password secretive. If someone is not careful with their hardware token and writes their password down, a thief can easily steal the token along with the piece of paper containing the password information to activate the token. Thus improper password recording and insufficient security practice would defeat all of the cryptographic strength of the token.

Tokens that require the use of a biometric to activate are more difficult, but not impossible to compromise through human deception as well. However, if one were to commit such a crime it, again, would call for something more technically advanced to be done and, again, this is not something that identity thieves are known to be involved in. For instance, if it is known that the hardware token will only operate if it reads the correct fingerprints of the user, then a thief could steal the fingerprints of their target before conducting the previously mentioned scam. As an example, the thief could obtain the victim’s fingerprints off of a discarded coffee cup and then replicate them on some form of glove. Again, this can be done but it requires a tremendous amount of technical resources and also can become nonproductive in terms of cost and time. Despite the thief spending a great amount of resources collecting and reproducing a

biometric, there is no guarantee the victim will fall for the scam.

14.3 Unlocking a Hardware Token

Unravelling the token's stored data is just as complicated as defeating most modern encryption systems. Identity thieves are not commonly hackers; the dumpster divers and social engineers far outnumber those who would have the expertise at digging through standard or airtight algorithms. The treasure behind this lock is worthy of the finest defense and that is exactly what NIST advocates: the FIPS 140-2 standardization for both hard and soft tokens [7].

The fatal flaw here, however, is not how well the guts of the token are protected, but how the token is used. The soft token is an item passed as software between the communicating parties on this open network. For the hard token, it is suggested that either password or biometric validation be used. Both of these are subject to common problems: the former a third party or "Eve", listening in on transfers, and the latter upon standards that have failed in the past (passwords are crackable, biometrics reproducible). Luckily, it is the mere possession of a hard token that is its greatest ally. If one is stolen, the owner should immediately invalidate it, the same way one voids a bad check or cancels a stolen credit card. That presumption of responsibility carries a great deal of uncertainty; people do not always report theft of such items immediately, and feel as though they are not liable for any misuse that resulted from this misfortune. As long as this mentality is nurtured by financial institutions that issue "fraud insurance" on credit accounts, phone companies reconciling cell bills because the unit was stolen, and other such means of displacing guilt from the consumer or end-user, people might not even know, much less care, that their tokens have gone missing, or have been noticeably tampered. Hard tokens are a step in the right direction, but giving a person one means they must understand that a certain degree of care is implied by possession.

14.4 Soft Token: Eve's Objective

This then leaves the soft token as the most vulnerable piece of the puzzle. NIST supports this conclusion themselves:

“Impersonation of an identity using a hard or soft token requires that the impersonator obtain two separate things: either the key (token) and a password, or the token and the ability to enter a biometric into the token. Therefore both hard and soft tokens provide more assurance than passwords by themselves normally provide. Moreover, a hard token is a physical object and its theft is likely to be noticed by its owner, while a soft token can sometimes be copied without the owner being aware. Therefore a hard token offers more assurance than a soft token [7].”

Level Four requires both these pieces be combined, whereas Level Three does not (only a soft token is used). However, it is suggested that a password (in accordance with Level One and Level Two), or a biometric be combined somehow with the soft token on Level Three [7]. Does this hint further at the soft token's weakness? While the framework recommends that levels be combined within an implementation (i.e. If your requirement is Level Four, use all four levels within your guidelines), it is for Level Three that this special consideration is made.

It was mentioned earlier that this soft token itself would be very secure, but now we suggest that the weakness lies in the connection that is carrying this token back and forth; that an eavesdropper (“Eve”) would be able to not only see the soft token, but create a copy for herself. The answer to the inherent question (Is the system now compromised?) will determine the safety of Level Three transactions, overall. This situation must be averted; we have to assume our opponent sees this token, and be confident that nothing can be obtained from inside. The latter is a matter of personal faith in the cryptographic system that forged this token, and the former will now be discussed.

14.5 Supplementation: The Difference Between Level Two and Three

The National Institute of Standards and Technology suggests that, in order to evade the problem of a listening party, or the usage of a stolen soft token, an additional requirement must

be instated. As far as Level Two goes, this is merely a password (similar to Level One), but, as mentioned before, Level Three suggests a biometric as the answer. Either way, increasing complexity seems to be the trick, although NIST will not say this is foolproof:

“Multiple factors raise the threshold for successful attacks. If an attacker needs to steal a cryptographic token and guess a password, the work factor may be too high. ... System and Network security controls may be employed to prevent an attacker from gaining access to a system or installing malicious software [7].”

So, we build bigger mazes and stronger doors and hope this is enough. Frankly, this is been the common philosophy of security since the first city walls were raised; bigger is better. Whether that necessarily sits well living inside a reformation of proofing guidelines is left up to the individual. Personally, given our findings in this area, too much work and too hard to access have not stopped many identity thieves. The prolific Kevin Mitnick proudly recounts a story of scavenging through a dumpster, only to find his quarry ripped into hundreds of pieces. He takes them to a nearby diner and goes about this arcane jigsaw puzzle, finally reassembling the original document. Patience and resourcefulness are not qualities these people lack.

Unfortunately, Level Two (and to some lesser extent, Level Three) now encounter a vicious cycle. Given the opportunity to try nigh-infinite attempts at a password, a dictionary attack would win most of the time. The suggested NIST solution is “requiring use of long passwords that don’t appear in common dictionaries”, which implies the expectation that people will memorize these random alphanumeric strings. The common remedy to that would be the famous Post-It note on the monitor, there for all to see and read. This situation exemplifies one of our major conclusions within this study: identity theft is not only a subject relevant to cryptographic means (a complex lock), but also to education (not losing the key to that lock). Case after case, the strongest doors in the world existed, but it takes just one person to open them for the “trusted” stranger.

14.6 Hijacking: Open the Door, Then I Knock You Out

A brief tangent, relevant to token dependency, is the subject of session hijacking. Essentially, once the requesting user has been verified, their accessing means are overtaken, and the “hijacker” is then free to “pose as subscribers to relying parties to learn sensitive information or input invalid information, or pose as relying parties to verifiers to learn sensitive information or output invalid information [7].” All of this care and consideration for tokens is wasted, because the attacker can wait for the connection to open, and then take the user out of the picture. NIST offers a specific plan to deter such efforts:

“An authentication and transfer protocol in combination is resistant to hijacking if the authentication is bound to the transfer in a manner that prevents an adversary capable of inserting, deleting, or rerouting messages from altering the contents of any information sent between the claimant and the relying party without being detected. This is usually accomplished by generating a per-session shared secret during the authentication process that is subsequently used by the claimant and the relying party to authenticate the transfer of all sensitive information [7].”

Could such a “secret” be used to prevent soft tokens from being obtained, and in a greater sense, be used to secure the connection?

15 Authorization - Putting Registration to Use

15.1 Generic Process at Each Level

The NIST booklet does contain the most generic of details about the interactions that take place during “authorization” (when a person uses the items obtained during “registration” to prove that they are who they claim to be), and in particular, potential threats that may occur at this time, which will now be discussed. As with remote registration, eavesdroppers and other such attacks are a realistic threat to this process. Session hijacking, discussed earlier, is probably the most threatening to the individual. Again, suggestions are made as to how to circumvent these threats, and once again, the details are left to the user. Our familiar adversary,

the social engineer, is included within a list of miscellaneous threats:

- Malicious code attacks that may compromise authentication tokens;
- Intrusion attacks that obtain credentials or tokens by penetrating the subscriber/claimant, CSP or verifier system;
- Insider threats that may compromise authentication tokens;
- Out-of-band attacks that obtain tokens in some other manner, such as social engineering to get a subscriber to reveal his password to the attacker, or “shoulder-surfing;”
- Attacks that fool claimants into using an insecure protocol, when they think that they are using a secure protocol, or trick them into overriding security controls (for example, by accepting server certificates that cannot be validated);
- Intentional repudiation by subscribers who deliberately compromise their tokens.

Clearly, most of these threats exist in today’s data interactions. Therefore, in order to ensure our new secure system is safe, we need a secure design for our transfer media, namely broadband connections, LANs, WANs, and MANs, the sort of “open networks” that the document references.

15.2 The Expectations of Registration

One potential problem that is not discussed within the pamphlet is that of implicit assumptions about the registered user. Although NIST admits that their registration is not fail-safe, once a person has passed through this process, it seems to be automatically assumed that this person is then in the clear; they must be who they say they are, and the user’s identity is never later questioned. This means that, given a social engineer who is able to complete the registration process, and receive the pertinent items, they may now pose as whoever it is they registered as, without dispute or risk of being caught. Removing risk factors only will encourage more criminal activity; either registration must become more rigorous, or, at random periods during

authentication, a re-evaluation of identity could be carried out.

16 Putting NIST To Work: An Application

The central authority model and NIST SP 800-63 both give possible solutions for the authentication problem that plagues America. However, as previously shown, both systems have their flaws that still allow for identity theft to occur. Firstly, the central authority model is merely a vague solution that has no substantial detail. The idea of forming a single, benevolent authority that stops all of the problems that plague society is impractical and naïve. Next, the model proposed by NIST will call for a variety of tokens to be given to individuals, with each token being used for a variety of different transactions. As shown, without proper user education, a thief can still commit identity theft under this system. In particular, the remote registration policies that NIST allows for will still permit for the common activities of dumpster diving and stealing mail and wallets that can be used to commit identity theft. On the other hand, if one was forced to register in person for each account that they possess, America would be filled with a tremendous amount of unhappy people. In a fast-paced world Americans do not want to wait to obtain a credit card.

Moreover, if one is required to have a token for all transactions in their life that require a form of authentication, the risk of identity theft will potentially increase. For instance, most of the tokens in the NIST publication require some form of password integrated with them. If an individual is required to have a password for each of their transactions that require a form of authentication, people will potentially be unable to remember all of the passwords that they have. As a result, the problem of writing passwords down could grow, thus causing these security procedures to be counter-productive. Also, due to the massive amounts of items requiring passwords, individuals might just resort to using the same password for all of their transactions. This would counteract the idea of having unique protection for different items as compromising one password (which has been shown to be fairly easy) can topple an entire system.

Hence, a system must be formulated that has the NIST authentication recommendations in mind but also recognizes the fast paced lives of Americans. Currently, the electronic wallet is slowly being adopted as a potential tool to combat identity theft. A system that incorporates the use of an electronic wallet along with modifications to the manner in which Americans receive sensitive information in the mail could be effective in stopping identity theft. However, without the strong cryptographic protection outlined by NIST or proper education of Americans about how identity thieves operate, such a system would only have minimal results in squelching the problem.

16.1 The Wallet of the Future

When someone is asked to define a wallet, the typical definition is a physical container that a person uses to hold their money, credit cards and other identifying information. While this conventional type of wallet is readily used in America, a new type of wallet is being used in other parts of the world and gradually making its way to American soil: the electronic wallet. The electronic wallet is a device that is used to store all of the information found in a wallet on an electrical device controlled by a computer chip. In particular, an electronic wallet can be used to download funds from a bank account. Then, much like the debit cards consumers are familiar with today, the electronic wallet can be used to purchase items. Moreover, the electronic wallet will also be able to function as a credit card and can even contain an electronic copy of a driver's license [4]. The idea of having an electronic wallet is something that was once only believed to exist in science fiction novels. However, the electronic wallet is something that is now being utilized in European and Asian countries.

16.2 How Is This Wallet Being Used?

While the idea of having everything in a physical wallet contained in a single electronic device might seem far-fetched, such a device is already being introduced to Asia. In the summer of 2004, a new generation of cellular phones, containing an embedded computer chip, went on sale in Japan. These new phones can be loaded with up to \$450 in electronic currency. Currently, the only way to load the phone with money is through the use of special machines but the phones will eventually have the capability to be loaded through electronic transfer. Once these phones are loaded with money, they can be used similar to debit cards at stores, restaurants and vending machines. One must merely wave the phone in front of a scanner and the amount of the purchase is deducted from the embedded chip. This new phone, besides being able to make phone calls, can also be used to pay bills as well [11]. Although electronic wallets can be implemented as standalone devices, it is rather convenient for such a wallet to be incorporated in an apparatus that is already widely used and familiar to people. In Japan, for example, there are 81.5 million cellular phones in a nation of 127 million people. Cellular phones are just as common place in America as more than 170 million Americans own cell phones. Introducing these new phones into the American marketplace will not require people to become familiar with an entirely new device. The electronic wallet will be merely viewed by consumers as an extra feature on an existing device. Thus, there is the potential for wallets such as these to become a part of American culture. As Naqi Jaffery, president of Telecom Trends International, a research firm in Falls Church, Virginia, states “And because of the uniqueness of cell phones - they’re always with you - one day, you will go to a store, take it out and make a payment for something. They will become that ubiquitous some day [14].”

16.3 Benefits of This New Wallet

The use of an electronic wallet brings many benefits to consumers. Since an electronic wallet is a hardware token, it should be incorporated with either a password or biometric in order to be operated. Moreover, as hardware token guidelines by NIST suggest, these tokens should be tamper resistant and have the capability of sounding an alarm and being remotely terminated if they are compromised. As a result, the simple task of stealing a wallet to acquire personal information no longer becomes so simple. No longer will this facet of identity theft be so simple that anyone can accomplish it. Instead, a criminal will have to be able to defeat cryptography and other computer security protocols to garner this sensitive information.

Under a system that use an electronic wallet, insecure paper mail credit offers can be eliminated. Instead, a system is in place where such offers can be electronically sent to the individual wallet. A consumer can have the option of downloading the new credit card functionality onto their wallet or simply refute it. Moreover, all documents containing sensitive information that are sent through insecure paper mail can be eliminated and, instead, be sent electronically to a wallet. As articulated previously, while identity theft may be initiated as a result of computer breaches, this is by far less common then initiated attacks not involving computers.

More importantly, new accounts can not be opened in a person's name without the possession of this token. No longer can credit applications be filed on the internet and instantaneously given or utility services ordered without proper authentication. If a new account is to be open, the electronic wallet must be present. The electronic wallet will therefore provide the high level authentication outlined by NIST and will also be convenient for consumers to use.

16.4 Security Risks of the Wallet

While the electronic wallet seems fundamentally like a good idea, as with other hardware tokens described in NIST SP-800, it is still vulnerable to attacks. First, there is the matter of registering for a wallet. It is imperative that in-person registration, specified as Level Three

or Level Four by NIST, would have to be used while dispersing these wallets. The potential pitfalls of registration have been discussed at length in the previous chapter. It should be made possible, through the cooperative interaction of businesses, that no one individual can have more than one wallet issued in his name.

Also, as discussed previously, while difficult, it is still possible to technically compromise this particular hardware token. Techniques may be developed to intercept digital communications or a clever criminal may be able to remotely take over the wallet. All of these techniques will require the time and money of a thief and, thus, will eliminate the common criminal from committing such a crime.

What still can take place - and this can be committed by any criminal of any skill level - is the use of social engineering to garner access to the wallet. Previously mentioned incidents, such as posing as Federal agents, can still be used to have an individual hand over their password and wallet. Moreover, if people write down their password and leave their token left unsecured, then committing identity theft will be as easy as before. As a result, the notion of a clear educational process for consumers utilizing these tokens is again pertinent. Under any system of authentication there are both security and educational issues and the use of an electronic wallet is no different.

17 Concluding Statements

Identity theft is clearly a significant problem in America. While it may be believed that this crime only affects the wealthy elite, the truth is that identity theft is a crime that crosses all demographics. According to statistics, one in twenty American adults have been victims of this crime and there are no signs that this epidemic will slow down. The reason that identity theft is such a rampant problem is that, much to the contrary of conventional belief, identity theft is a crime that is easy enough for anybody to commit for it is essentially just a two step process. The reason that fraud can so easily be committed is that there are no stringent authentication

procedures in place that ensure that an individual applying for credit or a service is who they actually say they are.

While services are offered, such as identity theft insurance and credit watch programs and recommendations are made to consumers such as securing mailboxes and shredding documents, the truth is they are merely serving as a band aid on a hole in a sinking ship. What really must be done is that a new system of authenticating Americans must be formed. Some of the recommendations made by NIST and even the use of electronic wallets can prove beneficial. However, in order for these authentication protocols to be effective, they first must be properly secured. Using cryptography and other security measures, it must be ensured that tokens that will be used for authentication are technologically sound. In order for an authentication system to truly be affective, the government must intervene to make authentication protocols not just recommendations that businesses can chose to enforce but actual laws that must be followed.

Equally important, Americans must be properly educated about the identity theft epidemic and how to handle the tokens they will be given to authenticate themselves. A system is only as secure as the people that are utilizing it and, therefore, equal efforts must be made to ensure that both humans and technology are sufficient to combat the epidemic. While identity theft might never be totally stopped, a combination of education and authentication can certainly significantly eliminate the crime of the 21st century.

References

- [1] ABC News. "Identity Theft." Feb. 9, 2004.
URL=http://abclocal.go.com/kabc/features/CONSUMER/020904_fs_identity_theft.html.
- [2] BBC Online. "Identity Theft: New Survey and Trend Report." Privacy & American Business: August 2003.
URL=<http://www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf>
- [3] BITS. "Financial Identity Theft: Prevention and Consumer Assistance." 2003.
URL=http://www.bitsinfo.org/BITS_pdf/Publications%20Page/bitsidtheftwhitepaper.pdf
- [4] Bleumer, Gerrit. "Electronic Wallets." August 11, 2003.
URL=<http://www.francotyp.com/research/bleumer/EncInfSec/GBI.ElectronicWallet.pdf>

- [5] Bolten, Joshua B. "Memorandum To The Heads of All Departments and Agencies." Office of Management and Budget. Washington, DC. 2003.
- [6] Bonner, Jesse. "Bankers, Law Enforcement 'phishing,' for Solution to I.D. Thefts." February 14, 2005. URL=<http://www.infozine.com/news/stories/op/storiesView/sid/5875/>
- [7] Burr, William E., Dodson, Donna F., and Polk, W. Timothy. "Electronic Authentication Guideline: NIST Special Publication 800-63." National Institute of Standards and Technology. Gaithersburg, MD. 2004.
- [8] Cable News Network "Thieves steal consumer info database" February 15, 2005. URL=http://money.cnn.com/2005/02/15/technology/identity_theft.reut/index.htm
- [9] CBS News. "All In The Family." Sept. 12, 2004. URL=<http://www.cbsnews.com/stories/2004/05/03/60minutes/main615304.shtml>
- [10] Church, Ellica. "Identity Theft 'scary' Surprise." News & Record. Accessed 2005. URL=http://www.news-record.com/news/local/uncgfraud_022505.htm
- [11] Community Developments Online. "Coming Soon: The Cellphone Wallet" URL=<http://www.occ.treas.gov/cdd/cellphonewallet.html>
- [12] Consumer Action. "Identity Theft." Accessed 2005. URL=http://www.consumer-action.org/English/CANews/2000_Spring_IdentityTheft.php
- [13] Court TV. "Man Steals Identity Of Sex Offender" Oct. 10, 2003. URL=http://www.courttv.com/people/scm/100903_ctv.html.
- [14] Eng, Paul. "Turning a Cell Phone Into A Virtual Wallet." URL=<http://abcnews.go.com/Technology/FutureTech/story?id=99516&page=1>
- [15] Equifax. "Equifax Credit Watch Overview." Nov. 17, 2004. URL=https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=cs_esn
- [16] Experian. "What Is Credit Fraud." Nov. 17, 2004. URL=http://www.experian.com/identity_fraud/fraud.html
- [17] Federal Trade Commission. "Federal Trade Commission: Your National Source for Identity Theft." URL=<http://www.consumer.gov/idtheft/>
- [18] Fight Identity Theft. "Fight Identity Theft: Citi Identity Theft Commercials." Jan. 5, 2005. URL=<http://www.fightidentitytheft.com/citibank-idtheft-commercials.html>
- [19] Givens, Beth. "The Saga of Shredding in the US: A Privacy Advocate's Perspective." May 21, 2004. URL=<http://www.privacyrights.org/ar/NAID.htm>
- [20] Identity Theft Resource Center. "Identity Theft: The Aftermath 2003, Conducted by Identity Theft Resource Center." September 23, 2003. URL=<http://www.idtheftcenter.org/idaftermath.pdf>

- [21] Javelin Strategy & Research. "2005 Identity Fraud Survey." 2005. URL=http://www.javelinstrategy.com/reports/documents/2005_Javelin_Strategy_Identity_Fraud_Survey_Complimentary_Report.pdf
- [22] MASSPIRG Education Fund. "A Road Map To Avoiding Credit Card Hazards." 2004. URL=<http://www.truthaboutcredit.org/roadmap.pdf>
- [23] May, George. "Stop Thief!" Journal of Texas Consumer Law: Spring 2002. URL=<http://www.idtheftcenter.org/IdentityV5N3.pdf>
- [24] Mercury News. "ID Thief Gets Prison: Losses May Have Totaled \$100 Million." Jan. 11, 2005. URL=<http://www.mercurynews.com/mld/mercurynews/news/10618771.htm?1c>
- [25] Mitnick, Kevin. *The Art of Deception*. Indianapolis, Indiana: Wiley, 2002.
- [26] Mohl, Bruce. "Massachusetts AG Seeks Tougher Identity Theft Law." The Boston Globe. Feb. 11, 2005. URL=http://www.boston.com/business/articles/2005/02/11/massachusetts_ag_seeks_tougher_identity_theft_law/
- [27] NewsNet5.com Staff. "Voter Scam Could Lead To Identity Theft." Accessed 2005. URL=<http://www.newsnet5.com/politics/3752778/detail.html>
- [28] Pinheiro, Robert. "Preventing Identity Theft Using Trusted Authenticators." Journal of Economic Crime Management: Winter 2004, Vol. 2, Issue 1. URL=http://www.jecm.org/archives/04_vol2_issue1_art2.pdf
- [29] Schneier, Bruce. *Secrets & Lies: Digital Security in a Networked World*. Indianapolis, Indiana: Wiley, 2004.
- [30] Silver Lake Publishing. "Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information and What to Do When Someone Hijacks any of These." Los Angeles, CA. 2004.
- [31] Sullivan, Bob. "The Meth Connection to Identity Theft." March 10, 2004. URL=<http://www.msnbc.msn.com/id/4460349/>.
- [32] Sullivan, Bob. "The Secret List of ID Theft Victims." Jan. 29, 2005. URL=<http://www.msnbc.msn.com/id/6814673/>.
- [33] Synovate. "Federal Trade Commission: Identity Theft Survey Report." Sept. 2003. URL=<http://www.ftc.gov/os/2003/09/synovatereport.pdf>
- [34] Teague, Dan. "Authorities: Scam Took IDs Of Deceased." Jan. 7, 2004. URL=<http://www.tecrime.com/llartI25.htm>
- [35] VeriSign, Inc. "Trusted Federated Solution Architecture." URL=<http://www.verisign.com/static/016543.pdf> 2004.

- [36] WESH Staff. "Nelson Says ID Theft Must Be Dealt With Immediately." WESH.com. Accessed 2005.
URL=<http://www.wesh.com/news/4234080/detail.html?subid=10100244>
- [37] Yip, Pamela. "Law Takes Aim At Identity Theft." Apr 4, 2004.
URL=<http://www.sunherald.com/mld/sunherald/business/8350794.htm>
- [38] Zicardo, Joe. "The burden is entirely on the victim to prove fraud over and over again." Privacy Rights Clearinghouse. Accessed 2005.
URL=<http://www.privacyrights.org/cases/victim7.htm>