IS COMPREHENSIVE FEDERAL DATA SECURITY LEGISLATION NECESSARY TO PROTECT U.S. BUSINESSES, CONSUMERS AND THE GOVERNMENT FROM IDENTITY THEFT AND OTHER CRIMES?

BY
ELIZABETH L. GARNER

A THESIS SUBMITTED TO JOHNS HOPKINS UNIVERSITY IN CONFORMITY WITH THE REQUIREMENTS FOR A DEGREE OF MASTER OF ARTS IN GOVERNMENT WITH A POLITICAL COMMUNICATIONS CONCENTRATION

BALTIMORE, MD
MAY 2008

© 2008 ELIZABETH L. GARNER
ALL RIGHTS RESERVED
Abstract

This thesis reviews the growing problem of identity theft and fraud that result from the misuse of stolen personal data, and seeks to determine whether or not comprehensive federal legislation is necessary to protect U.S. businesses, consumers and government from identity theft and other crimes. This thesis outlines the different ways identity theft can occur, the different risk levels associated with breaches, and who identity theft affects and how. This thesis explores existing laws and safeguards and their effectiveness in protecting financial institutions, business entities, education establishments, the federal government, and consumers from identity theft crimes and the theft of sensitive personal information.

This thesis addresses two schools of thought: 1) the data security status quo is sufficient, and 2) data security should be more highly regulated at a federal level. In doing so, it analyzes pending federal data security legislation and the potential for movement in the 110th Congress. Lastly, this thesis reviews emerging technologies and how they relate to the growing threat of identity theft.

This thesis finds that a national standard for data security breach notification, credit freeze policy, and social security number safeguards would be beneficial because of confusing state laws. However, this thesis guardedly recommends a national standard since the private sector has relatively strict data security regulations and compliance standards in place, and during the political process, pre-emptive federal legislation could end up creating unnecessary mandates for the private sector, and with ever-increasing criminal technologies, it will be virtually impossible to thwart identity theft criminals’ attacks one hundred percent of the time.
This thesis finds cybersecurity to be a more imminent threat than identity theft and recommends that federal lawmakers address cybercrime before basic data security standards. Cyber criminals are becoming more organized, and with emerging technologies, the anonymity of the Internet, and use of the Internet as a sharing tool, cyber criminals pose a real threat to U.S. national security. Coupled with deficient information security standards at the majority of U.S. federal agencies, the threat of a large scale cyber attack on U.S. infrastructure is imminent and must be addressed first and foremost.
# Table of Contents

## I. Chapter 1: Introduction

- Overview
  - p. 1
- Loss Resulting from ID Theft
  - p. 2
- Distinction in Type of Breach
  - p. 1
- Schools of Thought: Existing Standards are Strict Enough vs.
- More Should Be Done to Curb Identity Theft vs.
- Some Standards Should be Revisited
  - p. 7
- Support Data Security Status Quo
  - p. 8
- Increase Data Security Initiatives
  - p. 9
- Outline
  - p. 9
- Potential Problems
  - p. 11
- Political Feasibility
  - p. 11

## II. Chapter 2: Background

- What is Identity Theft and Why Is It a Problem?
  - p. 13
- How Does Identity Theft Occur? What Types of Breaches Exist and What Risk Levels are Associated with Those Breaches?
  - P. 14
- What Type of Fraud Results from Identity Theft? Who Does Identity Theft Affect? Where is it Most Prevalent?
  - P. 16
- Why Does Identity Theft Matter
  - p. 22
- Who has Acknowledged This as a Problem? Who is Funding Prevention Methods and Consumer Resource Centers?
  - P. 24
- How well-educated are Consumers, Businesses, etc. in regard to Identity Theft Prevention and Reaction Methods?
  - P. 28
- What Policy Issues Exist in Regard to Identity Theft?
  - P. 31
- What will the Rest of this Thesis Address? How Big of a Problem is Identity Theft Really?
  - P. 35

iv
III. **Chapter 3: Existing Safeguards on Personal Data**

What Laws and Safeguards are Already in Place? P. 41
What Existing Laws and Safeguards Apply to
Financial Institutions? P. 43
What Existing Laws and Safeguards Apply to Retailers
and Other Private Sector Businesses? P. 45
What Existing Laws and Safeguards Exist for
Education Institutions? P. 56
What Existing Laws and Safeguards Exist for the
Federal Government? P. 57
What Precedents Did the Veteran’s Affairs Breach Bill Set? P. 65

IV. **Chapter 4: Should Data Security Be More Highly Regulated?**

*If so, What Additional Regulations Should be Employed?* P. 67
Which Groups Think Status Quo Data Security Laws
are Sufficient? P. 68
Which Groups Think That Some Data Security Standards
Should Be Reformed or Enhanced? P. 69
Which Groups Think Data Security Need Increased Regulation? P. 73
What Federal Legislation Is Being Proposed By Those Who
Think Data Security Needs to Be More Highly Regulated? P. 75
What are those who Think Data Security Needs to be More
Stringent Proposing at a State Level? P. 81
What are Existing International Standards? P. 85
V. **Chapter 5: The Challenge of Emerging Technologies, Policy Recommendations, Political Feasibility, and the Importance of this Research**

Emerging Challenges/Related Issues/ Why Identity Theft is an Evolving Problem p. 87
Policy Recommendations p. 95
Political Feasibility p. 105
Difficulties with This Study p. 107
Why is this Research Important? p. 108

VI. **Glossary of Terms** p. 110

VII. **Bibliography** p. 114
Charts & Graphs

Risk Associated with Different Kinds of Data Breaches  p. 21
Victim Age  p. 23
Time Between Identity Theft and First Discovery  p. 24
Time Spent Resolving Identity Theft Problems  p. 26
Out of Pocket Payments by Victims  p. 27
Chapter 1: Introduction
Overview

For the seventh straight year, identity theft has topped the Federal Trade Commissions top 20 list of consumer fraud complaints. The risk of identity theft is real and prevalent in today’s society with massive of amounts of personal sensitive information available via online networks. According to a June 2007 report by the Government Accountability Office, “as a result of advances in computer technology and electronic storage, many different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers.” Government agencies store social security numbers and health records, retailers store credit and debit card account information for processing purposes, and financial institutions handle personal data, such as social security numbers, when a customer opens an account or applies for a loan.

Certain security measures and laws are already in place to help prevent the theft or accidental loss of this data; however, those laws and security measures fail to protect personal information 100% of the time and the threat of identity theft is prevalent and very real. Identity theft can occur in a variety of ways: through loss or theft of a laptop containing sensitive personal information, hacking into a private network, loss of paper records with sensitive information, compromising of computer logins and passwords, and skimming (where thieves install an instrument on card readers to steal credit and debit card data when the cards are scanned). While there are many fail-safes currently in place to help prevent and deter against identity theft, more could be done to curb the problem,

---

2 “Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown.” Report to Congressional Requestors. Government Accountability Office. June 2007, p. 1.
which appears to be growing with the increased use of the online marketplace and ever-evolving new technologies, which can be utilized by identity theft criminals to help extract sensitive data in-transit, stored on computer networks, or even using radio frequency identification (RFID) technology to extract consumer card data using a scanning device.

Identity theft is crippling to individuals, businesses, financial institutions and government because it is costly, reduces consumer and citizen confidence in affected businesses and branches of government, and it can create a security threat if certain federal agencies who maintain sensitive national security information are victims of a breach. Incidence levels of identity theft have begun to rise with the increased use of electronic payments and the Internet. The Federal Trade Commission (FTC) has documented a large increase in the number of identity theft victims over the past couple of years. This increase, coupled with overall high information security inefficiencies within federal agencies, poses not only a risk of identity theft through the loss of sensitive personal information, it also opens the door for wider information security standard reform. It poses a national security threat for our government’s electronic infrastructure. By in larger, the private sector does a better job of protecting access to personal data – one can postulate that increased efficiency and security is a result of market competition in which private retailers and financial institutions want to avoid low consumer confidence levels. National security implications for cyber security will be addressed in this thesis 1) because government breaches can result in identity theft; and 2) because federal agency breaches can pose serious national security threats as open and accessible electronic government networks could prove problematic for the U.S. in
dealing with foreign nation states and sub-state groups. One need not look further than the Estonia incident (ref. p. 39) in the spring of 2007 to realize that the economic and national security threats posed by cybercrime are very real.\(^3\) Since 2004, Congress has recognized the threat cybersecurity poses to our nation. As then Chairman of the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Rep. Adam Putnam (R-FL) said in his opening statement at a hearing on identity theft, “I am not convinced that we are prepared in either the public or private sector to adequately deal with these problems. I fear that cybercrime may get worse before it gets better, and I do not wish to wait for some large-scale failure of our Internet infrastructure or the launch of a combined physical and confined cyberattack against our citizens and our economy before we as a Nation get serious about protecting our information systems.”\(^4\)

It is important to note that the author of this thesis was employed by the Food Marketing Institute, a trade association representing supermarket retailers and wholesalers, from December 2005 to January 2008. The author also participated in Coalition for Data Security meetings on behalf of the Food Marketing Institute during that time period and as such is somewhat biased in her approach. The author is currently employed by the Merchants Payments Coalition, which consists of retail trade associations such as the Food Marketing Institute, National Association of Convenience Stores, the National Retail Federation, etc, and as a result may have additional biases

---


favoring the retail community over financial institutions in terms of breach and fraud liability.

**Loss Resulting from Identity Theft**

The mental harm inflicted on identity theft victims is similar to that of violent crime victims. Not only can identity theft make an individual feel less secure, it can put a strain on existing relationships because of psychological and economical hardships that the victim endures and is forced to cope with. Additionally, identity theft victims often bear substantial financial losses, as well as hours of lost time. A victim of identity theft may have money withdrawn directly from their bank account, may be denied a loan due to poor credit resulting from the theft, and may have their credit histories and financial records severely altered. In most cases, identity theft victims are liable for only a minimal amount of all financial monetary loss; however, in the aftermath of a theft, they often have to spend hours of their time recovering false charges and straightening out fraudulently created new accounts.

Businesses and financial institutions also face losses from identity theft. Consumers who feel that they are at risk for identity theft due to any type of data security breach or loss or theft of personal information, can freeze their credit, which is costly for credit reporting agencies, as well as financial institutions who may lose business as a result of frozen consumer credit. Additionally, consumer confidence is at stake in the retail industry. If consumers feel that their personal information is not being properly safeguarded, they are less likely to shop at the retail establishment they perceive to have lax security standards. If a large-scale retail data breach occurs, significant costs are incurred either by the retailer or financial institutions for the reissuing of credit and debit
cards to all potentially affected consumers, as well as the cost of issuing a breach notice in some instances. In some states there is a “reasonable” risk of harm standard that must be associated with the breach in order for a mandated breach notification to be sent; however, other states employ a standard which calls for mandatory notification any time personal data is compromised even if there is limited risk of harm resulting from that breach.  


**Distinction in Type of Breach**

This thesis will address different types of data breaches and the risk levels associated with each type. This thesis will also address the efficiency of the private sector vs. the government and education institutions in the safeguarding of sensitive data, as well as existing industry standards that require compliance with certain security standards in regard to Sarbanes Oxley, HIPAA, and Payment Card Industry data.

There are two major types of breaches: account level and identity level. An account level breach includes data found on a credit or debit card. An identity level breach includes information which serves as personal identifiers, such as name and address coupled with social security numbers and/or date of birth. Identity theft is much less likely to occur in the incidence of an account level breach, since access to personal records and the ability to open a new account or apply for a loan is limited without a social security number or other identifying factor. Account level breaches can still be harmful as they can result in significant financial loss; however, they are less likely to result in identity theft.
The risk of identity theft that results from a breach depends heavily on the manner in which the data was compromised. Unintentional loss of data yields very little risk of harm from the breach, while intentional loss of data or theft increases the risk of harm associated with the breach because the data was taken with malicious intent. Existing state laws and a number of pending federal bills take into account the different levels of seriousness associated with each type of breach by requiring a data breach notification only when a “reasonable” risk of harm exists. Along those lines, policymakers should take into account the differing severity of breaches and risks associated with those breaches in an effort to identify the most appropriate way those breaches can be handled.

Breach notification is a very contentious issue because consumer groups argue that individuals have a right to know any time their data has been compromised; however, if “reasonable” risk of harm does not exist, breach notification causes undue fear, is costly to retailers and financial institutions, and most importantly, desensitizes consumers.

Excessive breach notification runs the risk of being the next credit card solicitation – the mail you receive two to three times a week, glance at briefly, tear up and throw away immediately - which provides little value to consumers at a high cost for businesses.

II. Schools of Thought: Existing Standards are Strict Enough vs. More Should Be Done to Curb Identity Theft vs. Some Standards Should be Revisited

There are three main schools of thought in regard to data security standards that help prevent against identity theft and fraud. The first is that the status quo for data security is substantial and increased regulation is not needed. A need for lessened data security standards will not be addressed in this thesis because existing laws are not overly

7 Ibid. pgs. 7 – 8.
restrictive or overly regulated, and thus there is little evidence that a school of thought exists that calls for decreased data security standards. The second is that data security should be more highly regulated. Some believe that the existing laws are not sufficient enough and not effectively regulated. Some members of this school of thought favor increased security through a combination of stricter federal and state legislation while others believe a national standard should replace the existing state laws. The final school of thought involves adopting some new data security standards at either a federal or state level, but believes that some or most of the existing data security safeguards are sufficient. For example, this group may believe that increased safeguards on social security numbers should be implemented, but increased data breach notices should not. The third school of thought will be revisited in a breakdown of policy recommendations for a number of different issues that relate to data security and identity theft.

**Support Data Security Status Quo**

This section will address existing federal and state data security laws and standards and their effectiveness in promoting sound data security standards. It will also address the effectiveness of the current laws in preventing and deterring against identity theft. Groups that support the data security status quo argue that strict data security standards are already in place. For example, most businesses and financial institutions are subject to the Fair and Accurate Credit Transactions Act, Gramm-Leach-Bliley, Payment Card Industry Data Security Standards, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley reporting requirements, and other data security
safeguarding initiatives. As such, most businesses and financial institutions belong to this school of thought.

**Increase Data Security Initiatives**

A second school of thought is that information and data security standards should be more highly regulated. Most consumer groups feel that individuals are placed at undue risk by the failure of both public and private entities to safeguard sensitive personal information. This school of thought calls for stricter laws at both the state and federal level. It also appeals for increased enforcement of the existing laws. There are a number of pending bills in the 110th Congress, as well as in states where data security laws have not yet been enacted so a number of federal and state legislators support initiatives for increased data security standards or the creation of a national standard. This group also supports increased prevention measures and consumer and business education. The third school of thought involves a combination of status quo requirements combined with the addition of a few new laws or the creation of a national standard for existing laws. Credit freeze, social security number use, oversight, and breach notifications are a few of the policy issues where this group will vary in their policy recommendations.

**Outline**

The second chapter of this thesis, following the introduction, will provide background information detailing the different ways in which identity theft occurs, the distinction between type of breach, the risk of harm from those types of breaches, how consumers are affected by identity theft, and how well-educated consumers are in regard
to identity theft. This chapter will also explore the types of losses (economical, psychological, etc.) retailers, consumers, governments and financial institutions face in regard to identity theft. This chapter will also review who is most affected by breaches, how long it takes victims to notice that they are identity theft victims, and how well-educated consumers are on the proper preventative and reactive measures to anticipated identity theft.

The third chapter will address existing state and federal laws and regulations in regard to data security standards. It will also address the efficiency of the private sector, government and education institutions in safeguarding data, and it will explore the arguments of groups who feel that the information security status quo is sufficient to protect individuals from identity theft, and will explore the possibility that while identity theft may not be prevented wholeheartedly under the current system, there is unlikely to be a feasible and affordable alternative policy to the status quo.

The fourth chapter will address the school of thought that information security needs to be more highly regulated. It will address the concerns of consumer groups and others who feel that current data security standards are not stringent enough at either or both the federal and state level. It will also address pending state and federal legislation. And will take into account international standards with particular emphasis on the European Union. The fourth chapter will also briefly address a combination of the two other schools of thought as this thesis leads in to policy recommendations.

The fifth chapter will contain the policy recommendations derived from this thesis. It is anticipated that the policy recommendations will be for increased security standards in the public sector, but not the private sector, support for some, but not all, of
the components of federal and state legislation proposed to help prevent identity theft in
the event of a breach. This chapter will also address emerging technologies and the need
for both public and private institutions to keep up with the tactics employed by data
security thieves in order to adequately prevent against identity theft. Additionally, it will
address the shortcomings of some new payments technology. It will also cover the
increasing threat of cybercrime resulting from emerging technologies, and the danger of
federal agency exposure to cybercrimes because of lax government information security
standards, and the threat that poses to U.S. national security.

**Potential Problems**

It will be difficult to link specific data breaches with specific cases of identity
theft. Additionally, identity theft is a relatively new problem, at least at the current scale,
since electronic transfer and electronic data storage is a relatively new phenomenon so
existing data will be limited. It will be difficult to measure the effectiveness of current
policies, and as such, this thesis will rely heavily on GAO reports, and other academic
studies, for the state of data security standards. This thesis will also address the
viewpoints of special interests groups, and it will be difficult for the author to remain
unbiased as a result of her aforementioned employment by the retail community.

**Political Feasibility**

Data security legislation is unlikely to move in the 110th Congress because of the
shortened legislative agenda in an election year, in which Congress still needs to address
many more important issues. Another large scale data breach, which puts consumers at
high risk, could fast track data security legislation, but otherwise, it will be put on hold until the 111th Congress. The House of Representatives is unlikely to switch majority parties in the next election so Rep. Barney Frank (D-MA) is positioned to remain chair of the House Financial Services Committee. He has stated that data security is a top issue for him so if other timely issues are resolved (i.e. the subprime mortgage crisis) he will be able to focus on other priorities, such as data security. Jurisdictional issues have also caused legislation to stall in both the House and the Senate. Identity theft remains a key concern for consumers and as identity theft is linked closely with data security, constituents will likely remain motivated in asking their legislators to address this growing problem. As the U.S. trends toward increasing electronic payments and electronic infrastructure (i.e. online financial institutions and government), it is critical that the nation safeguard sensitive personal information in an efficient manner in order to protect U.S. citizens from financial harm and give peace of mind to consumers, retailers, financial institutions, and the government.
Chapter 2: Background
What is Identity Theft and Why Is It a Problem?

According to the Federal Trade Commission (FTC), “Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.”

Sensitive, personal identifying information can be compromised in a number of ways, many of which will be discussed in further detail in this thesis. The threat of identity theft in today’s society is very real and continues to grow. According to the U.S. Department of Justice Statistics, “identity theft is now passing up drug trafficking as the number one crime in the nation.”

As government, retailers, and financial institutions rely more heavily on the Internet for everyday business practices, the threat of identity theft will continue to exist and mature.

There are numerous ways in which identity theft can harm consumers. A fair amount of consumers can resolve account-related fraud and other identity theft crimes rather quickly; however, there is another set of victims who may spend hundreds of hours and thousands of dollars trying to repair the ills of identity theft. Identity thieves can open new accounts, which they often let go delinquent, and they may apply for loans, which they don’t end up paying off. Both actions have severe consequences for the identity theft victim whose credit report is tarnished by this activity and who might experience resulting problems when taking out a loan, applying for a mortgage, or having a potential employer run a credit check. Identity theft creates both emotional and financial stress that

---

10 FTC website. Online: http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html
affects both victims and their families and is a legitimate concern among many Americans.

Identity theft has topped the list of FTC consumer complaints for the past seven years.\textsuperscript{11} Identity theft was the number one complaint for 36 percent (246,035) of all 2006 FTC Identity Theft Survey Report respondents far surpassing the second place complaint, shop at home/catalog sales, which was the number one complaint for 7 percent (46,995) of respondents.\textsuperscript{12} The FTC-sponsored survey, released November 27, also estimated that over 8.3 million adults in the U.S. were victims of identity theft in 2006.\textsuperscript{13} Additionally, as chair of the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Senator Dianne Feinstein (D-CA) said in her opening statement in a hearing on identity theft, “since the beginning of 2005 . . . over 100 million data records containing individuals most sensitive personal financial data, health data, and other kinds of data, have been exposed due to data breaches.”\textsuperscript{14} Identity theft is a serious issue because it affects millions of people from a wide array of groups: consumers, businesses, financial institutions, information brokers, the education and medical sectors, and government.

Consumer fears regarding identity theft run high, which is not surprising given the media attention identity theft has received of late. According to a Zogby International
poll, “91 percent of people surveyed said they were ‘worried’ about identity theft.”\textsuperscript{15} Survey respondents were also very wary about retailers handling their sensitive personal information: “83% of Americans were concerned that information provided to retailers could end up in the hands of others, either through theft or sale, [and] 34% said they were not confident that retailers, credit card companies, banks, and other firms that have detailed records of customers’ personal information are taking the appropriate steps to safeguard that data.”\textsuperscript{16} Media coverage of recent retail breaches has not helped the public perception of retail data security protections even though existing security standards are rather high, and a number of breaches have occurred as a result of new technologies identity thieves are just now beginning to utilize. These new and innovative technologies make identity theft and fraud continuously evolving crimes. But is there really a very high risk that consumers will have their identity stolen any time their data is compromised? The sensitivity of information compromised and the manner in which it is obtained are major factors in whether or not individuals are at risk for identity theft. In most instances, the risks associated with data breach are minimal. This thesis will address the different levels of risk associated with different types of breaches later on in this chapter.

\textbf{How Does Identity Theft Occur? What Types of Breaches Exist and What Risk Levels are Associated with Those Breaches?}

\textsuperscript{15} Zogby Poll: Most Americans Worry About Identity Theft. “Survey shows vast majority concerned companies may sell their information or are not doing enough to keep it safe from theft” Released: April 03, 2007. \texttt{http://interactive.zogby.com/index.cfm}

\textsuperscript{16} Ibid.
“Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information.” Thieves can obtain this data in a number of ways, many of which are listed below. The FTC cites the following ways in which personally identifying information can be compromised:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.”

Skimming and phishing are two of the newest forms of theft. A breach of northeastern supermarket chain Stop & Shop Company customer data in early 2007 resulted from a skimming operation where thieves put skimming devices on a number of point-of-sale devices in one of the stores. Additionally, in just one year the number of detected phishing websites more than quadrupled. Phishing is defined as “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently

---

17 FTC Website.
18 Ibid.
19 Identity Theft Resource Center Website.
retrieve legitimate users’ confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion;” this type of novel communication is used to elicit confidential information from victims.\textsuperscript{20} A recent University of Indiana study found that 14\% of phishing scams are successful,\textsuperscript{21} and it is likely that number will continue to grow as phishing scams become more prevalent. The University of Indiana study sent out a phishing email pretending to be from eBay; the link embedded in the email did link the person to eBay’s website, but it sent a message back to the school telling them when the link was clicked.\textsuperscript{22} PayPal is also a site often used to “lure” in victims, and sophisticated attackers will even warn against linking to sites via email communications to throw off their victims and make them think the phishing email is legitimate since Internet users have a hard time believing attackers would give them a warning.\textsuperscript{23} Phishing is a growing problem that must first be addressed with increased consumer education, as not many people know exactly what phishing is since it’s a relatively new technique and is a rather complicated tactic to grasp for Internet user who are not the most technologically savvy. Phishing is estimated to cost U.S. financial institutions up to $1 billion annually in direct losses, and as such, should not be taken lightly.\textsuperscript{24} Additionally, Symantec found that 904 phishing messages were sent a day for the second half of 2006, up 6\% from the first half of the year, which indicates that phishing could continue to grow into an even bigger problem.\textsuperscript{25}

\textsuperscript{21} Identity Theft Resource Center Website.
\textsuperscript{22} Ibid.
\textsuperscript{23} Jakobsson, Markus and Myers, Steven. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. P. 10
\textsuperscript{24} Ibid. P. 31
\textsuperscript{25} Digital Transactions. Volume four, number eleven. November 2007. p. 34
In addition to the six types of loss addressed by the FTC, other forms of hacking such as in-transit data theft, as well as loss of property are also relevant causes of data breaches and identity theft. Hackers can gain unauthorized access to sensitive database information through the Internet. For example, hackers gained access to education records in the University of California Los Angeles (UCLA) breach by hacking into online records via the University network. Federal agencies, as well as their servers and internal communications, are also susceptible to hackers, which was realized in recent attacks on the Department of Energy and Department of State. Data breach can also occur when retailers transfer point of sale information electronically to the financial institutions which support their payment processing. This type of breach also falls under the umbrella of hacking. Some account level data that is transferred this way is unencrypted, and crimes of this nature are just now being realized as vulnerable. The Hannaford Bros. data breach (ref p. 49), which occurred in early 2008, was a result of this type of technology. Now that one set of thieves have proven that this type of data extraction is possible, future scams are sure to ensue.

In addition to sophisticated technology, simple loss of property is one of the most prominent ways in which data is compromised. If a laptop containing unencrypted sensitive data is lost or stolen, it puts individuals with records on that laptop at risk. According to the Identity Theft Resource center, “the U.S. Government Reform Committee reports that all 19 government departments and agencies reported at least one loss of personally identifiable information since Jan. 2003. . . the vast

27 Ibid.
The majority of losses occurred from physical thefts of portable computers, drives and disks, or unauthorized use of data by employees.28 However, while data breach resulting from loss of property may be prevalent, it is one of the least likely forms of data compromise to result in identity theft, especially if the data is compromised due to loss instead of theft. Additionally, a 2006 study by the Penemon Institute found that 45% of data leaks result from lost or stolen laptops while 29% result from records lost by third-party businesses, 26% resulted from misplaced or stolen files (such as those on portable USB drives), and 10% resulted from malware programs.29 A malware intrusion is when malicious software runs on a users’ computer causing data compromise; malware programs often result from phishing scams.30 Such a high number of laptop losses or theft is especially problematic because it is very costly, and also very difficult to prevent.

There are very distinct levels of risk associated with the type of data compromised in a breach and the way in which the data was compromised. An account level breach is loss of account information, such as the details on a credit card, name and account number, while an identity level breach is loss of other personal sensitive data, such as name, address, date of birth and social security number.31 An identity level breach is more serious because identity level data can more readily be used to steal an individual’s identity while an account level breach usually only results in fraud on existing accounts. Loss of one’s social security number is particularly sensitive because, coupled with other

---

28 Identity Theft Resource Center Website.
29 Ibid.
sensitive data (i.e. name, address), a thief can set up a new bank account, apply for a loan, etc. – all things that are more difficult to detect than suspicious activity on an existing account.  

Risk Associated with Different Kinds of Data Breaches

Source: ID Analytics

The way in which data is compromised is also very important in the determination of risks associated with the resulting from the data breach. Accidental loss results in the least risk, while incidental theft is a bit more risky, and intentional theft is the most risky. Intentional theft is the riskiest type of data breach because it is data stolen with malicious intent and is more likely to be misused. Incidental theft is when data is stolen as part of another crime. This is risky because it still involves malicious intent, but there is no way to know whether or not the thieves have plans or the ability to use the

---

32 Ibid. pgs. 7 - 8  
33 Ibid. pgs. 7 - 8  
34 Ibid. pgs. 7 - 8
compromised data. Accidental loss is the least risky because there is no devious intent and it is highly unlikely that the compromised data will be misused.

**What Type of Fraud Results from Identity Theft? Who Does Identity Theft Affect?**

**Where is it Most Prevalent?**

Thieves use personal sensitive information to perform a number of criminal activities. The first is credit card fraud, which accounts for 25% of all identity theft crimes. Credit card fraud can occur through the opening of new credit card accounts in a victim’s name, which can become delinquent when not paid and negatively affect the victim’s credit report. Phone or utilities fraud accounts for 16 percent of identity theft crimes, and involves opening a new wireless account or running up charges on an existing account, while bank or finance fraud also accounts for 16 percent of all identity theft crimes and can involve the creation of counterfeit checks, the opening of a new bank account under the victim’s name, the usage of the victim’s debit/checking account, or taking out a loan in the victim’s name. Government documents and other types of fraud account for the remainder of identity theft crimes.

Identity theft among 18 to 29 year olds is the most prevalent. According to the 2006 FTC survey, 29% of ID theft victims are ages 18 – 29, 23% are ages 30 to 39, and 20% 40 – 49.

---

36 Ibid. p. 5.
37 Ibid. p. 5.
38 Ibid. p. 7.
Source: FTC Identity Theft Victim Complaints Survey\textsuperscript{39}

There are several reasons 18 to 29 year olds are the most vulnerable age segment: 1) theft could occur from living in roommate situations, 2) they are more apathetic about identity theft in general and think it could never happen to them, 3) they are a larger segment of Internet users and are more likely to fall prey to hacking or phishing scams, 4) and they are more likely to bank online and make credit and debit card purchases over the Internet. According to Celent LLC, 13\% of banking customers banked online in 2004, and that number is expected to increase to 22\% by the year 2010,\textsuperscript{40} which could potentially make it more difficult for banks to protect against identity theft.

Age is not the only characteristic that increases the likelihood that someone will fall prey to identity theft; location also plays a large role. The top 10 states where identity theft occurs are (in order): Arizona, Nevada, California, Texas, Florida, Colorado, Georgia, New York, Washington, and New Mexico.\textsuperscript{41} Increased identity theft in certain states is important to note because some might argue that immigration and identity theft

\textsuperscript{39} Ibid. p. 7.
\textsuperscript{41} “Identity Theft Victim Complaint Data: January 1 – December 31, 2006.” P. 9.
run hand in hand. As mentioned, a number of identity theft criminals use stolen data to obtain government documents, and some might argue that this type of misuse is higher in states with large immigrant populations. Identity misuse as it relates to immigration is not something this thesis will cover in depth as there is little evidence that the two issues are strongly related. Identity theft incidents by state is also important background to have when examining the existing and pending state laws and their level of regulation in regard to credit freeze, breach notification standards, and other data security policy issues.

A major problem with identity theft is the time lag it takes for victims to identify that a problem exists.

\[
\text{Time Between Identity Theft and First Discovery}
\]

\[
\text{January 1 - December 31, 2006}
\]

\[
\begin{array}{|c|c|}
\hline
\text{Time} & \text{Percentage} \\
\hline
\text{Less than 1 Month} & 45\% \\
\text{1 to 6 Months} & 17\% \\
\text{7 to 12 Months} & 7\% \\
\text{1 to 2 Years} & 9\% \\
\text{2 to 4 Years} & 11\% \\
\text{4 to 5 Years} & 3\% \\
\text{Over 5 Years} & 9\% \\
\hline
\end{array}
\]

Source: FTC Identity Theft Victim Complaints Survey \textsuperscript{42}

Identity theft crimes can go undetected for an extended time period with the potential to cause great harm to the victims – both emotional and financial. The 2006 FTC survey found that 45\% of victims discovered evidence of misuse in less than 1 month; 17\% 

\textsuperscript{42} Ibid. p.11.
within 1 to 6 months; 7% within 7 to 12 months; 9% within 12 to 24 months; 11% within 25 to 48 months; 3% within 49 to 60 months; and 9% over 60 months. The longer identity theft crimes go on, the more financial and credit harm they can cause their victims. Since some identity theft victims are unaware that their personal data has been compromised in the first place, they do not have any suspicion of criminal activity and are not actively looking for devious behavior. Detecting new account or loan fraud is often difficult because thieves will use a different address to establish an account, and often by the time the discrepancies are discovered, the criminals have already done quite a bit of damage to the victim’s credit report.

Why Does Identity Theft Matter?

Both the emotional and financial stresses associated with identity theft are high. The Identity Theft Resource Center claims the “emotional impact on victims is likened to that felt by victims of more violent crime, including rape, violent assault and repeated battering. Some victims feel dirty, defiled, ashamed and embarrassed, and undeserving of assistance.” The Bush Administration also agrees that victims of identity may suffer beyond financial harm as “criminals committing identity theft can harm reputations, [and] create greater stress in family life and other relationships.” Additionally, victims often spend a significant number of hours trying to straighten out incidences of identity theft with their financial institutions and credit reporting agencies.

---

43 Ibid. p.11.
44 Identity Theft Resource Center Website.
While some victims are entirely successful in their recovery efforts, others have difficulty recouping full financial loss and are sometimes unable to entirely expunge negative effects the criminal’s activity may have had on their credit reports.

Most financial loss resulting from fraud related to identity theft is covered by banks and financial institutions; yet, sometimes victims may end up paying some out of pocket expenses. Financial losses have the potential to be significantly greater in the event of an identity level breach because of the additional ways in which the thief can use information, and the added difficulty in detecting such an incidence of fraud. Even though 59% of victims incurred no out-of-pocket expenses, 30% of that group experienced one or more annoyance, such as lost time in trying to resolve their identity theft problems.  


While some victims are not directly financially affected, they suffer other losses, such as emotional, physical, and financial strain from time lost that could have been spent doing something else.

---


Financial loss to businesses, financial institutions, and government resulting from identity theft is also considerable. “The loss or theft of just one laptop can cost a company as much as $90,000 or more in fines, credit monitoring for victims, public relations damage control, and class action litigation.”<sup>49</sup> While it might be difficult to prevent this type of data breach, it is certainly in the financial best interest of both private companies and government entities to attempt to reduce laptop loss or theft, or at least to encrypt and/or password protect all laptops to prevent misuse of sensitive data in the event of a compromise. Additionally, regardless of whether or not data is misused, a data breach can still be very costly to businesses. A 2006 study by the Ponemon Institute found that the average cost to U.S. companies per compromised data record was $182 resulting from lack of consumer confidence, breach notification, investigations, customer support, legal and auditing expenses, and overall security costs.

standard increases. Overall, there is a huge financial incentive for companies to avoid data breach and the negative business image and economic effects associated with a breach. A decrease in consumer confidence is one of the worst consequences businesses face in the aftermath of a data breach because it affects whether or not shoppers choose to visit their store. The current administration has been very conscious of the toll identity theft can have on American business and they have acknowledged that identity theft affects businesses of all sizes and can have “adverse effects on the economy as a whole by making some people feel less confident about engaging in electronic transactions and by increasing the costs to consumers as businesses undertake additional measures to protect customers' personal data from identity thieves.” Overall, a number of groups have recognized the threat identity theft and fraud pose to a number of different individuals and organizations, and are funding efforts to combat this evolving problem.

**Who has Acknowledged This as a Problem? Who is Funding Prevention Methods and Consumer Resource Centers?**

Congress addressed the growing problem of identity theft first and foremost with passage of the Identity Theft Assumption and Deterrence Act of 1998, and more recently the Bush Administration has expressed an increased interest in identity theft. In May of 2006, the White House issued an Executive Order, which among other things, created the President’s Identity Theft Task Force to make strategic recommendations to the administration on how best to control the growing problems of identity theft and data

---

50 Ibid.
51 “White House Fact Sheet: The President’s Identity Theft Task Force.”
security.\textsuperscript{52} Additionally, the Task Force’s goal is to increase consumer education efforts and enhance cooperation of law enforcement officials in their response to identity theft crimes.\textsuperscript{53} The actual recommendations of the Task Force will be addressed in the next chapters of this thesis.

The Bush administration continued to show their commitment to fighting identity theft by requesting additional funding for the FTC to back the FTC campaign against identity theft. The President’s proposed budget for fiscal year 2008 proposed a $17 million increase in funding for the FTC, $12 million of which would finance the agency’s consumer protection initiatives including the fight against identity theft.\textsuperscript{54} The increased funding would likely go toward the FTC Privacy and Identity Protection program, “which was created to enforce relevant statutes and rules, develop policy, educate consumers and businesses, and analyze the impact of legislative initiatives.”\textsuperscript{55}

The Department of Justice has also recognized the ongoing threat identity theft poses to consumers and businesses, and has made an effort to allocate funds to groups who help educate consumers on identity theft, as well as groups who assist victims in various regions throughout the country. At the end of 2007, the Department of Justice awarded $1.7 million in grant funds to these organizations – a significant amount when other crime assistance grants that groups can apply for are $200,000 grants.\textsuperscript{56} The

\begin{thebibliography}{99}
\bibitem{52} Ibid.
\bibitem{53} Ibid.
\bibitem{54} President’s Proposed Fiscal Year 2008 Budget. Online: \url{http://www.gpoaccess.gov/usbudget/fy08/pdf/appendix/oia.pdf} pg. 1084 - 1086.
\end{thebibliography}
Identity Theft Resource Center, a national organization providing free assistance to identity theft victims received $500,000, while the Texas Legal Services Center, which provides regional (Texas, New Mexico, Colorado, and Oklahoma) support and free legal services to identity theft victims through it’s VICARS (Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest) program, also received $500,000, and another regional support group, the Maryland Crime Victims’ Resource Center, received $500,000. The remaining $200,000 was presented to Atlanta Victim Assistance, Inc. to carry out a public education campaign aimed at stopping identity theft and financial fraud. Overall, DOJ’s commitment to helping these organizations demonstrates their ongoing attention to identity theft.

Identity theft continues to be a priority for the administration and federal agencies; however, their concerns have shifted somewhat toward emerging threats. The President’s proposed budget for fiscal year 2009 addressed the evolving problem of information security and the threat of cybercrime. Homeland Security Secretary Michael Chertoff acknowledged that improved cybersecurity was one of the top priorities for the Department of Homeland Security (DHS) in 2008. Consistent technology advancements make it increasingly difficult for the U.S. to defend against cybercrime. Additionally, sensitive information is readily available on federal agencies’ networks, such as the State Department’s server, and as that information becomes increasingly

58 “DOJ to Provide $1.7 Million to Aid Victims of Identity Theft, Financial Fraud.” Bureau of National Affairs Daily Report for Executives.
59 Ibid.
difficult to protect from evolving computer crimes, it creates a heightened national security risk for the United States. According to the budget request, funding for cybersecurity must improve to keep the country safe from terrorist or other cyber-attacks.\textsuperscript{62} Increased funding for the DHS U.S. Computer Emergency Readiness Team (US-CERT) was also included in the budget in an effort to help the division better monitor computer intrusions and provide strong network security.\textsuperscript{63} Overall, the threat of a cyber attack on the United States’ infrastructure could be exceptionally debilitating, and the possibility of such an attack should not be taken lightly. The administration’s concern in regard to such an attack and commitment to the deterrence of such an attack is evident in the increased proposed funding for cybersecurity initiatives. Cybersecurity will be addressed in greater detail in this thesis as it relates to the deficiencies in federal agency information security safeguards.

How well-educated are Consumers, Businesses, etc. in regard to Identity Theft Prevention and Reaction Methods?

Identity theft will not be going away any time soon as long as thieves have an incentive to steal sensitive personal information for fraud purposes. The public realizes the ongoing threat of identity theft, but few individuals know how to protect themselves from becoming a victim. A Zogby Interactive Poll found that “91% of respondents do not see an ‘end to the tunnel’ and expect a heavy increase in victimization. 49% also stated that they do not feel they know how to adequately protect themselves from this crime.”\textsuperscript{64}

\textsuperscript{62} President’s Proposed Fiscal Year 2009 Budget. P.71.
\textsuperscript{63} Ibid. p. 71.
Identity theft will remain a major problem because many people are uneducated on the ways in which it occurs, and many do not know the proper necessary steps if they believe their personal sensitive information has been compromised. According to the FTC, “Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter.”\textsuperscript{65} Surprisingly, very few people actually know that this precaution is necessary. Additionally, if someone is a victim of identity theft, “filing a police report, checking credit reports, notifying creditors, and disputing any unauthorized transactions” are some of the steps that must be taken immediately to restore the victim’s good name.\textsuperscript{66} Again, very few people recognize that these reactive measures are necessary in the event of suspected identity theft. In fact, only 26\% of victims surveyed even contacted the police; yet, that percentage increased to 44\% in incidences of new account creation.\textsuperscript{67} Ensuring that victims are properly refunded for any financial harm inflicted as a result of identity theft is another challenge in reacting to this problem. As mentioned, consumers are most likely to recover all financial losses if they follow the proper steps in filing an identity theft complaint and seeking a separate police report, but few individuals know both steps are necessary. Additionally, in order for victims to be entitled to full legal rights in the recuperation process, full details need to be included on the police report,\textsuperscript{68} which does not leave much room for error or uncertainty.

\textsuperscript{65} FTC website.
\textsuperscript{66} FTC Website.
\textsuperscript{68} FTC website.
Another tool consumers can use as a precaution against identity theft, if they believe their personal sensitive information has become compromised, is the placement of a fraud alert on their credit report. An individual who suspects they are a victim of identity theft can place either an initial 90-day fraud alert or an extended fraud alert on their credit report so that creditors know to be extra cautious when being approached to open new credit in their name.\(^6^9\) As with credit freeze, this method may not be entirely effective against the creation of new accounts, and will not affect the ability of an identity thief to access existing accounts. Additionally, fraud alerts may only be issued by victims of identity theft or individuals who suspect their identity may have been stolen so this is only available to a limited number of people; whereas, credit freeze is available to anyone in a number of states and through at least one of the big three credit agencies at a national level.\(^7^0\) Again, the problem with both fraud alert and credit freeze is that they are almost always reactive efforts, and they do very little to actually prevent and limit identity theft.

There are also a number of private companies who will monitor a consumer’s credit report for an annual fee. A few or the more well-know groups are Lifelock, TrustID and LoudSiren.\(^7^1\) While these fee-based programs may make sense for some consumers, they have annual fees of roughly $80 to $120 and may not be practical for all consumers. They are beneficial in that they take care of the credit monitoring responsibility that some individuals may forego, and beyond that, they offer insurance guaranteeing full recovery of losses including wages and time spent, which are not

\(^6^9\) Ibid.
\(^7^0\) Ibid.
\(^7^1\) “Identity Theft Protection Services Compared.” Identity Theft Labs. Online: http://www.identitytheftlabs.com/.
recoverable by any other means. Data security insurance is an emerging type of policy that companies like the American Insurance Group are beginning to offer to businesses who are worried about the unpredictable costs associated with a breach.\footnote{Brenner, Bill. “The pros and cons of data breach insurance.” \textit{Security Wire Daily News}. March 19, 2008. Online: \url{http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1306207,00.html}} While both data security insurance and commercial fee-based identity theft consumer tools have their benefits, they may not be economical for all businesses and consumers and both groups should be sure to weigh the costs and benefits of these tools and policies before subscribing to them. Just like credit freeze and fraud alerts, both data security insurance and these consumer tools are reactive in nature.

In addition to being poorly educated on both preventative and reactive measures to identity theft, consumers can often be too apathetic in regard to having their identity stolen. Consumers merely assume that they are not at risk and there is no way identity theft will happen to them. The FTC conveys that education and awareness are the main ways to deter against identity theft. “Armed with the knowledge of how to protect yourself and take action, you can make identity thieves’ jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community.”\footnote{FTC Website.} In an attempt to enhance consumer education efforts, FTC has prepared and made available on their website, information educating people on identity theft.\footnote{Ibid.} In general, identity theft is a relatively new problem at the scale it exists today. Fraud has existed for centuries, but only in recent years, has personal sensitive information become more readily available to thieves and more usable in efforts to access existing accounts and to create new ones. People are at risk of having their identities stolen because they...
are poorly educated on the ways in which their personal sensitive information can be stolen, and they also do not realize what types of data compromise often result in the most harmful forms of identity theft. For example, the media had overplayed a number of retail breaches in the past couple of years, but they fail to mention that identity theft resulting from these breaches is very unlikely. The TJX breach is a special case and will be addressed in the next chapter.

**What Policy Issues Exist in Regard to Identity Theft?**

A number of policy issues exist in regard to preventing and protecting against identity theft: data protection safeguards, breach notification standards, consumer rights & privacy, liability standards, fraud, safeguarding of social security numbers, credit freeze specifications, and national security issues.

Breach notification standards are a major point of contention. Consumer advocacy groups believe that any time a consumer is at remote risk for identity theft, they should be notified of such a situation – both account and identity level compromises are covered under this regardless of how the data is obtained. Others, including businesses, financial institutions, and the President’s Identity Theft Task Force have argued that consumers should only be notified if a data breach constitutes a “reasonable” risk of harm. For example, if account level information is compromised by accidental loss, there is not a high risk of harm associated with the breach. However, if thieves, with malicious, hack into a computer system and obtain records containing name, address, and social security numbers (an identity level breach), there is a high risk of harm associated with the breach, and almost all interest groups feel that this should be reported. According to the
Government Accountability Office, “requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft, but it also involves monetary costs and challenges such as determining an appropriate notification standard.”\textsuperscript{75} The main reasons for not notifying consumers in the event of any type of breach are cost and consumer desensitization. Breach notifications have the potential to be the next credit card junk mail – the piece of mail received two to three times a week, which is ripped up immediately upon receipt with no attention paid to its contents.

Consumer rights and privacy are closely tied to breach notification. Many consumer groups believe it’s the right of the consumer to know \textit{any} time their sensitive personal information has been comprised because their rights to privacy are endangered by a compromise of this data. Privacy rights are also a major component of some of the existing safeguards in place to protect against identity theft and the compromise of sensitive personal information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established strict privacy rights for individuals in regard to their medical records, which contain identity level information such as an individual’s date of birth and social security number. As such, pharmacies that fill medical prescriptions are already accountable for the safeguarding of patient information that is stored in their point-of-sale computers. HIPAA compliance was a timely and expensive undertaking and many would argue that privacy protections in place for individual consumers under HIPAA are already stringent enough.

\textsuperscript{75} Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown. P. 6.
Liability standards are another major policy issue being played out; although, this battle is being waged predominately at the state level. Retailers and financial institutions both argue that the other should be responsible for breach notification and the costs associated with notification and the re-issuance of credit and debit cards in the event of a breach. Retailers argue that card issuing banks have claimed that a component of the interchange fee, which is collected by the card issuing bank each time a cardholder uses their credit or debit card to make a purchase, is supposed to cover fraud that results from a data breach. Retailers claim that adding additional liability for a data breach would essentially constitute double-dipping by the banks. Another argument against the banks shirking the responsibility for costs associated with identity theft is that financial institutions are responsible for financial fraud, and they are not stringent enough when checking an identity when opening new accounts. On the other hand, banks argue that if retailers are responsible for a breach through lack of safeguards, they should cover all costs associated with the breach.

Safeguarding of social security numbers is another major policy concern, and there are a number of pending bills in the 110th Congress aimed at reducing the use of social security numbers as an account identifier. This poses a major challenge for universities who use social security numbers on college applications, and as student account identifiers. Social Security number reforms also affect financial institutions who store social security number data when opening new accounts; however, there are already major safeguards imposed on financial institution data due to Gramm-Leach-Bliley and

FACTA, which will be addressed later on in this thesis. Retailers are not as greatly affected by changes in social security number usage; yet, in the past, paper checks often contained an individual’s social security number or driver’s license number, and retailers may still possess such paper checks as a part of record-keeping requirements, and some pending legislation would cover those records.

An additional policy concern is the use of a credit freeze. The majority of states already have credit freeze laws in place, which many opponents of additional federal mandates use as a reason federal credit freeze legislation is unnecessary. FACTA created new consumer rights in regard to credit freeze, which included the right to a free credit report at least once every year, but credit freeze can only do so much to help protect consumers from identity theft. According to the FTC, “While a credit freeze can help keep an identity thief from opening most new accounts, it’s not a solution to all types of identity theft. It will not protect against an identity thief who uses existing credit cards or other accounts.”\textsuperscript{77} Other types of accounts, such as a mobile phone account, do not necessarily require identity level data, and are thus easily obtainable using less sensitive data. Also, “if there’s identity theft already going on when you place the credit freeze, the freeze itself won’t be able to stop it.”\textsuperscript{78} Credit freeze still makes it relatively difficult for thieves to open a majority of new accounts so it does have its merits. Credit freeze, while sometimes useful in preventing account misuse and continued theft, is almost always a reactive policy as opposed to a prevention method, and as such it not enough to deter against identity theft on its own.

\textsuperscript{77} FTC Website.
\textsuperscript{78} Ibid.
The final policy issue of concern is information security and how holes in the information security of a number of federal agencies pose a national security threat. The cybercrime incident that occurred in Estonia in May of 2007 is a prime example of how cyber criminals can infiltrate a nation’s infrastructure if the proper information security safeguards are not in place. In the Estonia incident, hackers infiltrated the Estonian government and financial institutions via the Internet.\textsuperscript{79} A similar attack would be incredibly debilitating in the United States, and such an attack is not unrealistic. In 2006, the Department of Homeland Security U.S. CERT tracked 477 incidents of information breaches at 59 federal agencies or at federal contractors with access to government-owned data.\textsuperscript{80}

What will the Rest of this Thesis Address? How Big of a Problem is Identity Theft Really?

The remainder of this thesis will attempt to determine how big of a problem identity theft really is and what are the best solutions to help curb identity theft and the harm that results from identity theft. This thesis will examine claims that identity theft results more often from public sector than private sector breaches, and will also take into account claims that incidences of data breach resulting in identity theft are actually very low. This thesis will also address government data security practices through an examination of a 2008 GAO study, which audited the information security standards of U.S. federal agencies. It will also examine private sector security measures which cover

\textsuperscript{79} Smith, Adam. “Estonia: Under Siege on the Web.”
\textsuperscript{80} Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown.” Government Accountability Office. p. 14.
multiple corporations, such as Payment Card Industry Data Security Standards, Sarbanes-
Oxley data security measures, and Health Insurance Portability and Accountability Act
safeguards on personal data.

This thesis will also examine the Identity Theft Assumption and Deterrence Act
of 1998 and whether or not it is a sufficient federal standard in light of evolving
technology standards. Additionally, this thesis will examine a data breach bill, which
became law in December of 2006, as a result of the theft of a laptop from a Department
of Veteran’s Affairs employee, which contained personal sensitive information on a
number of veterans. This thesis will also examine existing state laws and will seek to take
a position on whether or not data security and identity theft should be regulated at a state
or federal level.

This thesis will also examine the numerous pending data security bills in the 110th
Congress and the political feasibility of their movement and passage. This thesis will
highlight credit freeze, breach notification, liability standards, and protection of social
security numbers standards proposed in pending federal, as well as state bills. Lastly, this
thesis will address emerging technologies and necessary security standards for the future.
Chapter 3: Existing Safeguards on Personal Data
What Laws and Safeguards are already in place?

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which was later signed into law by the President. The law (PL 105-318) amended chapter 47 of title 18 of the U.S. Code relating to identity fraud making it a federal offense for an individual who “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 of local law.”\textsuperscript{81} It also established the FTC as the government lead on deterring and defending against identity theft. The law called for FTC to create information materials on identity theft, and made them the facilitator between victims and law enforcement officials, as well as charged them with informing the appropriate credit reporting agencies and law enforcement officials and agencies in the even of an identity theft.\textsuperscript{82} The Identity Theft and Assumption Deterrence Act laid the groundwork to increase deterrence efforts surrounding identity theft, but it is a ten year old law, and may not be suitable to deter against evolving identity theft crimes.

In 2004, Congress and the administration increased federal enforcement authority for identity theft crimes. President Bush signed the Identity Theft Penalty Enhancement Act, giving “law enforcement new tools to prosecute those who violated the financial privacy of American citizens . . . [creating] a new crime of ‘aggravated identity theft’ and added two years to prison sentences for criminals convicted of using stolen credit card numbers and other personal data to commit crimes.”\textsuperscript{83} While this law is a useful addition

\textsuperscript{81} FTC Website: \url{http://www.ftc.gov/os/statutes/itada/itadact.pdf}
\textsuperscript{82} Ibid.
\textsuperscript{83} “White House Fact Sheet: The President’s Identity Theft Task Force.”
to federal identity theft enforcement standards, it does nothing to prevent identity theft other than deter criminals through the promise of increased penalties for identity theft.

A number of state laws are currently in existence. Most of the state data security laws protect individual rights to a credit freeze and mandate a certain level of breach notification. Some require notification any time personal sensitive data is compromised, while some require notification only when there is a reasonable risk of harm. 84 This thesis will address pending state laws and recent activity at the state level in the next chapter.

What Existing Laws and Safeguards Apply to Financial Institutions?

The data security standards under which financial institutions are currently regulated are rather stringent. Financial institutions are regulated by the Fair and Accurate Credit Transactions Act (FACTA) and Gramm-Leach-Bliley. FACTA passed in 2003 and did the following to help ensure appropriate security standards were in place:

- required merchants to delete all but the last five digits of a credit card number on store receipts;
- created a national system of fraud detection so that consumers could issue a nationwide fraud alert with one phone call; and
- gave consumers the right to receive one free credit report per year from each of the nationwide credit reporting agencies. 85

85 “White House Fact Sheet: The President’s Identity Theft Task Force.”
FACTA not only enhanced security standards for financial institutions, it also created additional standards for retailers; thus, enhancing more than a single industry security standards.

The Gramm-Leach-Bliley Act (GLB), 15 USC, Subchapter I, Sec. 6801-6809 relates to the disclosure of nonpublic personal information. “Financial institutions’ use of social security numbers is regulated under the Gramm-Leach-Bliley Act, [which] prohibits financial institutions from disclosing customer SSN’s to third parties without consumer notice and consent, and requires institutions to implement physical, technical, and administrative safeguards to protect customer data.” Additionally, as part of GLB implementation, the FTC issued the Safeguards Rule, which required financial institutions to employ measures to secure customer data. “The Safeguards Rule applies to all businesses, regardless of size, that are ‘significantly engaged’ in providing financial products or services. These include, for example, check-cashing businesses, payday lenders, mortgage brokers, non-bank lenders, real estate appraisers, and professional tax preparers.” As such, Gramm-Leach-Bliley covers a number of businesses and financial institutions, effectively requiring strong security safeguards from those groups, which should now exist.

The only major breaches in the past two to three years resulting from financial institutions were cases of customer data being sold by bank employees, not necessarily any technological or procedural shortcomings. The ChoicePoint breach in 2005 was the case of a data broker providing a malicious third party that approached them under a false

---

86 FTC Website. [http://www.ftc.gov/privacy/glbact/glbsub1.htm](http://www.ftc.gov/privacy/glbact/glbsub1.htm)
87 FTC Website. [http://www.ftc.gov/privacy/privacyinitiatives/safeguards_lr.html](http://www.ftc.gov/privacy/privacyinitiatives/safeguards_lr.html)
pretense with information. Data brokers, however, are not regulated by the same laws as financial institutions that provide the aforementioned financial services. Given the existing laws, which regulate financial institutions and other money services businesses, coupled with the lack of a known major financial institution breach, financial institutions outwardly appear to have strict enough data security safeguards in place. Additionally, these regulations are enforced by a number of federal institutions so most covered entities are in compliance with the existing laws. Many argue that other industries, such as retailers, data brokers, and government agencies should be held to the same federal data security standards financial institutions must comply with since those standards are considered to be some of the most stringent in existence.89 One could also argue that if the aforementioned industries have more lax security standards than financial institutions, thieves will target those groups due to their vulnerable infrastructures. In other words, imposing strict standards on just one industry may do more harm than good because it will give thieves incentives to target other industries; if strict regulations exist, they should be across the board.

What Existing Laws and Safeguards Apply to Retailers and Other Private Sector Businesses?

One other group already regulated by strict security mandates are retailers. Recently, the five card associations, created security standards with which merchants must comply in order to continue accepting payment cards. In addition to having their card acceptance contracts at risk, merchants can also be hit with up to a $500,000 fine by the participating card associations if they fail to comply with these new standards know

as the Payment Card Industry Data Security Standards (PCI DSS). “The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.”90 The goal of the PCI Security Standards Council is to “enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.”91 PCI data security standards were very difficult for retailers, both large and small, to comply with. New standards were also very costly, but as along as the PCI Council sticks to its mission by modifying security requirements as needed to keep up with emerging technologies, PCI DSS has the potential to be very effective.

PCI DSS “requires merchants, their banks, and credit card transaction processors to build and maintain a secure computer network, maintain a vulnerability management program, and regularly monitor and test networks. The standard includes requirements for restricting access to data, encrypting sensitive data transmitted over public networks, using firewalls and current virus software, and other data security measures.” 92 The PCI DSS framework includes twelve main requirements, which mandate that card accepting entities:

90 PCI Council. Online: https://www.pcisecuritystandards.org/
91 PCI Data Security Standards. Online: https://www.pcisecuritystandards.org/tech/index.htm
92 Ibid.
1. “Install and maintain a firewall configuration to protect cardholder data;

2. Do not use vendor-supplied defaults for system passwords and other security parameters;

3. Protect stored cardholder data;

4. Encrypt transmission of cardholder data across open, public networks;

5. Use and regularly update anti-virus software or programs;

6. Develop and maintain secure systems and applications;

7. Restrict access to cardholder data by business need-to-know;

8. Assign a unique ID to each person with computer access;

9. Restrict physical access to cardholder data;

10. Track and monitor all access to network resources and cardholder data;

11. Regularly test security systems and processes; [and]

12. Maintain a policy that addresses information security for employees and contractors.”

Overall, PCI DSS standards are relatively strict and if retailers are properly employing these card association mandates, the risk of data breach should be relatively low. Additionally, all retailers should be compliant with PCI standards by now, but a few are still trying to meet the requirements.

PCI standards have the potential to be very effective once retailers have enough time and money to comply with them because the card associations hold retail groups accountable for meeting the required standards. The five card associations require

merchants to create and submit a “Report on Compliance” in order to ensure that each payment card company acknowledges the entity’s compliance status.94 Additionally, the card companies are creating financial incentives for retailers to meet compliance standards; last year Visa says it “levied $4.6 million in PCI-related fines, [and] this year, it announced a $20 million fund to reward companies which met PCI requirements.”95 Companies that are not PCI-compliant face fines of up to $500,000 and may not have access to Visa’s best interchange rates, which could greatly affect certain retail sector profits because of the large discrepancies in rates.96 As of August 31, 2007, only 44% of Tier 1 merchants and 38% of Tier 2 merchants were PCI DSS compliant.97 Additionally, a White Paper authored by VeriSign Global Security Consulting Services, who conducts onsite audit and scanning services under the PCI program, found that only 25% of merchants passed the assessment on their first attempt.98 While actual PCI-compliance is lagging slightly, the fact that PCI audits by the card companies hold retailers accountable for meeting the PCI requirements, and that the card companies offer financial incentives for becoming PCI-compliant, help validate the effectiveness of the PCI program.

In the largest retail breach to date, TJX Inc. was not PCI compliant. However, in a very recent breach reported by Hannaford Bros., they were PCI compliant, but thieves were still able to hack into data while it was in transit during the authorization process.

“It is not known whether hackers got the data as it was leaving the stores or when it came

96 Ibid.
97 Ibid.
back with the approval or decline message. The hacked data was stored briefly within the malware on Hannaford servers, and then transmitted to an offshore Internet service provider in batches. The intricacies of the Hannaford breach are still being explored given the complex and novel technologies utilized in the breach, but Carol Eleazer, vice president of marketing, has publicly affirmed “all indications was that it was a novel and quite sophisticated attack.” This demonstrates that PCI DDS may need to evolve at a greater speed in order to keep up with the emerging technologies hackers are able to utilize.

Another problem with PCI DSS is whether or not the PCI Council will change security standards if it’s not in their financial best interest. Card transaction processors do not currently accept encrypted credit card or signature debit data, just encrypted PIN debit card data. As such, data in transit, such as the data that was stolen in the Hannaford breach, is usable by thieves if extracted using malware programs or other technologies. Processors could upgrade their technology to accept PIN protected credit card data, but it would be very costly for them to do so, and even in the wake of the recent Hannaford breach, the PCI Council has not shown any sign of making a technology upgrade of this nature. It is also not the PCI Council’s (the credit card companies) or the card processor’s image that is hurt by a breach, it is the retailer’s reputation which suffers the consequences and the PCI Council executive committee consists only of representatives of the five major credit card companies – American Express, Discover Financial

---

Services, JCB International, MasterCard Worldwide, and Visa Inc.\(^{101}\) PCI is not a perfect solution in part because the Council consists of a limited number of groups who it is assumed will act rationally to support their own best interest. PCI DSS, is however, more expedient than continually attempting to pass federal legislation, which affords the opportunity for the standard to remain up to speed with emerging technologies, and PCI standards are very stringent so it is highly unlikely that a breach will occur at a PCI compliant merchant unless the breach utilizes the most cutting edge technology.

Another major data safeguarding standard that retailers (at least those containing pharmacies) must comply with is the Health Insurance Portability and Accountability Act (HIPAA), which limits the disclosure of patient SSNs without authorization.\(^{102}\) According to comments filed with the Department of Health and Human Services by the Food Marketing Institute, a trade group representing supermarket retail pharmacies, a covered entity must “establish the permitted and required uses and disclosures of protected health information” and further require their employees not disclose patient information, use appropriate safeguards to prevent unauthorized use or disclosure of the data, report any unauthorized use or disclosure of customer data, and destroy all records after record-keeping requirements expire.\(^{103}\) Patient records necessary for pharmacies to fill prescriptions contain more sensitive information than almost any other record stored by retailers, and since HIPAA employs strict mandatory compliance standards in regard

\(^{101}\) PCI Council Website. Online: [https://www.pcisecuritystandards.org/pdfs/executive_committee.pdf](https://www.pcisecuritystandards.org/pdfs/executive_committee.pdf)


\(^{103}\) Ibid.
to the safeguarding of that data, this is just another front on which retailers are already held to strict security standards.

Private corporations are also regulated by the internal control management and data security standards in Sarbanes-Oxley (SOX). According to a study by Hightower, two sections in SOX are particularly relevant to information security: Section 404, Management Assessment of Internal Controls, and Section 409, Real Time Disclosure.\textsuperscript{104} Section 404 requires corporations to assemble an annual internal control report containing an account of the effectiveness of the internal control structure.\textsuperscript{105} Section 409 calls for real time reporting, which is critical to information security practices. “Weak authentication methods could, for example, result in security-related breaches in which unauthorized access to critical servers that hold financial accounting or accounts payable data could be obtained. The result could be destruction or unauthorized modification of such data, something that would very much affect an organization’s financial condition.”\textsuperscript{106} Real time reporting requirements in Section 409 are important because a company can quickly identify and react to security breaches, which helps minimize financial loss and cuts off the breach before more damage can be done.\textsuperscript{107} Sarbanes-Oxley standards are related more closely to internal controls, but the reporting requirement creates one more level of public disclosure, and real time reporting helps companies detect breaches in their early stages often making them less harmful. If a breach goes undetected, the perpetrator might gain dangerous access privileges to the

\textsuperscript{105} Ibid.
\textsuperscript{106} Ibid.
\textsuperscript{107} Ibid.
company database for a lengthy amount of time; thus, increasing the risk of financial loss.\textsuperscript{108} “Without an effective intrusion detection capability, SOX compliance with SOX real time reporting requirements is impossible,”\textsuperscript{109} and breaches could go undetected for days, even months, potentially resulting in excessive corporate loss. Additionally, SAS 70 audits, established by SOX, require that companies verify the accuracy of their financial statements, which can be a useful tool in auditing third-party vendors to be sure they meet the security standards necessary to contract with that business.\textsuperscript{110} SAS 70 audit requirements are a loose set of goals and principles that vary organization to organization, but whether or not a third-party meets these outlined standards can provide some feedback on outsourced vendor security controls.\textsuperscript{111} While the control objectives outlined in SAS 70 audits are not nearly as important as the real-time reporting requirements, they are an additional tool in an arsenal of weapons to help corporations prevent against identity theft.

Given the constraints placed on retailers by PCI DSS, HIPAA, and SOX, data breaches should be fairly limited and not particularly harmful if retailers are in compliance with the existing data security standards in the private sector. Additionally, retailers usually collect and transfer account level data so the risk of a very harmful incident of identity theft resulting from a retailer breach is relatively low. However, if the security standards outlined in these laws and industry guidelines are not sufficient

\textsuperscript{108} Ibid.
\textsuperscript{109} Ibid.
\textsuperscript{110} Fitzgerald, Michael. “SAS 70.” \textit{CXO Media Inc.}, November 1, 2005. Online: \url{http://www.CSOonline.com}.
\textsuperscript{111} Ibid.
enough to combat emerging computer technology being employed by identity theft criminals, these standards will need to be revised or replaced by other mandates.

As previously mentioned (p.49), Hannaford Bros. fell prey to a data breach in February 2008 even though they were PCI compliant. The PCI standards require encryption of data that is being transmitted as part of the card authorization process, so how are criminals stealing data in transit? “Fraudsters increasingly are targeting data in transit . . . by enlisting employees or . . . partial insiders to help them steal and decode it. This group includes technology vendors, outside maintenance personnel, and others who have credentials and know passwords that can get them inside a company’s computer systems, or have so-called keys that can decrypt encrypted data.”112 The Hannaford case demonstrates that outside parties, such as hackers from other countries, may also be gaining access to these payment systems through the remote importation of malware onto computer servers. Overall, the theft of in transit data is very rare, but it has the potential to be the next major type of identity theft crime. Another form of relatively novel theft is skimming. A prime example of how easily skimming can occur even when a company is PCI compliant, and employs other strict security safeguards is the Stop & Shop Company breach incident where sophisticated thieves “switch[ed] out PIN pads with rigged devices that pick up PINs and account numbers” when cards are swiped at point-of-sale terminals.113 PIN debit has always been one of the most secure forms of payments; however, thieves are increasingly targeting PIN debit in point-of-scale schemes such as this, and PIN debit fraud losses are rising at an alarming rate with an increase from $8

112 Ibid.
million dollars in losses in 2004 to $21 million in losses in 2005.114 Again, it is important to note that the Stop & Shop breach was also an isolated case of thieves using a novel criminal technique to steal point-of-sale payment card data.

So where have retailers gone very wrong? What about data breach incidences has really fostered a negative image surrounding retail's ability to safely handle sensitive account data? Most of the negative backlash against retailers has been a result of the TJX breach, which broke in early 2007, and in which case it is believed that TJX failed to meet 9 out of the 12 PCI data security standards. In regard to the TJX breach, banks have alleged that the company “failed to follow credit card industry data security standards and knew its computer network was vulnerable prior to discovering a breach of millions of card accounts, banks suing the retailer alleged.”115 Additionally, the banks claim that “the TJX breach included the release of so-called ‘Track 2 data’ . . . [which] includes the payment card account number and verification code and may also include the customer’s personal identification number.”116 Breach of Track 2 data is a huge anomaly because “in the early 1990s, long before the implementation of PCI DSS, retailers and their merchant banks had been prohibited by agreements with the separate card companies from retaining such Track 2 data . . . even if the data was encrypted.”117 While a breach of Track 2 data, such as the one that occurred in the TJX breach, poses a high risk of harm, is it very rare that Track 2 data is breached because it shouldn’t be stored in the first place. At the same time, it appears that real time theft may be a new hacker tool,

114 Ibid.
116 Ibid.
117 Ibid.
which means that Track 2 data is vulnerable even if it’s never stored; it’s believed that Track 2 data was compromised in the Hannaford breach.118

As a result of the TJX Companies’ failure to comply with existing security standards, “payment card-issuing banks filed complaints seeking reimbursement for their costs associated with the breach, including the cost of replacing cards affected by the breach and covering fraudulent purchases.”119 Breach liability is an ongoing battle between retailers and financial institutions in regard to fraud and re-issuing costs. A precedent favoring retailers in the breach liability battle was set in 2006 when lawsuits filed by card issuing banks seeking to recover costs they incurred as a result of the 2005 incident where BJ’s Wholesale Club allegedly mishandled consumer’s credit information were dismissed by a Pennsylvania federal court.120 At the same time, TJX just agreed to settle with MasterCard over a pending lawsuit and will provide up to $24 million to settle loss claims in connection with the data breach.121 Millions of merchants accept credit and debit cards and store and transmit electronic data, which creates many challenges in getting cross-industry compliance with existing data security standards; however, as merchants begin to pass PCI audits demonstrating that they meet private sector data security standards, businesses should be better able to protect against data security threats. Granted that undetected or undisclosed data breaches may exist in the private sector, it appears that the private sector is taking the necessary steps to ensure the safety of consumer data.

What Existing Laws or Safeguards Exist for Education Institutions?

Breaches of higher education records are one of the most prevalent incidences of data breach. In testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Joanne McNabb, Chief of the California Office of Privacy Protection, noted that from an approximately 500 breach notification sample, universities and government agencies account for the majority of notifications at 28% and 25%, respectively, with 14% of financial services companies reporting breach incidents, medical facilities 11%, retailers 5%, schools 3%, and manufacturers, data brokers and other businesses accounting for the other 15%. In 2006 the University of California Los Angeles experienced a data breach which put students, parents, faculty and staff at risk of identity fraud after an unknown attacker breached a university-administered database containing personal information on approximately 800,000 people. Breached data included names, Social Security numbers, dates of birth, home addresses and contact information, but not banking and credit-card information nor driver's license numbers. In a statement announcing the breach, UCLA’s Chief Information Officer, Jim Davis said “In spite of our diligence, a sophisticated hacker found and exploited a subtle vulnerability in one of hundreds of applications,” effectively implying that the Internet is an open arena for hackers making networks difficult to defend. Additionally, in written testimony submitted to the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Davis noted that hackers were able to exploit the universities’

network even though “UCLA’s systems were in full compliance with University of California (UC) and campus policy governing security standards and practices.” Given the nature of data collected and maintained by universities, it is critical that additional safeguards and encryption standards abound in the higher education sector. Similar to the sensitive information in the U.S. federal agency networks, universities maintain identity level information, which creates a much greater risk of harmful identity theft fraud than risk resulting from account level data, the type predominately stored by retailers.

**What Existing Laws or Safeguards Exist for the Federal Government?**

Information security by federal agencies is arguably more important than in other sectors given the sensitive nature of agency data. In 2002, Congress passed the E-Government Act (PL 107-347), which was later signed into law by President Bush, and which demonstrated the government’s commitment to the protection of U.S economic and national security interests through sound information security requirements. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) “requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.” Under FISMA, “an effective information security program should include: periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, 

---


127 Ibid.
or destruction of information and information systems that support the operations and assets of the organization.”128 It should also contain “policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system, [and it should have] . . . security awareness training to inform personnel of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.”129 FISMA puts strict guidelines in place for federal agencies, but more importantly, it requires periodic evaluation of the effectiveness of information security polices, which should encourage agencies to comply with the existing standards.130 Even though FISMA compliance is reviewed often, a strict enforcement mechanism does not exist to help motivate federal agencies to comply with these information security standards, which is evident in the lackluster performance of the agencies in the recent GAO report audit.

Additionally, even though FISMA standards appear strict on the surface, the government supports cost-effective, risk-based policies in regard to the protection of sensitive agency information, which implies that they could be employing additional information security tactics, but choose not to because it’s not in their financial best interest. Congress and the Administrations could threaten to withhold funding for agencies who do not meet FISMA standards, but that would be a pretty open threat given that it’s not really politically feasible to withhold funding from major government

128 Ibid.
129 Ibid.
130 Ibid.
agencies. The ultimate objective of FISMA is to “conduct the day-to-day operations of the agency and to accomplish the agency’s stated missions with adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.” Given that FISMA standards only seek to enforce “adequate security,” there seems to be room for improvement, but agencies also employ risked-based security tactics, which means classified materials would travel only over the most secure channels. This should effectively lessen national security risks associated with deficient information security standards at federal agencies, but it doesn’t really reduce the risk that unclassified data, such as individual records, could be compromised.

A February 2008 GAO study found that federal agencies still had a way to go in their FISMA compliance efforts. “19 of 24 major federal agencies had not fully implemented agency-wide information security programs as required by FISMA. As a result, 13,029 incidents involving data loss or theft, computer intrusions, and privacy breaches were reported by federal agencies to the U.S. Computer Emergency Readiness Team in fiscal year 2007.” Not only were reported incidents high, they also showed a dramatic increase from reported incidents in 2005 almost quadrupling, which demonstrates that federal security standards are, if anything, worsening, or else emerging technologies are becoming more difficult to detect and deter. The GAO report also found that many of the government's computer systems are at “undue and unnecessary risk”

---

131 Ibid.
simply because established programs have not effectively been fully implemented. In order to better protect against emerging threats, the U.S. government must first implement basic security measures.

The GAO report found that in 2007 out of 24 federal agencies, inadequate information security controls were a significant deficiency for 11 agencies, a material weakness for nine agencies and not a significant weakness for only four agencies. Major weakness found were”

“access controls, which ensure that only authorized individuals can read, alter, or delete data; configuration management controls, which provide assurance that only authorized software programs are implemented; segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and an agency-wide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.”

While the GAO found that lax information security standards are an ongoing problem, there may not be a quick end in sight. As more federal agencies increase their reliance on the Internet and their internal networks for day-to-day operations, they remain vulnerable to outside attacks. “The National Vulnerability Database found more than 13,000 products with security vulnerabilities and 29,000 security vulnerabilities or software defects that a hacker could use to infiltrate a government network,” with an

---

135 Ibid. p. 13
average of roughly 17 new vulnerabilities being added on a daily basis. Additionally, “the Federal Bureau of Investigation identified a variety of sources posing cyber threats to the nation, including criminal groups, foreign nation states, hackers, hacktivists (who hack Web sites and e-mail servers to send a political message), disgruntled insiders, terrorists and virus writers.” This thesis will address these criminal groups in greater detail in chapter five. This should serve as a strong alert to the U.S. intelligence community, which will hopefully make tightening information security standards one of their top priorities in 2008 and the future.

A handful of people have testified before Congress that information security is a major concern and if not taken seriously, could prove to be a major national security risk for the U.S. In a February 5, 2008 hearing before the Senate Select Committee on Intelligence, Director of National Intelligence Mike McConnell said, U.S. information infrastructure “increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious.” GAO director of information security issues, Gregory Wilshusen echoed sentiments of the need for much tighter information security controls by the government in February 6, 2008 testimony before the House Oversight and Government Reform Subcommittee on Government Management. In his testimony, Wilshusen said “federal agencies had greatly strengthened their security protocols, but most were not in full compliance with the Federal Information Security Management Act of 2002 . . . the

---

137 Ibid.
138 Ibid.
need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology,"139 According to Wilshusen, “five years after FISMA was enacted, we continue to report that poor information security is a widespread problem with potentially devastating consequences.”140 It is apparent that even though identity theft and information security have been identified as high-risk crimes, the government, in many cases, has not taken the proper steps to avoid a security breach. Additionally, “personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes,”141 Not only are insufficient government information security standards exposing the U.S. to national security risks, they are also putting individuals at risk for identity theft.

While it is apparent that federal agencies are still in need of some major progress in their information security controls, it appears as though U.S. CERT is doing a decent job of deterring attacks behind the scenes, and the President has proposed additional funding for their efforts. “US-CERT responds 24 hours a day and reports national-level incidents to the National Cyber Response and Coordination Group (NCRCG), the cyber-incident response coordinator. NCRCG guides federal agencies and works with private

140 Ibid.
141 Ibid. P. 17.
sector, states, and other nations to defend U.S. cyberspace.”\textsuperscript{142} In response to a recent thwarted attack on 13 root-server computers that direct Internet traffic, deputy director of U.S. CERT, Mike Witt said it was “‘just another day of firefighting.’”\textsuperscript{143} The target servers in the attack included those that handle traffic for the Department of Defense, but none were ever reached according to U.S. CERT. While a number of networks remain vulnerable to hackers, there are at least some groups who are consistently providing efforts to thwart such attacks.

There has been some government progress in the effort to deter and protect against identity theft and attacks on information security, but the threat of both will continue to be a major issue as a result of deficient government safeguards coupled with emerging technologies. Perhaps the federal government does not have the same financial incentive that private corporations do to keep their name from being associated with a breach. Competition and consumer confidence alone, not taking into account direct financial loss, is enough to influence private business to enhance security controls, but the federal government isn’t constrained by anything other than public opinion, which matters less for federal agencies who are part of a four-year administration term. Additionally, private sector businesses succeed and fail based on their ability to turn a net profit so they will often go above and beyond regulatory mandates to ensure their customers are satisfied and remain loyal; whereas, that is not the case for the government whose citizens are automatically part of the government by electing to live in a society and conform to those society’s norms. Case in point in regard to profit, the current budget deficit is abysmal, and in any private sector business accountable to its customers,

\textsuperscript{143} Ibid.
shareholders, Board of Directors, and the remaining public, any CEO allowing for such a large net loss would be fired, but governments can get away with being much less efficient because they are less accountable to the public in most instances. The budget deficit is a large reason it is also not feasible for Congress to appropriate additional funds to the FTC to fight data security and emerging threats. With recent Democrat control of both the House and Senate, legislators have needed to find a “pay-for” for any increased funding initiatives so it’s not likely that an already stretched thin economy will be able to allocate more resources toward fighting data security threats. None of this means that the problems of identity theft and information security will necessarily be going away for federal agencies any time soon. According to the Information Technology Association, “information technology security and privacy protection topped the agenda of federal chief information officers in 2006 and will continue to be their number one concern for the foreseeable future.”

There does not appear to be a quick fix to enhance information security standards, but the federal government should do their best to ensure that at least the most commonplace security practices are being utilized and enforced. In 2007, the DHS Office of Inspector General found that most DHS laptops were still unencrypted. Five years after FISMA, it seems that basic security standards should be in place, namely password protections and laptop encryption, especially given the high number of laptop loss or theft incidences, and particularly in the aftermath of the Department of Veteran’s Affairs breach, which resulted in the passage of a federal law.

What Precedents did the Veteran’s Affairs Breach Bill Set?

In May 2006, a Department of Veteran’s Affairs employee had a laptop they had taken home without prior authorization stolen and 26.5 million active and retired military personnel records were compromised in the breach. This spurred legislative action from Chairman of the Veterans Affairs Committee, Rep. Steven Buyer (R-IN), and Rep. Tom Davis (R-VA), Chairman of the Government Reform Committee. The Department of Veterans Affairs Information Security Enhancement Act of 2006 moved as an amendment to a Veterans Affairs omnibus bill (S. 3421), and it passed quickly through both the House and the Senate. The VA breach bill is important in the review of existing data security laws since it was the first federal mandate regarding a breach notification standard. “The data security provisions of S. 3421 would require that the VA 1) notify law enforcement and other government officials outside the department and relevant congressional committees in the event of a data breach; 2) implement agency-wide information security procedures, including limiting employee access to sensitive information; and 3) provide yearly information security training to VA employees.

Even though entities covered by the law are limited, passage of the breach bill was significant because it set precedents for the definition of access to information, a risk trigger, and the definition of sensitive personal information. “In the event that unauthorized access to an individual's sensitive personal information--in either electronic or paper form--is detected and a risk analysis reveals that there is "a reasonable risk" for potential misuse of the information, the VA would be required to notify those affected

147 Ibid.
148 Ibid.
and provide free credit monitoring services.”\textsuperscript{149} Additionally, “sensitive personal information, the breach of which would trigger the notification requirements, is defined in the bill as: (A) education, financial transactions, medical history, and criminal or employment history; (B) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records.”\textsuperscript{150} Overall, the VA breach bill addressed a couple of the policy issues prevalent to identity theft, but as it was not comprehensive in its scope of issues or coverage, many people feel there is still a need for more comprehensive federal data security legislation. While some of the policies (i.e. the breach notification standard) in the VA breach bill would be workable across other industries, the provision in regard to stricter information security mandates is highly unnecessary for retail and financial institutions, which arguably have stricter laws and standards already in place. The VA breach bill information security standards would be an unnecessary mandate on the aforementioned private sector groups.

While there are a number of groups who feel that some portion of data security standards should be stricter at the federal level, there are a number of people who believe that the current federal regulations are sufficient and oppose a comprehensive federal legislative solution. In the next chapter, this thesis will address different schools of though in regard to whether or not components of data security need stricter regulation at a federal and/or state level. Additionally, the next chapter will include a synopsis of pending federal and state bills that relate to identity theft and cybercrime.

\textsuperscript{149} Ibid.
\textsuperscript{150} Ibid.
Chapter 4: Should Data Security Be More Highly Regulated? If So, What Additional Regulations Should Be Employed?
Which Groups Think Status Quo Data Security Standards Are Sufficient?

While there is a clear need for increased data security standards in some organizations, some groups argue that existing federal standards are sufficient. Many proponents of this school of thought recognize the inefficiencies that exist in the public sector, and argue that only private sector safeguards are substantial. Most businesses and financial institutions are of the mindset that strong enough private sector safeguards on consumer sensitive personal information already exist. Business security standards are already highly regulated by existing laws and procedures, such as HIPAA, SOX and PCI DSS, and as long as businesses continue to be held accountable for compliance with these laws, there is little need for additional private sector regulation at either a federal or state level. Additionally, a number of state laws currently exist in regard to breach notification standards and credit freeze leaving little need, these groups argue, for increased federal mandates. Additionally, a fair number of state bills have been introduced in 2008 in regard to breach liability, and those bills are currently playing out in those state legislatures.

According to the Coalition for Data Security, a group of retail associations and financial institutions, major distinctions between the public and private sector need to be taken into account. They claim “government and universities were responsible for close to 60 percent of all security breaches in 2006,” in their argument that any additional federal mandates should at least cover both sectors since the private sector does a better job of protecting consumer data than the public sector. The group also asserts that the

---

likelihood of harm associated with data security breaches is relatively small, “thirty percent of all U.S. consumers were involved in a data breach last year, but fewer than 1/10th of 1 percent (0.09 percent) became actual victims of identity fraud.”\textsuperscript{152} As such, they argue that identity theft does not affect a large number of people whose data is compromised as a result of a data breach so there is not necessarily a need for stricter federal data security regulations. Overall, financial institutions and retail groups argue that the threat posed by common, everyday data breaches is not very high. They acknowledge the danger associated with high risk level breaches, but feel that because incidences of intentional identity theft are relatively low, the existing state laws provide substantial consumer protections.

**Which Groups Think That Some Data Security Standards Should Be Reformed or Enhanced?**

While retail groups (many of which are members of the Coalition for Data Security) believe that existing data security standards are stringent enough, they feel that security standards could be more uniform. In a letter to Rep. Bart Gordon (D-TN), Chair of the House Science and Technology Committee during the 110\textsuperscript{th} Congress, the Food Marketing Institute, an association representing the retail and wholesale supermarket industry, reports the following recommendations obtained from a survey of supermarket industry professionals:

- “The primary goal of standards, guidelines and best practices from the perspective of our membership needs to be maintaining consumer trust.

\textsuperscript{152} Coalition for Data Security Website and “National Data Breach Analysis.” \textit{ID Analytics}.
• There was strong consensus that a universal set of security standards is needed. Currently, we are required to comply with a series of different industry standards and government regulations that focus on protecting a specific class of information – HIPPA (medical records), SOX, PCI (credit card data).

• Existing standards need to be integrated to protect information across the board with a single source by which to measure compliance and maintenance, particularly in light of rapidly changing technology.

• Several supermarket retailers saw the need to increase security directly on payment cards or other access devices themselves (PIN on credit, etc.) and saw a potential role for NIST in reviewing the need for a revision to product constructs to address security directly on the access device.

• Understandably, merchants also felt it was important to address security, standards and compliance with all stakeholders and hold all parties accountable, not just those in the merchant community.153

Overall, retail groups are not in favor of stricter federal mandates, but would support more uniform data security standards because it would ease compliance efforts and reduce confusion, especially since different states currently employ different standards on a number of fronts. Other groups, such as the Business Software Alliance, agree that there should be a national information security standard and that it should provide the appropriate enforcement authority for the U.S. Attorney General.154 Even if a national information security standard is created, emerging technologies will make the battle against identity theft a difficult one.

The President’s Identity theft Task Force, established by a 2006 Executive Order, found that while certain existing security safeguards are sufficient, more needs to be done on a number of fronts to increase data and information security standards. In its strategic plan, the task force concluded that “industry has made some strides in protecting sensitive

consumer data from identity thieves, but more could be done.”\textsuperscript{155} The Task Force also cited an April 2006 survey by the Ponemon Institute, which showed only 45 percent of large multinational corporations headquartered in the United States had a formal process for handling security violations and data breaches.\textsuperscript{156}

The Task Forces’ strategic plan also included recommendations to establish a national standard for the private sector safeguarding of personal information, it called for a reduction in the unnecessary use of Social Security numbers by federal agencies, and it recommended an update to criminal statutes addressing identity theft.\textsuperscript{157} The Task Force also suggested that a reasonable risk breach notification trigger was the most appropriate standard to avoid costly, unnecessary notification and consumer desensitization as a result of over-notification.\textsuperscript{158} The same standard is supported by groups who believe existing data security standards are stringent enough, including those in regard to breach notification.

One major point of contention in pending federal legislation in the 110\textsuperscript{th} Congress is whether or not any federal regulations should pre-empt existing state laws. The retail and financial services industries have argued that state laws create a sufficient security standard, and also point out pre-emptive federal regulations may actually lessen security in some states. The President's Task Force recommended preemption of state laws “to ensure comprehensive national requirements that provide clarity and predictability.”\textsuperscript{159}

\textsuperscript{156} Ibid.
\textsuperscript{158} Ibid. p. 2.
\textsuperscript{159} Ibid. pgs. 4, 34.
Even if numerous data security precautions are taken, networks may not be secure enough to prevent computer-related identity theft. As such, the Task Force also called for legislation “to provide new penalties for malicious spyware, as well as ‘cyber-extortion’ cases involving individuals who steal confidential information from a company and threaten to make the data public if certain conditions are not met.” ¹⁶⁰

With emerging technologies, hackers, such as those involved in the recent Hannaford breach, will continue to discover new ways to extract account information in transit. Also, business and government face the additional challenge of protecting against compromised information on portable data devices, such as laptops, hard drives, USB drives, and PDA’s. There are limited means for ensuring that employees don’t take unauthorized items off their organization’s premises. Organizations are adopting encryption methods to help deal with the threats posed by lost or stolen mobile devices, and according to the Ponemon Institute, 66 percent of organizations have some type of encryption strategy, which isn’t terrible, but also means that most groups still have room to grow in their standards for securing this part of their business. ¹⁶¹

Overall, identity theft will continue to be a problem regardless of increased federal oversight; however, perhaps the only way to help cut down on incidences of theft will be to better educate the public about how identity theft occurs and educate the public on reactive measures, as well. Some feel that additional laws are not necessary because breaches will happen regardless of the laws in place so it is necessary to take preventative

measures to protect sensitive data and it is important to have a user-friendly system in
place to help victims of identity theft.

The FTC has a very comprehensive, educational website geared toward both
consumers and business. However, visiting the website requires individuals to either be
proactive or reactive; either they are deciding to self-educate themselves on the dangers
of identity theft or the procedure they should follow if they anticipate a breach of their
own identity. A more passive means of education might garner a more widespread
audience. Also, the Privacy Rights Clearinghouse keeps a running list of breaches at:
http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP. Consumer education tools
exist, but they need to be more widely publicized in order for the public to become fully
educated on the perils of identity theft.

**Which Groups Think Data Security Needs Increased Regulation?**

In their campaign to help protect consumers from the evolving threat of identity
theft, consumer groups are the main proponents of increased data security regulation.
Jeannine Kenney, senior policy analyst for Consumers Union said “that more restrictive
regulation is necessary to protect consumers from unlimited use of consumer SSNs by the
private sector, which could put consumers at increased risk for identity theft.”\(^{162}\) She also
asserts that “businesses currently have no incentive to decrease reliance on SSNs because
their liability risks are low or nonexistent under current standards.”\(^{163}\) Consumer groups
recommend the following best practices for businesses and financial institutions in regard

\(^{162}\) Bivens, Amy. “Data Security Officials Warn Businesses Against SSN Use for Identity Authentication.”

\(^{163}\) Ibid.
to the secure handling and use of social security numbers: asking individuals for “wallet” information, logging telephone numbers used to call and checking against the number in the customers record, sending changes or applications to previous customer addresses, enhanced training of employees, and discontinued use of last four digits of a social security number as an account identifier.\textsuperscript{164} Consumer groups strongly support a number of the existing social security number reform bills pending in the 110\textsuperscript{th} Congress, but are most supportive of comprehensive reforms. The U.S. Public Interest Research Group (U.S. PIRG) has also expressed their sentiment in support of increased data security mandates. According to U.S. PIRG, “in an increasingly high-tech marketplace, we trust businesses with more of our personal information than ever before. Yet many companies aren’t as careful as we think—concealing security breaches or questionable sales of information that make consumers vulnerable to identity theft.”\textsuperscript{165} Overall, consumer advocates strongly believe that it’s the consumers right to know any time their data has been compromised in any type of breach. They also believe that social security number protection standards must be much tighter, and credit freeze should be made available to all consumers. For obvious reasons, they have stayed on the sidelines during the debate over breach liability since their interests are unaffected by this as along as either retailers or financial institutions take responsibility for breaches reimbursing consumers for their financial loss.

\textsuperscript{164} Ibid.
\textsuperscript{165} Ibid.

A number of policy issues are in play in the current 110th Congress. Legislators are looking to address breach notification standards, credit freeze, the handling of social security numbers, and cybersecurity. No breach liability bill, similar to what has arisen in a handful of states, is in play in the U.S. Congress to date. Currently, there have been minimal signs that data breach legislation of any sort might move this Congress. During the final week of March 2008, a story broke detailing a State Department breach of passport files of the three Presidential candidates, Senators Hillary Clinton, Barak Obama, and John McCain, which could motivate Congress to act more expeditiously to pass data security legislation. Otherwise, jurisdictional issues have kept data security legislation from gaining much momentum this Congress, and with it being an election year, it is unlikely that data security will make it onto the shortened legislative agenda.

The Chair and Ranking Member of the Senate Judiciary Committee were some of the first out the gate in the 110th Congress in introducing data breach legislation. Chairman Patrick Leahy (D-VT) and Ranking Member Arlen Specter (R-PA) introduced S. 495, the Personal Data Privacy and Security Act of 2007, on February 6, 2007. This piece of legislation would prohibit the concealment of a data security breach. It would also amend the penalties for fraud associated with the unauthorized access of personally identifiable sensitive information. Additionally, it would establish new safeguard standards for protecting sensitive personal information and impose strict penalties on

businesses who fail to meet such standards and fail to notify the proper authorities required to receive notice in the event of a breach. This bill would require “business entities to notify: 1) any individual whose information has been accessed or acquired; and 2) the U.S. Secret Service if the number of individuals involved exceeds 10,000.”

Lastly, this legislation grants combined enforcement authority to the U.S. Attorney General and State Attorney Generals. Overall, business groups and financial institutions oppose this legislation because it does not provide a trigger for breach notification so any type of breach is covered, regardless of the risk of harm associated with it. They also oppose this legislation on the grounds that it increases security mandates, and calls for additional civil penalties when businesses are already susceptible to excessive non-compliance fines from the Payment Card Industry Security Council. Given that the Chair and Ranking Member of the Senate Judiciary Committee are the lead sponsors of the bill, it has a better chance than some pending legislation to move this year; however, as mentioned before, a number of committees will seek joint referral on any comprehensive data security legislation.

Another member of the Senate Judiciary Committee, Senator Dianne Feinstein (D-CA), introduced a breach notification bill roughly a month before the Leahy/Specter bill, on January 10, 2007. S. 239, the Notification of Risk to Personal Data Act of 2007, came on the heels of one of the largest scale university breaches in history where thousands of student, staff, alumni, and applicant records were compromised at the University of California Los Angeles (UCLA). The UCLA breach compromised identity level data such as name, address, social security number, and date of birth. The goal of

---

167 Ibid.
168 Ibid.
legislation introduced by Senator Feinstein is to ensure that consumers are properly informed any time their sensitive personal information has been compromised so they can take the proper steps to protect themselves from identity theft. This legislation requires notification to any U.S. resident or third party contractor whose information may have been accessed or acquired in a breach to receive notification upon discovery of that breach unless the business affected by the breach concluded within 10 days of the breach, with input from the Secret Service, that there was no significant risk of harm to individuals whose data was involved in the breach. “Any federal agency or business entity engaged in interstate commerce that uses accesses, transmits, stores, disposes of, or collects sensitive, personally identifiable information” is covered by this breach notification standard with exemptions for national security and law enforcement purposes.169 Overall, this pending piece of legislation is not all that stringent for businesses and financial institutions because of the exemption, but it is still opposed by many under the fundamental principal that it requires the affected business to prove that there is no harm associated with the breach. It assumes guilt before innocence as some other breach notification standards require there to be proof that potential harm exists instead of proving it does not exist. Others who think stricter federal mandates, in general, are unnecessary also oppose the bill. It is unlikely that the Feinstein bill will move unless it is added as an amendment to a more comprehensive Judiciary Committee bill since the Chair and Ranking Member have their own bill.

Senator Jeff Sessions (R-AL) also introduced a breach bill, S. 1202, the Personal Data Protection Act of 2007.170 Senator Session’s bill differs from Senator Feinstein’s in

169 Ibid.
170 Ibid.
that it would establish a reasonable risk of harm trigger to require breach notification in the event that a data breach is found to have the potential for harm. It also seeks to ensure that any organization, which maintains personal sensitive data, shall implement reasonable security standards to protect personal sensitive data. This legislation also outlines the proper content, timing and method for breach notification, and it requires state attorney generals to be the primary enforcer of these security and breach standards. Additionally, it affords law enforcement ample time to proceed with an investigation prior to necessitating a public announcement regarding the breach. Lastly, it accounts for different costs associated with notification and allows for reasonable notification methods based on the size of the business responsible for the breach.

A very comprehensive bill, which has since been amended slightly, was introduced by Senators Daniel Inouye (D-HI) and Ted Stevens (R-AK) in April of 2007. S. 1178, the Identity Theft Prevention Act, addresses information protection standards, breach notification, and credit freeze. The Inouye/Stevens bill sets reasonable risk notification standards in regard to consumer notification, and similar to the Sessions bill, S. 1178 outlines the timing, content and methods for breach notification, only this bill goes into much greater detail on the specifications of all three. This legislation also provides a national credit freeze standard and seeks to curb the misuse of social security numbers by cutting down on use of it as an account identifier. This bill also covers federal agencies in regard to stricter information security standards, and is one of the overall most comprehensive pending data security bills in the Senate.

A bill introduced by Senators Tom Carper (R-DE) and Robert Bennett (R-UT), S. 1260, the Data Security Act of 2007, among other things, would hold government

\[171 \textit{Ibid.}\]
agencies accountable to the same standards as private business. The bill also outlines breach notification methods, timing, and content. One way it differs from other bills is that it accounts for the financial sectors’ current security constraints already in place under the Gramm-Leach-Bliley Act. It also spreads enforcement authority over a number of different organizations, which could create enforcement difficulties. A companion bill, H.R. 1685, was introduced in the House by Rep. Tom Price (R-GA), and essentially contains all the same provisions.\textsuperscript{172} Price’s bill was referred to three separate committees – Financial Services, Government Reform, and Energy & Commerce – so it has minimal chance of moving unless the Senate bill does.

In the House of Representatives, Rep. Bobby Rush (D-IL) introduced H.R. 958, the Data Accountability and Trust Act, which would establish stricter safeguards for electronic personal sensitive information. This legislation would require breach notification unless the covered entity can demonstrate that there is not a reasonable risk of identity theft. This is effectively much stricter than a reasonable risk trigger as the entity responsible for the breach must prove it is not at risk instead of being able to assume it’s not at risk unless a reasonable risk of harm is found, in order to not send a breach notification. This notification standard is similar to the Feinstein bill provisions. This bill also provides direction for timing, content and breach notification methods and grants enforcement authority to the FTC and state attorney generals.

Also in the House, Judiciary Committee Chairman John Conyers (D-MI) introduced H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007, in December of 2007.\textsuperscript{173} This legislation makes the unauthorized access of computers

\textsuperscript{172} Ibid.
\textsuperscript{173} Ibid.
networks a federal crime in an effort to combat increasing incidences of cybercrime. A similar bill was introduced earlier in the year by Judiciary Committee Ranking Member, Lamar Smith (R-TX).[^174] The bill, H.R. 836, the Cyber-Security Enhancement and Consumer Data Protection Act of 2007, also would crackdown on cybercrime and unauthorized access of computer networks. As Conyers and Smith are the Chairman and Ranking Member of the House Judiciary Committee, each bill has some chance of moving during the 110th Congress; wherein, the Chairman’s has a slightly better chance. Additionally, a less comprehensive bill which seeks purely to enhance federal security standards has been reported out of the House Subcommittee on Information Policy, Census, and National Archives.[^175] H.R. 4791, the Federal Agency Data Protection Act, introduced by Rep. William Lacy Clay (D-MO), “amends the E-Government Act of 2002 [which contains FISMA] to prohibit agencies from contracting with data brokers to access information on U.S. persons unless the agency head completes a privacy impact assessment and implements other safeguards.”[^176] This legislation could prove valuable in the effort to enhance federal government information security standards, and since it is limited in scope, it has at least slight potential to move this Congress.

Several bills designed to protect use of social security numbers have been introduced in the 110th Congress.[^177] H.R. 3046, The Social Security Number Privacy and Identity Theft Protection Act, was introduced by Rep. Michael McNulty (D-NY) in September and would restrict the use of social security numbers in numerous cases. The Social Security Number Protection Act, H.R. 948, was introduced by Rep. Edward

[^174]: Ibid.
[^175]: Ibid.
[^177]: Ibid.
Markey (D-MA) and would prohibit the purchase or sale of social security numbers. Also, H.R. 5234, the Social Security Misuse and Prevent Act, which calls for comprehensive social security number use reform was introduced by Rep. Rodney Freylinghuysen (R-NJ), and H.R. 136, the Identity theft Notification of 2007, introduced by Rep. Elton Gallegly (R-CA) would ensure the misuse of social security numbers would be reported to the appropriate agencies. The Gallegly bill was only referred to one committee, and as such, may have a better chance of moving than some of the other pending social security bills.

One other piece of pending data security legislation would allow for increased federal prosecution of identity theft and would seek to recover damages for time spent resolving identity theft crimes since currently victims are only reimbursed for tangible financial losses. This legislation, S. 2168, the Identity Theft Enforcement and Restitution Act of 2007, was introduced by Senate Judiciary Committee Chairman Patrick Leahy (D-VT) in October of 2007. This legislation was recommended by DOJ and the President’s Identity Theft Task Force and would empower federal law enforcement to deal with identity theft. “Under the proposed bill, federal jurisdiction could be obtained if the victim’s computer is used in interstate or foreign commerce—the same standard used in other computer hacking offenses.”

There are various other pending data security bills in the 110th Congress, and it’s highly possible that more will be introduced this year. While many groups believe some increase in federal data security regulation is necessary, others believe that existing state

laws are efficient and counteract the need for additional federal mandates. Concurrently, however, a number of state legislatures are trying to further increase data security standards.

**What are those Who Think Data Security Needs to be more Stringent Proposing at a State Level?**

Opponents of increased federal mandates have argued that state data security laws are stringent and effective. And while there are a number of credit freeze and data security breach notification laws already in existence, there has been a recent push in a number of state legislature to increase the consumer friendliness of those laws. There has also been a recent trend at the state level, on the heels of the winter 2007 announcement of the TJX breach, to implement retailer liability legislation. So far this year, retail associations in Wisconsin, Alabama, and Washington states have blocked retail liability bills. Last year, they blocked bills in Connecticut, Massachusetts, Texas, and in California where a bill passed, but was vetoed by Governor Arnold Schwarzenegger on the grounds that strict enough security measures were already in place.\(^{180}\) Legislation is still pending in Iowa, Maryland, Alaska, and New Jersey.\(^{181}\) Last year, Minnesota passed a law, the Plastic Card Security Act, which mandates retailer compliance with the Payment Card Industry Data Security Standards. The law covers any retailer doing business in the state and enforcement is effective as of August 2008 after which time retailers must cover the costs associated with fraud, breach notification, the re-issuance of

---


\(^{181}\) Ibid.
cards, and the opening and closing of accounts if they are responsible for a breach and are not PCI-compliant.\textsuperscript{182}

State credit union associations have been the leading voice in promoting increased retailer liability. Banks have stayed on the sideline for the most part due to a battle over interchange fees, fees charged to merchants every time a customer uses a credit or debit card in their store. Interchange fees average roughly 2\% of each transaction, and while that may not sound like much, it really adds up in retail industries, which operate on paper thin profit margins. One example of an industry that is feeling the interchange fee crunch is the supermarket industry with a penny on a dollar, or 1\%, average profits. With the number of electronic payment transactions rapidly increasing, estimated to constitute 55\% of all payment transactions by 2011, up from roughly 40\% in 2005,\textsuperscript{183} retailers continue lose money on increasing interchange fees. In a competitive industry, one would expect interchange fees to experience economies of scale and fall as a result of increased card transactions and technology advancements. In short though, retailers have argued that interchange fees are not competitive and not transparent, and there a number of existing bill at the state level which would increase disclosure in the setting of interchange fees or would prohibit financial institutions from collecting interchange fees on the sales tax portion of a purchase.

While interchange fees may still seem like a small percentage of a transaction, those pennies really add up for the credit card companies, and they made and estimated

\textsuperscript{182} Ibid.

profit of over $42 billion from interchange fees alone in 2007.\footnote{Merchant Payments Coalition. Online: \url{http://www.unfaircreditcardfees.com}.} As such, bankers do not want to do anything to jeopardize the way in which these fees are set, and are wary to engage retailers on data security at the state level. Last year, in Massachusetts a situation played out where the bank associations pressing for increased retailer liability in the pending state bill let up a bit because of retail threats to push interchange fee legislation. This exchange has come to the forefront with the recent introduction of federal interchange fee legislation, H.R. 5546, the Credit Card Fair Fee Act of 2008, by House Judiciary Committee Chairman John Conyers (D-MI) and Rep. Chris Cannon (R-UT).\footnote{Bill Search. Online: \url{http://thomas.loc.gov/}.}

The reason interchange fees even matter in the fight over identity theft is that banks claim that a portion of interchange fees help cover identity theft related fraud costs. According to Brandon Scholz, CEO of the Wisconsin Grocers Association, “Retailers pay very high interchange fees, and part of that is to pay for the re-issuance of cards and fraud losses in data breaches.”\footnote{Kuehner-Herbert, Katie. “Bank-CU Tactical Divide on Breach Liability Bills.” \textit{American Banker}. March 14, 2008.} In response to the recently defeated retail liability bills in Wisconsin, he said, “if the bills had passed, financial institutions ‘would be double-dipping.’”\footnote{Ibid.} To date, interchange fees have only really come into play in the state fight against increased retail liability, but it could become an argument against federal breach liability legislation if such a bill were introduced. Additionally, if the interchange fee setting process was revised in a manner that rates decreased, the government would likely save money on the interchange fees that they pay and thus would be able to use that increased revenue as a “pay-for” to appropriate additional funds toward combating

\begin{footnotesize}
\begin{enumerate}
\item[\footnote{184}]{Merchant Payments Coalition. Online: \url{http://www.unfaircreditcardfees.com}.}
\item[\footnote{185}]{Bill Search. Online: \url{http://thomas.loc.gov/}.}
\item[\footnote{186}]{Kuehner-Herbert, Katie. “Bank-CU Tactical Divide on Breach Liability Bills.” \textit{American Banker}. March 14, 2008.}
\item[\footnote{187}]{Ibid.}
\end{enumerate}
\end{footnotesize}
identity theft. This “pay-for” would make sense, especially since card companies have claimed a portion of interchange fees already go toward covering fraud costs that result from identity theft.

**What Are Existing International Standards?**

Europe has an existing EU Data Protection Directive and European Union privacy authorities are making it a priority to comply with security standards in the Directive. European Data Protection Supervisor (EDPS) Peter Hustinx believes data breach notification laws similar to the U.S. state laws may eventually be adopted in the EU, and additionally, EU companies may eventually be required to publicly disclose how they are doing in terms of data protection similar to how U.S. corporations are required to meet SOX reporting standards. Currently, data protection laws are quite different in the United States and Europe, and the EU Data Directive prohibits data transfers to countries that lack privacy standards considered adequate by the EU. The United States is not on the EU Data Directive’s list, but the EU and U.S. have created a partnership for transferring protected data between companies in compliance with the U.S.-EU Safe-Harbor agreement, which has a permanent working group to constantly monitor and upgrade the program.

---

190 Ibid.
Chapter 5: The Challenge of Emerging Technologies, Policy Recommendations, Political Feasibility, and the Importance of this Research
Emerging Challenges/Related Issues/Why Identity Theft is an Evolving Problem

“The costs of preventing identity theft will need to be balanced against the benefits of doing so to limit identity theft to an economically efficient degree.”191 Emerging technologies make it virtually impossible to combat against identity theft in full. According to a study on the economy of the Chinese web, “driven by the economic profits, cyber criminals are on the rise and use the Web to exploit innocent users;” one common form of attack is the injection of malicious code (or malware) into a compromised website.192 Additionally, the number of malicious websites continues to grow as do the number of evasion techniques.193 Consumer education of phishing and pretexting email scams is very minimal, and as these two practices continue to evolve and look more authentic, all email users remain vulnerable to these criminal tactics.

So who are these cyber criminals? “Lured by shoddy computer security and the ability to commit crimes from far-flung countries, the Russian mafia and other Eastern European gangs are plunging into spam, phishing schemes, cyberextortion and the trafficking of stolen goods online authorities say.”194 According to Andrew Klein, the existing Internet infrastructure has helped build a cyber community with, “a fair number of professional organizations in some of the foreign countries, over in Europe and such

193 Ibid. pgs. 7 and 8.
that utilize these resources, these youngster.”195 For example, “Russia has become a leading source of Internet ills, home to legions of high tech rogues who operate with seeming impunity from the anonymous living rooms of Novosibirsk or the shadowy cybercafes of St. Petersburg” with greed as the motive for most wrongdoing.196 Additionally, research has left “little doubt that the Chinese government has mounted a non-stop, well-financed attack to breach key [U.S.] national security and industry databases” likely using personnel from the China’s People’s Liberation Army . . . this is not amateur hacking. They are going back to the same places 100 times a day, every day. This kind of an effort requires a massive amount of money and resources.”197 As a result, the SANS (SysAdmin, Audit, Network, Security) Institute, placed cyber espionage on their top 10 list of security threats for 2008 and claim that these well-financed nation-state attacks will expand as hackers increasingly utilize tools, such as targeted spear phishing, to gain economic advantage.198 Cybercrime has also been linked to organized crime revenues and reports have surfaced about “organized crime and terrorist links using computer crime, hacking, and intellectual property crimes as a way of raising revenue.”199 Overall, the hacker community no longer consists predominately of

amateurs, but rather is inhabited by very well-organized groups, and historically aggressive foreign powers, posing a real threat to U.S. consumers and national security.

As hacker technologies also continue to increase coupled with the increased organization of the hacker community, the threat of cyber crime will continue to grow. One need not look any further than YouTube for mapped out instructions on how to hack into a website administration site through a procedure called an SQL Injection, a procedure which would help a hacker gain access to data stored on a mainframe computer and could prove disastrous for retailers, consumers, government, and financial institutions alike.200 “SQL Injection attacks are especially threatening because hackers can penetrate the network simply by using an Internet browser to execute code at the database layer of an application. This code can cause the database to hand over private information to hackers, redirect users to a bogus site without their knowledge, or compromise data in some other way.”201 Additionally, YouTube and the Internet create a forum for domestic and foreign terrorists to exchange emerging hacker technologies, which could eventually target the United States’ electronic online infrastructure. Not only that, cyber crimes will be increasingly difficult to punish under U.S. laws since the Internet affords foreign hackers the opportunity to remotely infiltrate U.S. computer systems without setting foot on U.S. soil; thus, not being constrained by U.S. criminal penalties. In a world where international law is not generally enforced in commonplace cases, Russian, Chinese, and other hackers essentially have default immunity from their

---

crimes because of the global nature of the Internet, which makes cyber crime a particularly difficult threat to police.

As evidenced by the Hannaford breach, hacking technologies also continue to evolve and become more sophisticated. In this case, data was stolen in transit as it was being transmitted during the authorization process due to malware, which was likely remotely installed on the company’s mainframe server. Credit card data is not currently PIN protected like PIN-based debit is and is thus more vulnerable as it is being transmitted electronically. Retailers would prefer PIN credit standards, but that requires costly technology enhancements on the part of the card processor’s (merchant acquires), which have little financial or consumer confidence incentive to change their data acceptance standards, since they are not the outward face of a data breach. Even PIN protecting credit card information may not be enough, however, in today’s world of continuous technological advancement. Early findings from the Hannaford breach indicate that the malware installed on the company server may have been able to convert PIN-based debit over to signature debit making that data vulnerable, as well.

Princeton University researchers recently discovered that they could extract data from a computer’s dynamic random access (DRAM) chip. According to the study, DRAM (or memory) chips used in most computers retain contents for seconds after the computer is powered off, and the Princeton study shows new techniques for extracting that data.202 “When the chips were chilled using an inexpensive can of air, the data was frozen in place, permitting the researchers to easily read keys out of the chip’s

---

This is a potential threat to laptop users who rely on disk encryption since a criminal could effectively mount an attack to access sensitive information even if a computer is locked or turned off. Considering a number of government-issued laptops are lost or stolen each year, this could potentially be a very large national security hazard in the future.

Data extraction on another front, also poses a major concern. Recently, radio frequency identification (RFID) technology tests have shown that RFID technology scanners have the ability to extract card data through card reader technology so a criminal could steal credit card information using one of these devices without the victim ever being aware. At a 2008 conference, a security expert used a card reading device to scan an RFID American Express ExpressPay card, and was able to extract card account data without ever removing the card from the victim’s wallet. RFID technology “toss[es] out bits of data that are caught by receivers, with little or no contact, just thorough the air in some cases,” which makes new contactless credit cards, such as ExpressPay and MasterCard’s PayPass, particularly vulnerable. The bigger issue is that a number of “wallet” items are utilizing RFID technology ranging from Metro SmarTrip cards, to driver’s licenses and passports, so more and more personal information is being thrown

---

204 “Lest We Remember: Cold Boot Attacks on Encryption Keys.” Princeton University.
out over radio frequencies just waiting for thieves to capture it. Credit Card companies have claimed that data on these cards are encrypted making it very difficult for thieves to use any information they may obtain via radio frequencies, but nonetheless, security experts argue that a metal cover or shield for RFID enabled cards can help keep sensitive data secure as hackers and identity thieves continue to employ new theft techniques.

Two forms of emerging payments that host security concerns as a result of their utilization of RFID technology are contactless and mobile payments. With contactless payments data is transmitted openly over radio frequencies, and there is the possibility of it being intercepted by anyone. Many consumers have said they will adopt contactless payments because of the convenience, but 47% of 1,300 surveyed adults said they would not use this new technology because of security concerns, such as someone stealing card information or the possibility of the card technology not working properly. Regardless of some security concerns, contactless cards continue to grow in the U.S. as the 10 million cards in circulation in 2005 has increased to upward of 60 million cards in circulation today. Similarly, RFID technology has security information implications for mobile phone payments technology. Mobile phone payment technologies do not just include point-of-sale transactions, but also cover the payment of bills from a handheld device and person-to-person (P2P) payments. While these are novel ideas that haven’t really been targeted to the proper market segment just yet, they have the potential to take off in the near future. There are some security risks involved with mobile payments because

---

207 Ibid.
208 Ibid.
payment data is transmitted using Near Field Communication (NFC) technology, which utilizes contactless chips that can transmit payments data via short-range radio frequency technology at the point-of-sale,\textsuperscript{212} so mobile payments are no more secure than other forms of RFID–based technology. Citigroup plans to release NFC-enabled mobile phones in the second half of 2008.\textsuperscript{213}

Additionally, technology advancements have enabled electronic manufacturers to combine a number of wants and necessities into one device. If people use the same device they use to check their work email to download music, access YouTube videos, store pictures, access the Internet, and make phone calls, it creates a security risk for the network supporting the work email. To link banking information to that device, while convenient, would just cause more security concerns. Lackluster IT security options on the Apple iPhone made recent headlines in the \textit{Wall Street Journal} which claimed that the iPhone is less secure than business smart phones, such as Blackberry’s, because it is a consumer-oriented product.\textsuperscript{214} Additionally, the \textit{Journal} conveys that “there is no way to force employees to protect their iPhones with passwords and that they can’t erase sensitive corporate data from remote locations if the device is stolen or lost.”\textsuperscript{215} In a business-environment where technologically savvy users may take it upon themselves to sync their personal technology, such as their iPhones, with their employer’s network server, they add an often unknown security risk to their employer’s IT operation. Apple is

\begin{flushright}
  \textsuperscript{213} Ibid.
  \textsuperscript{215} Ibid.
\end{flushright}
preparing to launch software upgrades in summer 2008, but it will likely be awhile before
the iPhone is completely business-friendly.216

Data security complications for consumers, retailers, and financial institutions are
manifest in the number of emerging technologies that have the potential to circumvent
existing data security standards. While these complications pose the potential for
significant financial loss and emotional harm, they present and even greater threat to the
U.S. government as cybercrime technology continues to evolve. According to Kim
Cameron, who is employed by Microsoft, “The internet was built without a way to know
who and what you are connecting to, [which is bad enough in the private sector, where
the only thing at stake is money, but] for dealing with government, it is potentially
catastrophic.”217 Additionally,

“there is little legal basis for dealing with cybercrime. Identities are
valuable, allowing crooks to empty bank accounts or buy things online. Cybercriminals have been targeting individual internet users with
“spyware” (which records keystrokes) and “phishing” (bogus e-mails that
trick users into providing personal information online). But the huge
databases held by governments would be a much bigger prize. If you
know someone's name, address, date of birth, mother's maiden name and
bank-account details, you are well placed to steal from them. Medical
histories could prove equally valuable . . . E-government looks like a
potential crock of gold for fraudsters, with huge databases compiled by
law, most of them only lightly and incompetently protected, and ambitious
plans for even more.”218

Overall, theft by emerging technologies could have more devastating affects on the
government than on consumers, retailers and financial institutions merely because of the
sensitive nature of data stored by federal agencies. Emerging cybersecurity threats are not

216 Ibid.
218 Ibid.
addressed in detail in existing security standards or regulations, and will need to be addressed in future policies. A research fellow at the National Defense University’s Center for Technology and National Security Policy, recently declared, “‘where we are on cyber is like where we were in the early 1970s with respect to the environment . . . the government knows there is a problem percolating, but does not know how it should be handled.’”219 Overall, cyber crime will continue to be a threat to U.S. economic and national security as it continues to evolve utilizing new and innovative technologies.

**Policy Recommendations**

With emerging technologies and the prevalence of portable handheld devices in the workplace, it is virtually impossible to completely safeguard all sensitive stored information and in effect deter identity theft attacks 100% of the time. As such, it is absolutely imperative than any comprehensive federal legislation emphasize the need to do one of two things or a combination of both: 1) cut down on the misuse of compromised data; and/or 2) take away hacker’s motives to access sensitive data by not requiring retailers to store any data beyond a transaction authorization code. David Hogan, senior vice president and chief information officer at the National Retail Federation (NRF) argues that “the problem of major data breaches would virtually disappear if credit card companies adopted NRF’s solution and gave retailers a choice in how they store their data. It makes more sense for credit card issuers and networks to protect their data from thieves than to expect millions of merchants scattered across the

---

nation to lock up their data for them.”²²⁰ Hogan also believes that PCI compliance is not by any means a solution to the ongoing problem of identity theft and he cautions, “once the industry is 100% [PCI] compliant, we will realize that we never attacked the problem at its root. We made it harder for criminals to attack us, but we never took away their incentive.”²²¹ Others have also hypothesized that “the most effective way to control the damage from a breach if it does occur is to ‘make the data useless’ – that is, have infrastructure in place such that even if data are compromised, they cannot be used to access cardholder accounts.”²²² Changing data storage standards may also be the most cost-effective means by which to protect data in the future. “NRF estimates all merchants have spent more than $1 billion over the past three years on PCI compliance, an expense that will be ongoing because of required periodic system scans and audits. All that effort won’t deter hackers if they know a retailer may be storing thousands or millions of card numbers, according to Hogan.”²²³

As long as PCI DSS continues to require retailers to store data, effectively creating an incentive for thieves to launch attacks to retrieve the data, the payment card networks (i.e. Visa and MasterCard) and card-issuing banks (i.e. Bank of America, Citigroup, JP Morgan Chase, Capitol One) should be liable for data compromised as a result of a breach because 1) most retailers would prefer not to store data at all, but they are mandated to under PCI DSS; 2) retailers have already spent millions of dollars in efforts to comply with PCI DSS and will continue to spend more annually to keep up

²²¹ Ibid.
with improved security standards;\textsuperscript{224} 3) large card-issuing banks and financial institutions operate on much larger profit margins than most retailers where there is more industry-wide competition and thus much smaller profit margins; and 4) banks have a longer pre-existing relationship with most of their account-holders than do retailers, making notification a much easier process for the banks since they already have mailing addresses, and likely email addresses, of their customers stored in a database. Additionally, if payment card networks and card issuing banks are not held at all accountable for breaches, they have limited financial incentive to do everything within their capability to prevent a breach:

“Networks can adopt policies that impose minimum security practices or contractually assign liability for data breaches to improve within-network investment in security, but a network’s security will still be too lax if the network’s own breaches can impose losses on entities outside the network, including other networks, and the network does not bear the cost of those losses.”\textsuperscript{225}

As previously mentioned, retailers have a consumer confidence incentive to protect against a breach, without the additional looming threat of an increased liability standard.

Liability should also fall to banks and card networks because fraud protection was one of the incentives banks used to entice retailers to accept credit and debit cards long before electronic payments saturated the payments market. It would not be fair to now pass off additional fraud costs to retailers, essentially taking away an incentive originally used to entice businesses to accept electronic payments, now that those businesses cannot

\textsuperscript{224} Ibid.
reverse that decision without losing exceptional profits. Additionally, card issuing banks and card associations claim that a portion of the interchange fee charged to retailers on every card transaction goes to cover fraud costs so passing breach liability and fraud costs on to retailers would essentially be double dipping, and would be poor policy. Also, retailers already take a financial hit with the costs of charge-backs in the event that purchases are fraudulently obtained; covering the costs of breach notification and card re-issuance would mean additional financial loss for retailers, and it would be more suitable and cost-effective for financial institutions to continue to shoulder the burden of that cost. There should, however, be an exemption if compromised data results from a breach where the business entity is not PCI DSS, SOX, and HIPAA compliant (if any or all of those apply). The 2007 Minnesota law, under which retailers must cover the costs associated with fraud, breach notification, the re-issuance of cards, and the opening and closing of accounts, is poor public policy.

Identity theft itself is of course a crime; however, major financial loss, as well as emotional trauma result from an identity thieves’ ability to use stolen information to fraudulently access existing accounts, open new accounts, apply for loans, etc. As such, banks and financial institutions are financially and socially responsible for damages resulting from identity theft because they are, in many cases, responsible for whether or not stolen data can be misused. Data will never be 100% secure so it’s imperative that banks and financial institutions be more cautious when granting access to accounts and when allowing the creation of new accounts. Identity theft and resulting fraud are similar to drug manufacturing and trafficking. Production of illegal drugs is a crime in this country, similar to how the theft of sensitive data and the means through which it is
obtained is a crime. It is, however, the misuse of stolen data, or fraud, which results in the most harm to consumers. Similarly, it’s the trafficking and eventual misuse of illicit drugs that leads to the greatest harm for consumers. As such, U.S. policies should reflect the importance of the latter and the prevention of misuse of stolen data.

Both business and consumers may be better off without comprehensive federal legislation if legislation creates any undue and unnecessary mandates; however, there are some basic policies (i.e. social security number safeguards, credit freeze and breach notification) associated with data security that should be addressed at a national level to help create a more uniform standard to ease data breach response by multi-state corporations, and to protect consumers who live in states with rather lax data security laws. Given that it is difficult to pass legislation with it’s original language, the offensive pursuit of these basic policies is rather risky, and it may not be in the best interest of businesses and financial institutions to pursue such national standards offensively unless more restrictive state laws, such as the Minnesota law, begin to surface. In other words, while national standards for social security number protections, credit freeze, and breach notification may encompass the most sound policy prescriptives, the lack of political feasibility of passage of these policies in their intended form may be enough to deter business interests from actively pursuing federal breach standards at this time. In the event that consumer groups push for national standards, which they will likely continue to do, other special interests will try to pursue legislation that is the least restrictive to their businesses.
Increased safeguards for social security numbers are a sound policy idea, but businesses, financial institutions, and education establishments need adequate time to comply with new standards. Reducing the use of social security numbers as an account identifier is a good, preventative method to deter against theft, and should be included in any comprehensive federal legislation. There should, however, be a four to five year phase-in period for covered entities to comply with the new safeguard standards since most entities have at least a three year record retention period. Overall, a phase-in period is the only practical and feasible way to get businesses and financial institutions to comply with increased social security number safeguard mandates, as well as to gain the support for any social security number reform policies from those groups.

As for credit freeze policy, national credit freeze became available in November 2007 as TransUnion, one of the big three credit firms, announced it would allow consumers in all 50 states to place a credit freeze.²²⁶ This thesis supports a national standard for credit freeze because credit freeze affords all consumers the opportunity to help prevent identity thieves from opening new lines of credit; however, this thesis recommends that the costs associated with a credit freeze should be incurred by individuals. If there is not a charge associated with credit freeze, it could create a free for all where consumers would likely abuse their right to a credit freeze, and it could become costly and an annoyance for credit companies, as well as for consumers who would eventually have to unlock their credit reports to obtain new credit. Maintaining a financial

cost for credit freeze will help prevent against unnecessary use of this tool. Additionally, the placement of a 90-day fraud alert on an individual’s credit report, is also a suitable option for potential identity theft victims, and should be more widely encouraged as an alternative to credit freeze.

Ideally, there would be a national standard for breach notification, even though there are a number of existing state laws. A national standard for breach notification would help reduce confusion businesses face in the wake of a breach. Since different states currently have different laws, it causes confusion for regional and multi-state operators. A reasonable risk trigger is an absolute necessity as part of a national breach notification standard. A number of states have acquisition-based triggers at the moment, which is costly and runs the risk of desensitizing consumers. Data breach notification is merely a fear-mongering tactic if there is minimal chance of data being misused. Overall, this thesis strongly supports a national breach notification standard as long as legislation contains a reasonable risk trigger that assumes first that a reasonable risk of harm does not exist unless proven otherwise as opposed to a breached company having to prove that no reasonable risk of harm exists to avoid issuing a breach notification.

Both breach notification and credit freeze are reactive policies to minimize loss in the event an identity theft occurs, and while not poor policies, if implemented under the standards previously mentioned in this thesis, they do very little to actually curb identity theft and fraud except that they help uncover incidences of misuse more quickly, which should prevent further financial loss and emotional harm. In determining appropriate breach notification standards, it is important to account for small businesses and their cost
constraints in regard to reactive methods, as well as their hardship in becoming PCI-compliant in the first place. Policies need to adequately reflect the needs of smaller merchants and financial institutions.

Education and awareness are the key components necessary to minimizing preventable incidences of identity theft. Identity theft is virtually unpreventable, but it is critical that U.S. consumers take the necessary precautions to prevent identity theft whenever possible and those precautions begin with sound consumer education. One way to educate consumers is via newspapers and cable news networks, as well as morning shows with top viewer ratings, such as the *Today Show* and *Good Morning America*. The government could also use public funding for the Ad Council to run advertisements on public radio. The FTC could start a nation-wide education campaign, similar to D.A.R.E. (Drug Abuse Resistance Education), and could try to reach parents through educating their children who fall into the most at risk age segment when they turn 18 anyway. Additionally, consumer groups, such as U.S. PIRG, could orchestrate town hall meetings across the country to help educate consumers, and banks could increase identity theft prevention education when they sign people up for new accounts. Overall, increased education in regard to protecting sensitive personal data in an effort to deter identity theft and fraud, could be part of a larger piece of banking reform legislation promoting greater fiscal responsibility and increased responsibility toward consumers in light of the subprime mortgage fall out.

Making information available over the Internet is useful, and the FTC website is very well organized; however, the Internet is an active tool, not a passive one. People
generally have to have an interest in identity theft in order to seek out information on it, and as such, exploring the World Wide Web for identity theft information is more likely to happen as a reaction to anticipated or existing identity theft, as opposed to passive education methods which better serve a preventative purpose. Overall, there is a profit to be made from identity theft so the market for identity theft crimes is not going to disappear. Not only is there a financial incentive tied to identity theft related fraud, there is also the incentive to use someone else’s identity to help get a job or to obtain government documents regarding proof of citizenship, such as in the case of illegal aliens trying to find a way to stay in the country.

Another reactive measure would be to create a national crime center for victims of identity theft. This could be run by the FTC or DOJ, but would need to obtain adequate funding from the appropriations process. Since data security is not a huge partisan issue, obtaining such appropriations would likely not be much of a problem. Along these same lines, the U.S. should do everything possible to make recovery of assets as easy as possible for identity theft victims. While it makes sense to have a national enforcement arm for identity theft crimes, such as the U.S. Attorney General, the attention paid to victims will likely suffer. Instead, it makes more sense to allocate enforcement power to state attorney generals, as localizing the response efforts is likely to make victim recovery a more expedient and well-monitored process.

As mentioned before, while a national breach standard may be the best policy recommendation, lack of a national standard may prove a better option than the risk of being faced with an unworkable piece of federal legislation under tangible political
constraints. As interstate and global commerce are commonplace business practices, the need for a cross-border strategy will continue to grow, and will likely become an eventual necessity, but for the time-being, or at least through the end of the 110th Congress, businesses and financial institutions may just want to defend against harmful consumer-backed data security legislation mandates. As previously mentioned, a number of state data security laws exist, but there are large discrepancies in the protections that many states provide, and thus, pre-emptive national data security standards will likely be necessary at some point in the future.

Data security standards in the private sector, which retains mostly account level data, are rather stringent already. Security safeguards appear to be less stringent for public sector entities, such as public universities, which often maintain identity level data. “A network’s security is only as effective as the security of the weakest link- the participant most likely to experience a data breach.”227 As such, any federal legislation that mandates increased security standards for the private sector should also cover public sector entities, such as the government and public universities.

Hacking, phishing, pretexting, and other online criminal tactics are more serious than data security breaches as a whole because they are all acts done with malicious intent; thus, there is a greater risk of identity theft associated with them. Additionally, emerging technologies to combat these types of theft are more difficult to keep up with than other theft techniques. Overall, government data is more at risk for this type of theft than private retail businesses, which creates a greater risk of national security and lends

itself to the question of whether or not the government should be held to higher security standards. While national data security standards are important, they should take a back seat to increased enforcement of information security standards for the government. To fuel this school of thought, retailers and financial institutions could employ a campaign entitled “Bigger ‘Phish’ to Fry” advocating for stricter government protections against phishing attacks before the targeting basic data security enhancements. Overall, cybercrimes against the government pose a much greater threat than the theft of personal sensitive data, which can sometimes later be used to commit identity theft crimes. This thesis recommends eventual national policy standards for preventing and protecting against identity theft, but finds that it is much more important to first address the lackluster information security standards employed by U.S. federal agencies. The real problem with increased security standards for the government is employing an enforcement mechanism. As previously mentioned, it is not feasible to withhold funding from the majority of federal agencies who do not meet current FISMA standards so there is not a financial incentive for government entities to enhance security efforts. Short of revoking an agency’s Internet access, there do not seem to be many ways to enforce government information security standards, which will make government enforcement and incentives the main information security policy challenges going forward.

**Political Feasibility**

Barring a large-scale data breach, it is unlikely that any federal legislation will pass during the 110th Congress because of the shortened legislative agenda in an election year. It appears as though comprehensive data security will not be addressed until the
111th Congress due to time constraints unless a data security measure passes at the end of the 110th Congress as part of a larger spending package. There is also the possibility that data security measures could be tied in to a larger banking reform package. The main reason data security has not moved is there are a number of jurisdictional battles being fought over security policy, and a handful of congressional committees want to offer insight into the crafting of comprehensive legislation, as well as hold hearings on the issue. According to Senate Commerce committee staff, the committee will be looking to reconcile the Inouye/Stevens data security bill with the Leahy/Specter bill, but even if they accomplish that reconciliation, they will still face the Banking Committee, which has some jurisdiction over data security legislation, and as such, data security legislation is not likely to move until the next Congress.228

It is important to evaluate the main political players and their stances on each policy issue in an effort to outline the political feasibility of any of the smaller components of data security legislation passing. A reasonable risk of harm breach notification standard is strongly supported by both retailers and financial institution; whereas, consumer groups feel that notification should happen any time a consumer’s information is compromised. The battle over liability standards exists predominately at the state level between retailers and the credit unions. Banks are mostly staying out of this battle because of the implications tied to profitable interchange fee structures. Additionally, banks are hit with very minor fraud costs because fraud chargebacks are covered by retailers. In regard to credit freeze, some financial institutions and credit firms

are adamantly opposed to increased regulation. Retailers don’t care all that much, and consumer groups feel very strongly that increased access to credit freeze is vital. Lastly, social security number misuse is a huge issue for consumer groups. If compliance standards are feasible, social security number safeguard reform isn’t likely to be one of the battles banks and retailers choose to fight. Overall, anytime two of the three of these groups feel very strongly about one of the policy issues, it’s likely that the other group or groups will have to give in on that issue or elsewhere. It’s likely that federal credit freeze and social security number legislation could pass and become law, but it’s highly unlikely that a liability bill will pass Congress anytime soon, and it’s unlikely that a national breach notification standard that does not contain a reasonable risk of harm trigger will pass.

**Difficulties with this Study**

The main difficulty with this study is that it is virtually impossible to link a data security breach directly to an incidence of identity theft fraud so it is hard to say that certain data breaches are more harmful than others. In the event of a data breach, the theft of the data is the initial crime, but fraud used to open new bank accounts or access existing accounts is the real crime associated with identity theft since it’s the misuse of stolen personal data. Not only that, there are likely many breaches that go undetected or that are not publicly disclosed.

Additionally, this study is constrained by the ability to measure actual compliance with existing security standards. Aside from the recent GAO study regarding federal agency information security standards, there are no real benchmarks for sounds security
practices and standards. PCI DSS is supposed to act as a major deterrent to the accidental compromise of data; however, the Hannaford Bros. breach demonstrates that those safeguards certainly are not fool-proof, and new criminal technologies continue to emerge, which make those standards outdated. As such, data security issues continue to change as this thesis is being written; additional technologies could emerge tomorrow effectively making some of these policy recommendations outdated.

One final difficulty is author bias. The author of this thesis has worked for the retail industry for two and a half years and is better-educated on private sector retail standards and is more inclined to agree with the security stances taken by those in the retail community than those employed by the government or public universities.

**Why is this Research Important?**

This research is important because it outlines how identity theft harms it’s victims, how identity theft occurs, which safeguards are currently in place to deter against identity theft, pending state and federal legislation and the policy issues contained in those bills, and it explores new technologies that information security professionals and state and federal lawmakers and law enforcement officials will need to keep up with in order to prevent identity theft from becoming an out of control problem.

This study is important because it examines the compliance of federal agencies with existing security safeguards, and this study addresses the national security risks associated with lax government and other public sector security standards. Cybercrime continues to grow as a real threat, and this thesis emphasizes the importance of keeping up with emerging information security threats. With ever-increasing technologies, it will
be more and more difficult for businesses, government, and financial institutions to thwart identity theft criminals. With rapid growth of the Internet and exponentially increasing electronic banking and retail payments, more and more sensitive information is being shared over the Internet and electronic channels. Additionally, as generations who are more comfortable using the Internet, computers, and online services become financially independent, more personal information will be floating around on the World Wide Web. Currently, there are a number of people from older age groups who are uncomfortable using the Internet for certain services, such as banking needs and shopping, but as those numbers shift over time, more and more volatile information will become available online. Overall, identity theft will remain a problem because there is a market for fraud tied to the theft of personal sensitive information. Until it becomes more difficult to misuse compromised data, identity theft will remain prevalent because there is a profit to be made from this criminal activity. Ever-evolving technologies will make it virtually impossible for consumers, retailers, financial institutions, and government to keep up with identity theft criminals so this analysis is important as identity theft will likely remain a relatively prominent crime for many years to come regardless of any increased data security standards that become federal or state law, and regardless of pre-existing security standards.
Glossary of Terms

Department of Justice (Office of Justice Programs/Office of Crime Victims)
The Identity Theft and Fraud pages provide information about identity theft and fraud, what to do if you are a victim, and updates on DOJ responses to identity theft and fraud.

Federal Trade Commission (FTC)
The FTC provides the U.S. Government's central website for information about identity theft. The website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.
http://www.ftc.gov/bcp/edu/microsites/idtheft/

Department of Homeland Security (DHS)
The National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America’s cyber assets. The Department of Homeland Security is also home to the U.S. Computer Emergency Readiness Team.

U.S. Computer Emergency Readiness Team (CERT)
The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation’s Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.
http://www.us-cert.gov/

National Cyber Response and Coordination Group (NCRCG)
Established in partnership with the Department of Defense and the Department of Justice, NCRCG serves as the federal government's principal interagency mechanism for coordinating efforts to respond to and recover from cyber incidents of national significance.
http://www.us-cert.gov/federal/collaboration.html

National Institute of Science & Technology (NIST)
Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. Promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act.

Federal Information Security Management Act (FISMA)
Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
President’s Identity Theft Task Force
The President’s Task Force on Identity Theft was established by Executive Order 13402 on May 10, 2006, launching a new era in the fight against identity theft. The President’s charge was to craft a strategic plan aiming to make the federal government’s efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. To meet that charge, the Task Force, chaired by the Attorney General and co-chaired by the Chairman of the Federal Trade Commission, focused on several areas including government safeguards, education, and law enforcement.
http://www.idtheft.gov/about.html

Payment Card Industry Standards Council
The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
https://www.pcisecuritystandards.org/

Payment Card Industry Data Security Standards (PCI DSS)
The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.
https://www.pcisecuritystandards.org/tech/index.htm

Identity Theft Resource Center (ITRC)
Identity Theft Resource Center® (ITRC) is a nonprofit, nationally respected organization dedicated exclusively to the understanding and prevention of identity theft. The ITRC provides consumer and victim support as well as public education. The ITRC also advises governmental agencies, legislators, law enforcement, and businesses about the evolving and growing problem of theft.
http://www.idtheftcenter.org/

Privacy Rights Clearinghouse (PRC)
The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization with a two-part mission -- consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, California.
http://www.privacyrights.org/identity.htm

Coalition for Data Security
The Coalition for Data Security is a resource for consumers, businesses, policymakers, and the media for matters related to data security breaches. Members include retail associations and financial institutions.
http://www.coalitionfordatasecurity.org/about/default.aspx

Food Marketing Institute (FMI)
Food Marketing Institute (FMI) conducts programs in research, education, industry relations and public affairs on behalf of its 1,500 member companies — food retailers and wholesalers — in the United States and around the world. FMI’s U.S. members operate approximately 26,000 retail food stores with a combined annual sales volume of $680 billion — three-quarters of all retail food store sales in the United States. FMI’s retail membership is composed of large multi-store chains, regional firms and independent supermarkets.
http://www.fmi.org/
National Retail Federation (NRF)  
The National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail companies, more than 25 million employees - about one in five American workers - and 2007 sales of $4.5 trillion.  
http://www.nrf.com/

Consumers Union (CU)  
Consumers Union (CU) is an expert, independent, nonprofit organization, whose mission is to work for a fair, just, and safe marketplace for all consumers. CU publishes Consumer Reports and ConsumerReports.org in addition to two newsletters, Consumer Reports on Health and Consumer Reports Money Adviser with combined subscriptions of more than 7 million.  
http://www.consumersunion.org/

U.S. Public Interest Resource Group (U.S. PIRG)  
U.S. PIRG, the federation of state Public Interest Research Groups (PIRGs), takes on powerful interests on behalf of the American public, working to win concrete results for our health and our well-being. With a strong network of researchers, advocates, organizers and students in state capitols across the country, we stand up to powerful special interests on issues where powerful special interests stand in the way of reform, like product safety, identity theft, political corruption, prescription drugs, and voting rights.  
http://www.uspirg.org/

Identity Theft and Assumption Deterrence Act of 1998  

Sarbanes-Oxley  
The legislation came into force in 2002 and introduced major changes to the regulation of financial practice and corporate governance. Named after Senator Paul Sarbanes and Representative Michael Oxley, who were its main architects, it also set a number of deadlines for compliance.  
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107

Health Insurance Portability and Accountability Act of 1996  
The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information.  
http://www.hhs.gov/ocr/privacy/privacyinitiatives/hipaaglobal.html

Gramm-Leach-Bliley Act (GLB Act)  
The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.  
http://www.ftc.gov/privacy/privacyinitiatives/glba.htm

Fair and Accurate Credit Transaction Act of 2003 (FACTA)  
FACTA imposed increased security standards on retailers, created a national system for fraud protection, and gave consumers the right to receive one free credit report per year from each of the nationwide credit reporting agencies.  

http://www.nrf.com/  
http://www.consumersunion.org/  
http://www.uspirg.org/  
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107  
http://www.hhs.gov/ocr/privacy/privacyinitiatives/hipaaglobal.html  
http://www.ftc.gov/privacy/privacyinitiatives/glba.htm  
**Ponemon Institute**

Ponemon Institute is an organization dedicated to independent research that advances responsible information, privacy and security management practices in business and government. Founded by Dr. Larry Ponemon in 2002, the Institute, in addition to research, engages in projects to educate leaders in the private and public sectors about responsible information management and to verify the privacy and data protection practices of organizations.

http://www.ponemon.org/fellowsabout.html

**Gartner Research Firm**

Gartner, Inc. (NYSE: IT) is the world’s leading information technology research and advisory company. Through the resources of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events, Gartner works with every client to research, analyze and interpret the business of IT within the context of their individual role. Founded in 1979, Gartner is headquartered in Stamford, Connecticut, U.S.A., and has 4,000 associates, including 1,200 research analysts and consultants in 75 countries.

http://www.gartner.com/it/about_gartner.jsp

**The SANS (SysAdmin, Audit, Network, Security) Institute**

A leading organization in computer security training, the SANS Institute is also known for developing, maintaining, and making available at no cost the largest collection of research documents about various aspects of information security. SANS also operates the Internet's early warning system - the Internet Storm Center. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

http://www.sans.org/why_sans.php

**EU Data Protection Directive**

Provides security directives for EU Member States in regard to their right to privacy with respect to personal data, as well provides security protection guidelines for the cross-border transmittal of personal data.

Bibliography


“Bush Asks $17 Million Increase for CTC, Bulk of Funding to Address Identity Theft.” 


PCI Council. Online: https://www.pcisecuritystandards.org/
PCI Data Security Standards. Online: https://www.pcisecuritystandards.org/tech/index.htm


“Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown.” Report to Congressional Requestors. Government Accountability Office. June 2007.


Zogby Poll: Most Americans Worry About Identity Theft. “Survey shows vast majority concerned companies may sell their information or are not doing enough to keep it safe from theft” Released: April 03, 2007. http://interactive.zogby.com/index.cfm
Curriculum Vita

Elizabeth L. Garner was born in Dallas, Texas on December 18, 1981. She graduated from Greenhill School, Addison, Texas, in June of 2000. She earned a Bachelor of Arts from Vanderbilt University in May 2004. Her major was International Studies and her minor was Spanish. Elizabeth studied abroad in Cambridge, England during the summer of 2002 attending classes at the Institute of Economic and Political Studies. She also studied abroad in Melbourne, Australia at Melbourne University during the spring of 2003. Elizabeth enrolled in the Johns Hopkins Master of Arts in Government program during the fall of 2006 and anticipates graduating in May 2008 with her M.A. in Government and a concentration in Political Communications.