9-1-2010

Strengthening Credit Freeze Legislation in the States: Empowering Consumers to Prevent Economic Loss from Identity Theft

Richard G. Kunkel J.D.
University of St. Thomas, Minnesota, rgkunkel@stthomas.edu

Cover Page

Strengthening Credit Freeze Legislation in the States: Empowering Consumers to Prevent Economic Loss From Identity Theft

Richard G. Kunkel
Associate Professor of Business Law
Department of Ethics and Business Law
Opus College of Business
University of St. Thomas
2115 Summit Avenue
St. Paul, MN 55105
651-962-5132
rgkunkel@stthomas.edu

Strengthening Credit Freeze Legislation in the States:
Empowering Consumers to Prevent Economic Loss From Identity Theft

Identity theft has been described as the "crime of the new millennium"[i]. Since the mid-1990s, it has been known as the fastest growing crime in the United States.[ii] In November 2007, the Federal Trade Commission ("FTC") reported the results of its comprehensive survey of identity theft incidents during 2005.[iii] (hereinafter, the "FTC 2007 Survey"). The FTC 2007 Survey estimated that 8.3 million Americans were victims of identity theft.[iv] Economic losses from identity theft have been estimated at $50 billion annually.[v] Beyond the economic loss, the various forms of identity fraud have been condemned as a crisis threatening national security, global commerce and protection of society.[vi]

Identity theft has continued to grow despite new legislation intended to prevent it. The state and federal legislative response to identity theft has primarily focused on *information theft prevention* by criminalizing theft of personally identifiable information. Though necessary and well intended, these laws have not stopped the growth of identity theft. Sophisticated criminals already have access to substantial amounts of identity information and are readily able to steal more information through hacking, data breaches, computer theft, phishing scams, spyware and other malicious activity. These criminals also are able to sell or acquire the information on global black markets[vii] and they have the computing power to aggregate identity data from many disparate sources in order to carry out their schemes.

Laws criminalizing information theft prevention must be complemented by laws aimed at *economic loss prevention*. The FTC's first survey of identity theft in 2003 (hereinafter, "FTC 2003 Survey"), estimated that nearly $37 billion dollars of identity theft losses, or nearly 70 percent, are caused by identity thieves' ability to open new lines of credit.[viii] Credit reporting agencies, lenders and merchants continue to use risky identity authentication practices that are not adequate to protect consumers from loss. Savvy criminals quickly convert stolen identity information into money, goods and services. These industry practices are unlikely to change because there are strong disincentives against making them more rigorous in a marketplace that expects instant credit. Thus, the key to preventing economic loss is empowering consumers to protect themselves by taking control of their own credit information.

This article will focus on state legislation designed to prevent identity theft economic losses - the credit freeze (also known as a security freeze). Beginning with California in 2003[ix], forty seven states and the District of Columbia have now have armed consumers with a tool to prevent economic loss – the ability to place a freeze on their credit files.[x] Once a credit freeze is in place, credit reporting agencies are prohibited from releasing the credit verification information required for identity thieves to open new accounts with merchants and lenders. Further, credit freeze legislation is an important as first step toward providing consumers with increased control over the security of their credit records.

This article will first introduce the nature of the identity theft schemes, the economic losses caused and the broad extent and seriousness of identity theft. Second, the article will review the legislative response to identity theft. Most legislation has focused on preventing information theft prevention by means of criminal statutes that have been largely ineffective. Third, the vulnerabilities in identity systems that make it exceeding difficult to effectively prevent theft of personal information will be considered. Fourth, the article will review the risky credit and lending practices that enable identity thieves to open fraudulent new accounts and the disincentives against changing these practices. Finally, the new state credit freeze legislation focused on economic loss prevention will be explored. Permitting consumers to obtain a security freeze on their credit reports, thereby disrupting ability of identity thieves to open new accounts, is the most feasible and effective means to prevent economic loss. It also is an important first step toward further strengthening consumer control over their credit information.

I. Identity Theft and Economic Loss.

An identity fraud scheme can be divided into two main operational segments. In the first segment, or "front end" of the scheme, the thief needs to illegally obtain and aggregate the personal information of the victim. This stolen information enables the identity thief to assume the identity of the victim and transact business in the victim's name. In the second segment, or "back end" of the scheme, the thief needs to convert the stolen personal information into cash, property, vehicles, goods or services. Identity thieves can manipulate

existing banking and credit accounts of the victim or they can establish new lending and credit accounts in the victim's name. This segment of the scheme enriches the thief and causes economic loss either to the individual victim, to the lenders or merchants holding the manipulated fraudulent accounts, or both. This article will focus on the "back end" of the identity theft scheme, i.e. the thieves' ability to convert stolen personal information into ill-gotten lucre.

Mushrooming identity theft in the early 2000s caused the FTC to undertake a comprehensive attempt to estimate the number of victims and the economic losses caused by identity theft. The FTC 2003 Survey concluded that over 9.9 million Americans were victims of identity theft that caused losses of $52.6 billion per year.[xi] It also found that identity theft victims spent a total of 297 million hours of time attempting to recover from the effects of their stolen identity.[xii] Frauds involving new accounts and other frauds accounted for nearly $37 billion dollars in losses to businesses and consumers. The average loss involving fraudulent new accounts was more than seven times larger than consumers' average loss caused by misuse of existing accounts.[xiii] For businesses and financial institutions, the average loss from fraud involving new accounts was $10,200, nearly five times the average loss of $2,100 on existing accounts. Frauds involving new accounts also took four times as long for victims to correct.[xiv] It is clear from the FTC 2003 Survey that restricting the identity thieves' ability to open new lines of credit is essential to reducing economic loss from identity theft.

Other studies supported the conclusions of the FTC 2003 Survey. Research in 2003 by Gartner Inc.[xv] and Harris Interactive[xvi] estimated that identity theft affected 7 million U.S. adults per year. Harris estimated 33.4 million total victims in the U.S.[xvii] Aberdeen Group research estimated U.S. losses at $73.8 billion by the end of 2003, with worldwide losses at $221 billion.[xviii] A study by Javelin Strategy and Research conducted in 2004 estimated that 9.3 million Americans became victims of identity theft in the 12 months preceding the survey.[xix] The Javelin survey reported a mean cost per victim of $5,686 and a total loss from identity theft of $52.6 billion.[xx]

The Identity Theft Resource Center ("ITRC") study in the summer 2003 reported that in 73 percent of identity theft cases, the stolen identity information was used to open new accounts.[xxi] The ITRC study found the victims spent an average of 600 hours attempting to resolve their claims[xxii] and that 41 percent of victims were still attempting to resolve their problems more than two years after the fact.[xxiii]

One difficulty in accurately quantifying the frequency and cost of identity theft is that most identity crimes go unreported. The FTC 2007 Survey found that only 26 percent reported their loss to police.[xxiv] The FTC's Consumer Sentinel reported that 65 percent of identity theft victims do not contact police, and a further 6 percent of victims never have a report taken.[xxv] The Consumer Sentinel Network law enforcement database logged only 313,982 identity theft complaints in 2008 even though FTC 2007 Survey estimate of the number of victims was 8.3 million adults.[xxvi]

In the wake of this alarming data, consumers, merchants, and lenders attempted to reduce identity theft by modifying their credit practices. However, identity theft rings also have increased in their size, scale and sophistication. Whether identity theft losses have increased or decreased in recent years is open to dispute.[xxvii] The FTC 2007 Survey estimated 8.3 million victims in 2006, which is 17% lower than the estimate of 9.9 million victims reported in the FTC 2003 Survey.[xxviii] The FTC 2007 Survey estimated that economic losses had dropped to $15.6 billion from $52.6 billion in the FTC 2003 Survey. However the survey methodology had changed, so it could not be determined whether significant reductions in economic loss had actually occurred.[xxix]

Javelin Strategy and Research estimated that in 2006 there were 8.4 million identity theft victims who suffered losses of $49.3 billion.[xxx] However, Javelin reported an increase to nearly 10 million victims during 2008.[xxxi] Further, a 2007 study by Gartner estimated that the number of victims actually had grown to 15 million, an increase of 50 percent over the FTC 2003 Survey.[xxxii] Gartner also found that the average loss in new account fraud cases had more than doubled to $5,962.[xxxiii]

Whether identity theft losses have increased or decreased since 2003 may be debated, it cannot be disputed that they remain at intolerable levels in 2009. In the late 1990s, when identity theft was estimated to have 100,000 victims per year and annual losses were $2 billion dollars, one commentator concluded, "Identity theft is out of control".[xxxiv] Today

there are approximately 100 times more victims annually and economic losses have increased approximately 25 times since the late 1990s. The recent studies indicate that identity theft remains as "out of control" as ever and that restricting new account fraud is critical to preventing economic loss from identity fraud.

II. Legislation Directed at Information Theft Prevention Has Been Ineffective.

The rapid rise in identity theft claims and the mounting losses have received substantial legislative attention. Statutes criminalizing identity theft activities has been enacted at both the federal and state level. The Identity Theft and Assumption Deterrence Act of 1998, (ITADA) made it a federal crime when an identity thief:

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

ITADA broadly defined "means of identification" to include an expansive range of personal identifying information.[xxxvi] ITADA also outlaws production, transfer and possession of false identification documents or authentication features.[xxxvii]

ITADA consolidated aspects of identity theft treated in other statutes and imposed a uniform and comprehensive approach to criminal penalties.[xxxviii] It also made identity theft a crime against the individual person whose identity was stolen, allowing the victim to seek restitution.[xxxix] Under previous law, identity theft was a crime only against the institution that suffered the loss and victims had no distinct legal standing.[xl] ITADA also directed the FTC to take an active role in consumer education, victim assistance and creating a centralized complaint and record keeping database to track identity theft.[xli]

States also took up the challenge of responding to identity theft. Arizona was the first state to enact an identity theft statute in 1996.[xlii] By 2002, forty-four states had criminalized identity theft.[xliii] Today, all fifty states have enacted some form of criminal statute outlawing identity theft,[xliv] and all states classify some form of identity theft as a felony, except Maine.[xlv]

Congress has continued to act. The Identity Theft Penalty Enhancement Act,[xlvi] created the crime of aggravated identity theft, and increased penalties for identity theft when used in connection with other specified felonies. The Internet False Identification Prevention Act made distribution of counterfeit identity information over the Internet a criminal offense. [xlvii] The Secure Authorization Feature and Identification Defense Act (SAFE ID Act) made it a federal crime to traffic in false identification features for use in document or false identification documents or means of identification.[xlviii]

In addition to criminal statutes, Congress has enacted new privacy regulations to better safeguard consumers' personal information. The Health Insurance Portability and Accountability Act (HIPAA)[xlix] imposed new privacy regulations on the health care industry. The Gramm-Leach-Bliley Act (GLBA)[l] created new privacy requirements for the financial services industry. The Fair and Accurate Credit Transactions Act of 2003, (the "FACT Act")[li] amended the Fair Credit Reporting Act[lii] to extensively regulate the manner in which credit reporting agencies ("CRAs") and other financial institutions handle consumer credit information. The FACT Act allows consumers to place a fraud alert in their credit files held by CRAs if they believe they have been a victim of identity theft . The fraud alert notifies potential creditors that they must use reasonable procedures to verify the identity of the person requesting credit.[liii] The FACT Act also allows consumer to obtain free credit reports, and identity theft victims have the right to request and obtain information regarding transactions on their accounts, and to block information in their credit reports arising from identity theft.[liv] In addition, President Bush created the President's Task Force on Identity Theft to draft a strategic plan for a coordinated governmental approach for combating identity theft.[lv]

These legislative efforts are clearly steps in the right direction toward more secure and private handling of personal identifying information. However, legislative solutions that have focused on criminalizing misuse of personal identifiable information have had profoundly little effect[lvi] for several reasons. First, while handling private information more

carefully in the future is clearly important, these laws do not reduce the vast amounts of information already in the hands of identity thieves. Second, criminal sanctions lack effectiveness because only a fraction of identity theft crimes are reported[lvii] and investigated. Gartner has estimated that only one in 700 claims lead to an arrest.[lviii] Lacking sufficient resources, the Department of Justice had charged only 658 defendants with aggravated identity theft in 2005 and 2006 combined.[lix] Third, identity theft crimes are difficult and expensive to investigate. The U.S. General Accounting Office (GAO) reported estimates of the cost of investigating white collar crimes, including identity theft cases, that ranged between $15,000 and $20,000 dollars per case.[lx] The GAO estimated average prosecution costs for white collar crime cases at an additional $11,400 per case.[lxi] Criminal investigation resources are usually directed towards violent crimes, drug offenses and other serious crime.

Unfortunately, the volume of resources committed to identity theft investigations and prosecutions is dwarfed both by the number of victims and the economic losses. Despite the new laws, identity thieves will continue to stealing the personally identifiable information of their victims with impunity – i.e. operating the "front end" of their schemes – for two reasons. First, because criminal arrests, prosecutions and sanctions for information theft do not operate as an effective deterrent. Second, past and current vulnerabilities continue provide ample opportunities to steal personal identifying information.

III. Insecure Records, Data Storage and Identification Systems Make Information Theft Prevention Impossible.

The Internet and other computing and information technologies have brought enormous economic and social benefits, yet these technologies also have created new dangers to privacy that have outpaced existing legal protection. The explosive development of computing power, information technologies and network connectivity over the past two decades has dramatically changed the landscape for securing the privacy of personal information used for identity theft. One commentator described the situation as follows:

> These three developments all concern the changes wrought by digital technology on the ability to manipulate information. First, the amount of digital information generated is breathtaking. Every interaction with the Internet, every credit card transaction, every bank withdrawal, every magazine subscription is recorded digitally and linked to specific individuals. In the analog world, these transactions were either not recorded at all or recorded on paper in a single location. Second, all this information, once it is collected in networked databases, can be sent instantly and cheaply around the globe. In this newly commoditized information market, buyers anywhere can collate and manipulate the data for marketing, profiling, or more sinister purposes. Third, individuals have little ability to control this collection or manipulation. Not only does much of this happen far from the reach of regulators, but most people are not even aware what information has been collected or how it is being used.[lxii] {Citations omitted}

The accumulation and distribution of this flood of data exposes individuals to a variety of systemic vulnerabilities enabling widespread identity information theft that is impossible to prevent.

A. Vulnerabilities From Insecure Data Collection, Aggregation, Storage and Distribution.

Today, massive amounts of personally identifiable information are collected, aggregated, stored and maintained by thousands of public and private entities with inadequate security protection. Government agencies, businesses, educational institutions, hospitals and other social institutions store large volumes of electronic data that are subject to potential theft, pose very serious threats to personal privacy. Identity thieves can easily obtain, aggregate, sell and exploit this sensitive information using ultra-fast computers, massive amounts of inexpensive data storage, and the ability to transfer information instantly and remotely via the Internet.

Privacy expert Daniel Solove has noted the huge volume of personal information collected and maintained by various governmental entities regarding every aspect of personal life – financial, medical, professional, criminal, etc. Prior to the late 1990s, most of these records were accessible to the public or available for purchase.[lxiii] Today, merchants, banks, credit card companies, health care facilities, retirement plans and hundreds of other entities

affecting consumers daily routinely store and maintain massive amounts of personal data about their customers, clients and patients -- the very same data identity thieves exploit.

Before the digital revolution, records were kept on paper records were protected by their "practical obscurity" -- it was expensive and impractical to keep and maintain such records, and immensely difficult to attempt to assemble discrete items of personal information maintained by a variety of independent record keepers.[lxiv] This is no longer the case. Solove reported 165 data aggregation companies were selling public record information over the Internet.[lxv] The largest of these are Choice Point, Acxiom and LexisNexis. ChoicePoint, which merged with LexisNexis in 2008, claimed to have access to more than 17 billion public records, including 90 million criminal records, 170 million annual vehicle registrations and 240 million consumer credit and demographic histories.[lxvi] In addition, there is a substantial gray market for personal information.[lxvii]

Business enterprises gather extensive data about their customers that is used to build in-depth profiles that are a critical asset to modern businesses.[lxviii] Data analytics is a $25 billion industry with hundreds of data mining companies.[lxix] Internet advertising companies track consumer online activities to support targeted advertising and behavioral marketing. All of this personal information, whether from public records or from private commercial or personal transactions, is susceptible to theft by criminal organizations operating multi-million dollar identity theft schemes that become more sophisticated each year.[lxx]

These digital records are notoriously and dangerously insecure. The Privacy Rights Clearinghouse maintains a chronology of hundreds of reported data breaches since 2005. By April 2009, more than 245 million records had been breached.[lxxi] One information security firm estimates that 285 million records were compromised in 2008 alone.[lxxii] No segment of government, business, education or industry is immune from such troubles. Data has been stolen from government agencies, credit card companies, data aggregators, universities, hospitals, health plans, banks, insurance companies, media giants, and securities brokerages. In some cases the data was mistakenly sold to criminals, but theft of data occurs in a variety of means including attacks by hackers, use of keylogging software, theft of computers or backup tapes, loss of backup tapes in transit and employee malfeasance.[lxxiii]

Massive amounts of personally identifiable information about millions of Americans has already been stolen and cannot be recovered. This information is extensively available to identity thieves and will remain so for the foreseeable future. The data not already stolen is vulnerable to future theft as discussed further below. New privacy laws have not markedly interrupted the flow of personal data to identity thieves. In the past, privacy of personal data was protected by its "practical obscurity". Today so many parties use, share and rely on large volumes of personal identifiable information as a necessary part of modern living that restricting data flows to criminal elements is a "practical impossibility". As one commentator put it, "statutes regulating use of information are already obsolete - the technology and types of harms change too fast"[lxxiv].

B. Vulnerabilities From Insecure Identification Document Systems

The infrastructure of human identification in the United States is fundamentally insecure. Prof. LoPucki has properly characterized the explosion of identity theft as a problem of human identification rather than theft.[lxxv] Solove attributes identity theft to an architecture of vulnerability that is exploited by identity thieves to impersonate victims.[lxxvi] Our flawed identification systems make it impossible for lenders and merchants to distinguish between legitimate consumers and impostors who possess certain personal information used for identity theft.[lxxvii]

The critical document in the U.S. identification system is the Social Security Number ("SSN"). The SSN functions as a *de facto* personal identifier, even though such a purpose was expressly disclaimed on the face of the cards.[lxxviii] Organizations of many types use a person's name together with the SSN to function as an "extended name" that can distinguish one person from all others, particularly from persons with same or similar names.[lxxix] U.S. consumers are heavily dependent upon the SSN because it is a practical necessity for credit, employment, health care and countless other forms of daily functioning in modern society.[lxxx] The SSN is so widely held by thousands of entities, that it is a "financial time bomb".[lxxxi] -- It is the magic key that opens the door to personal records and financial accounts for identity thieves.[lxxxii]

Unfortunately the SSN lacks the necessary protections that would protect it against counterfeiting.[lxxxiii] The SSN card lacks a photo or a hologram so the card is easily reproduced using modern digital imaging and printing software. Further, until the identity theft surge, legitimate SSN cards were easily obtained from the Social Security Administration by fraudulent means.[lxxxiv] Multiple replacement cards for legitimate SSNs were readily obtained because they issued with less rigorous documentation based other publicly available documents such as birth certificates or counterfeit documents.[lxxxv] Identity thieves also obtain new SSN cards in the names of newborn children using birth records.[lxxxvi]

The SSN is a "token-based" form of identity, i.e. the person in possession of the token is presumed to be the person identified in token.[lxxxvii] Passports, driver's licenses and birth certificates are other examples of identity tokens. Tokens that do not contain photographs or physical descriptions, such as birth certificates and social security numbers, are especially insecure because it is not possible to compare the physical characteristics displayed on the token with the characteristics of the person presenting the token.[lxxxviii] For years, counterfeit and fraudulently issued birth certificates, and drivers' licenses were relatively easy to obtain. Thieves will use a single counterfeit, stolen identifier or fraudulently issued identity document as a "breeder document" to fraudulently obtain other officially issued identity documents, such as the SSN.[lxxxix]

Congress has acted to make issuance of Social Security Cards more secure.[xc] Replacement cards were restricted to no more than 3 per year and improved standards for

verifying documents used for original or replacement cards.[xci] The REAL ID Act established new authentication and security standards for state issued drivers' licenses or state identification cards that often are used to obtain fraudulent Social Security cards.[xcii] While these are necessary improvements, the Social Security card still lacks enhancements such as machine readability, fingerprints, or biometric information that would seriously deter identity thieves and counterfeiters.[xciii]

The weaknesses in identification systems allow thieves to use false identity documents and stolen personal identity information to establish new credible identities posing as their victims. These identities are used fraudulently to obtain employment, credit cards, bank accounts, leases, mortgages and other forms of credit.[xciv] More frightening is the fact that false identity documents enable other more serious crimes such as terrorism, money laundering, drug trafficking, alien smuggling, and weapons smuggling.[xcv] Faulty identification authentication also imperils border security, and permits unauthorized persons to enter airports, military installations, federal buildings and other secure facilities.[xcvi]

Collectively, insecure records and insecure identification systems make information theft prevention impossible. Credit granting processes that rely solely on identity information obtained from this insecure environment are at substantial risk for new account fraud. Fortunately, the credit industry will able to overcome these weaknesses if it is provided with the proper incentives to do so.

IV. Economic Loss From Information Theft Is Preventable.

Every day banks, credit card companies, financial institutions and merchant make decisions about whether to lend money, extend credit or sell goods on credit. Their decisions will be based on an assessment of the prospective borrowers' creditworthiness based on credit history information from a credit reporting agency (CRA). Experian, Equifax and TranUnion are the three largest CRAs and each maintains files on over 200 million Americans.[xcvii] Relying on credit reports from the CRAs, lenders and merchants often act carelessly to extend credit to imposters who have stolen the identity information of their victims, causing billions of dollars in economic loss. Unlike the insecurity of records systems and identity systems, this vulnerability is self-created by CRAs, lenders and merchants, and is substantially preventable. While lenders, merchants and CRAs control the *means* to prevent these losses, they have no market or legal *incentives* to do so because the risks are borne by others.

A. Insecure Credit Granting Processes Enable Economic Loss.

Like countless other record keepers, the CRA uses the SSN as an extended name and unique identifier to identify the relevant credit account. When the CRA receives an order for a credit report, it must determine whether the credit applicant is truly the person identified in its credit records and not an identity thief. To do so, it uses a knowledge-based identification method. This method presumes that if the credit applicant is able to supply

unique knowledge that only the correct person would know, the applicant must be the correct person named in the credit report.[xcviii] The knowledge requested of the credit applicant operates as a *password* to access the credit file and verify the identity of the applicant. After matching certain knowledge fields, the CRA releases the credit report and the merchant or lender reviews the report to decide whether to extend credit.

A knowledge-based password with be most secure if the knowledge is not widely known or attainable, can easily be changed by the account holder, and if numerous unique knowledge fields must match. Unfortunately, the knowledge fields used as passwords by CRAs to match credit applicants to credit files are extremely insecure. The knowledge fields are widely known and readily attainable rather than secret. They are permanent rather than changeable. Frequently those in the credit industry do not demand that the matching knowledge fields be either numerous or uniquely known. Instead, they rely on the very fields most easily stolen and traded by identity thieves.

The fields commonly used for the matching an applicant to a credit file are the SSN, name, address, and date of birth.[xcix] In some cases perhaps a telephone number or mother's maiden name may be used as well.[c] Each these knowledge fields are widely available, are easily obtained by thousands of persons, and probably already in the possession of identity thieves due to the security issues mentioned above[ci]. They either do not change at all (SSN, birthdate, mother's maiden name) or change infrequently (name, address, telephone number). They are not uniquely known because nearly anyone can get access to them

through online directories. It certainly is not difficult for resourceful identity thieves to obtain them, by legal or illegal means, and match them using data mining techniques. These knowledge fields may have usefulness if they function as more precise identifiers or extended names for common names such as "John Smith".[cii] But these knowledge fields are utterly ill-suited as passwords used to allow access to a credit report and to authenticate the identity of the credit applicant. The current system is creates unnecessary risk because both the extended name identifiers and passwords commonly used to obtain credit consist of the same readily available information.

Once the CRA provides easy access to the credit report, it generally is up to the prospective lender or merchant to carefully verify whether the information in the report matches the information provided by the applicant and make the decision to extend credit. Merchants and lenders have control over the quality and amount of identity information they require and the care used in their identity verification procedures. Unfortunately, credit reports frequently contain errors[ciii] or inconsistencies that complicate the ability to identify the applicant. Credit reports often may contain inaccurate information submitted by past creditors.[civ] Many identity thieves would be thwarted if CRAs and creditors were simply more careful in their reporting and lending practices.[cv] Precise matching of extended name fields can be a challenge because more than 38 million Americans move to a new residence each year. [cvi] Millions more become married, divorced or use second addresses such as vacation homes.[cvii] Lenders and merchants may willingly create risks by overlooking discrepancies rather than losing a sale or lending transaction.

Given the enormity of identity theft losses, the credit industry's failure to rigorously enhance the security of their lending practices seems wholly irrational. In fact, however, CRAs, lenders, and merchants are responding appropriately to the incentives and disincentives in the market. The credit reporting industry, the consumer lending industry and merchants have strong incentives to make large volumes of credit available as quickly, easily and inexpensively as possible. CRAs have control over the accuracy of their information and could restrict release of credit reports only upon careful matching of several knowledge fields that are not readily available from online records. In the highly competitive credit industry, however, the ability to rapidly open new credit account "tradelines" is critical.[cviii] The CRA uses an automatic and highly mechanical process to match the information provided by the applicant (principally just the name and SSN) to an existing credit file within seconds.[cix] The ability to produce the report instantly is an important feature of the CRAs' service. CRAs must provide the fastest possible credit verification service or lose their merchants and lender clients to faster providers. The CRAs have no incentive to create rigorous identity authentication standards that remove unnecessary risks because those risks are substantially borne by others.

Similarly, lenders who take the time to pursue extensive credit verification processes to reconcile credit report discrepancies will incur greater costs and lose credit volume to faster, more convenient lenders. For merchants the benefits of facilitating more sales by providing instant credit may outweigh the risks costs of identity theft. Prof. Sovern points

out that merchants and lenders with tight credit procedures may offend customers who will take their business to less inquisitive competitors.[cx] The economic losses to merchants arising from identity theft are estimated to be approximately one percent of total retail sales.[cxi] Thus, if the name and SSN are somewhat close to matching, lenders and merchants have significant market incentives to take risks by willingly disregarding credit report discrepancies rather than refuse a new sales or lending opportunity.

Collectively these practices create a lending environment of unnecessary risk that is fully avoidable. The situation is much like the sub-prime lending crisis, in which the market participants understood that they were introducing substantial risks into the financial system, but continued to so. Borrowers, loan brokers, banks and secondary market investors all had substantial and immediate financial incentives to continue creating excessive risk. They relied on a mistaken belief that the risks could be shifted to other parties and would not affect the financial system as a whole. Credit industry participants also have continued to create unnecessary risk because of its immediate benefits. But the excessive risks to identity theft victims and to society at large have become too great to tolerate any longer.

B. Creating Incentives For Secure Credit Processes Will Prevent Economic Loss From Information Theft.

Economic losses from fraudulent new accounts will remain rampant because those who control and profit from the instant credit practices are not held accountable for the full

range of the losses caused. Prof. Sovern proposes that loss allocation principles be applied to the costs of identity theft. Under such principles, the loss should be reallocated to the parties who are best able to avoid the loss at the least cost.[cxii] The present system perversely places great loss on the party with the least control - consumers.

CRAs have control over the collection, organization and dissemination of credit information and thus could offer more accurate identification and robust authentication. For example, CRAs have the ability to establish and implement systems that would rely on more sophisticated passwords. These could require multiple fields of information that are unique to each consumer, not widely known or discoverable, and are controlled and changeable by individual consumers. These systems to reduce risk do not exist because CRAs have no incentive to incur the costs necessary to create them.

Credit reporting agencies bear few, if any, costs of identity theft despite having the greatest ability to prevent loss on new accounts. This is the inverse of traditional loss allocation rules. The FCRA substantially shields CRAs from liability for the content of their reports except in limited circumstances. There are disincentives for individual CRAs to take meaningful steps to prevent losses. First, developing robust authentication procedures to reduce risk will incur costs without providing benefits. Second, unless all CRAs were required to develop similar procedures the increased costs could make prices of an individual CRA less competitive. More rigorous practices also would slow credit approval times and the CRA will lose clients to less rigorous providers. Third, and most perversely of all, CRAs

are able profit by selling credit monitoring services that allow consumers to monitor their credit files for suspicious activity.[cxiii] The CRAs both create the risk, and then profit from insuring the risk. Note, however, that such services merely allow consumers to discover economic losses from information theft more quickly rather than prevent economic loss before it occurs.

Merchants and lenders initially bear the bulk of the approximately $50 billion in annual economic losses from identity theft.[cxiv] Under loss allocation rules, this is appropriate because merchants and lenders have the ability to prevent loss by using greater caution. As noted above, if the profits of increased sales enabled by instant credit exceed the economic losses of identity theft, merchants have no incentive to tighten their credit practices. Further, assuming that the losses are either widely and/or evenly distributed among competitors, all merchants will be able to pass along the losses to consumers through higher prices without loss of price competitiveness. If so, then consumers ultimately pay substantially all of the $50 billion of economic loss of identity theft through higher prices. On the other hand, selected lenders and merchants acting alone to reduce risky practices will incur additional costs and potentially lose customers. Under such a cost-benefit analysis, it is rational behavior for merchants and lenders to continue to create risk and to tolerate identity theft losses.[cxv]

While this behavior is rational on purely economic grounds, it ignores the huge external costs borne by consumers and society. Consumers' out of pocket losses from lax

credit authentication practices greatly outweigh the benefits they perceive from the instant credit environment. Consumers directly suffer more than $5 billion dollars of identity theft losses annually.[cxvi] They also may suffer indirectly from higher prices passed on by merchants, the costs to remedy the harms of identity theft, and through the cost of credit monitoring services.

Nor do lenders, merchants or the credit industry bear the huge external non-economics costs to consumers. The FTC 2007 Survey, the FTC 2003 Survey, the ITRC Study, and Prof. Sovern all describe how consumers grievously suffer from the damage to their credit ratings, the time spent to correct erroneous information, to defend against claims for payment and even crimes committed in their names.[cxvii] While consumers have strong incentives to prevent these economic and personal losses, they have little power to do so. They have little control over how their information is collected and disseminated by CRAs, or how it is accessed and used by credit grantors, or the means used to verify the identity of imposters attempting to borrow in their name. The FACT Act has provided consumers only with some rights to review and correct their credit information, to place fraud alerts on their credit files and assistance in recovering from the harms inflicted by identity theft that has already occurred. [cxviii]

In addition, the substantial costs to society are not borne by the credit industry participants that could prevent them. Identity theft costs society several million dollars to investigate and prosecute. The billions of dollars stolen annually through identity fraud are

diverted to support organized crime, terrorism and other criminal enterprises causing other societal harm. The cumulative losses to consumers, business and society -- losses that are largely preventable -- are too great to justify further inaction to correct the insecure and vulnerable credit authentication system.

New legislation is necessary to make the credit system more secure and to prevent economic loss from identity theft. The most effective legislative strategy will be a two-pronged approach. First, create incentives for more secure credit authentication by imposing liability for identity theft on the parties in the credit system. Second, grant consumers substantial control over the security measures required before their credit information can be released by CRAs or used to establish new accounts by merchants and lenders.

Applying loss allocation principles, legislation should impose liability on CRAs for losses caused by releases of a credit report if they breach a duty of care to properly authenticate the identity of the credit applicant. Facing billions of dollars in annual liability, CRAs would have a strong incentive to create a cost effective authentication system in which the SSN, date of birth and other knowledge fields would serve only as extended names, not passwords. CRAs would create systems to establish robust passwords for each credit filethat are known only to the credit applicant, that require matching of multiple fields, and that require the fields to be changed from time to time. These could be similar to the security questions now used by banks to authenticate access to online accounts.

Similarly, merchants and lenders should be liable if they fail to meet their duty of care to verify that the identity of the credit applicant is consistent with the credit report released by the CRA. Consumers should not be liable for any economic loss arising from new account fraud absent their own carelessness.[cxix] Consumers should be able to recover damages for the costs of repairing damage to their credit files and credit rating that result. Since such legislation would impose liability on all CRAs, lenders and merchants, each competitor would have a strong market incentive to develop the fastest and most cost effective methods for credit authentication that are sufficient to avoid liability, while still maintaining the best features of instant credit access desired by consumers.

Prof. Sovern suggests that a scheme of statutory liquidated damages and attorney fees also might be implemented that would impose sufficient costs on lenders and/or CRAs to create further incentives for robust credit authentication.[cxx] The level of damages could be set to appropriately reflect the typical non-economic harms suffered by victims and high enough to create further incentives for strong authentication. If the combination of actual damages, statutory damages and attorneys fees were greater than the costs of better credit authentication procedures, CRAs would implement robust procedures in a quick and efficient way.

An additional benefit of imposing losses upon the credit granting industries is their superior ability to identify, reduce and spread the risks of identity fraud losses broadly

among all market participants. Strengthening credit authentication systems will create initial transaction costs for the credit industry. These costs should be substantially less than the savings from preventing the billions lost to identity thieves. These costs can be recouped by imposing an additional charge on each of the one billion credit reports issued each year.[cxxi] Spreading the risk also reduces the highly disproportionate losses of the present system in which a few random unfortunate victims suffer substantial economic and non-economic losses and many others suffer none.[cxxii]

While such cost-shifting legislation is highly desirable, it will be strongly opposed by industry groups such as the Consumer Data Industry Association. The credit industry has demonstrated the political clout necessary to stifle other attempts to broaden the liability of CRAs and the credit industry. Such legislation is unlikely to be enacted until identity theft losses become so pervasive and severe that such proposals become politically feasible. In the absence of legislation creating incentives for the credit industry to take responsibility for protecting consumers, the next best alternative is to empower consumers to protect themselves.

As is further discussed below, empowering consumers with the right to freeze access to their credit records is an important first step toward preventing new account fraud and the economic loss. In the future these rights should be expanded to equip consumers with even broader powers to control the security of their credit accounts.

V. State Credit Freeze Legislation.

It is impossible to prevent identity thieves from obtaining important personal information. There simply is too much information, too easily accessed by too many parties and subject to too much vulnerability to theft and misuse. Current remedies for identity information theft are retrospective. They focus upon criminalizing past conduct, recovering money stolen and repairing damage already done to victims. In contrast state credit freeze legislation is a prophylactic remedy. When a credit freeze is in place CRAs are prohibited from releasing any credit information without the consumer's consent. The credit freeze empowers individual consumers to take action to protect themselves *before* theft occurs.

California pioneered the credit freeze in 2001 by enacting legislation taking effect on January 1, 2003.[cxxiii] Forty-eight states have enacted some form of credit freeze legislation.[cxxiv] Only Alabama, and Michigan lack credit freeze laws.[cxxv] The adoption of credit freeze laws in a majority of states led the three largest CRAs, Experian, TransUnion and Equifax, to voluntarily permit consumers in any state to place a credit freeze as of November 1, 2007.[cxxvi]

The credit freeze provides superior protection compared to the fraud alert available to consumers under the FACT Act since 2004.[cxxvii] The fraud alert notifies potential credit grantors that new credit is not to be extended without verifying the identity of the consumer identified in the credit report. However, the fraud alert does not prohibit release of the credit report.[cxxviii] The consumer is protected only if the merchant or lender receiving the

report is diligent in verifying the borrower's identity. In contrast, credit freeze legislation prohibits CRAs from releasing the credit report or any information from the report without the prior express authorization from the consumer.[cxxix]

Initially, some states enacting the credit freeze made it available only to identity theft victims. This was problematic because consumers frequently do not discover new account fraud until substantial losses have already occurred. The FTC 2003 Survey found that 24 percent of victims did not discover that new accounts had been opened in their name for more than 6 months.[cxxx] Another 33 percent of victims discovered the new accounts between 1 and 5 months later.[cxxxi] The IRTC Study found that 24% of victims did not discover the theft for more than two years.[cxxxii] The Javelin 2005 survey found that frauds involving new accounts correlated with the longest detection times and a mean loss of over $12,000.[cxxxiii]

Statutes that required consumers to be victimized before requesting a freeze thwarted consumers' ability to act to prevent theft from occurring. This requirement has not been included in most recent statutes and has been removed from older statutes.[cxxxiv] A substantial majority of the states now allow any consumer to seek a security freeze. Only Arkansas[cxxxv], Kansas[cxxxvi], Mississippi[cxxxvii] and South Dakota[cxxxviii] continue to limit the credit freeze protection to victims of identity theft. These states typically require victims to supply the credit reporting agencies with a copy of a police report, investigative report, or filed complaint along with their written request for a security freeze.[cxxxix]

California's law provided a model substantially followed other states.[cxl] State credit freeze statutes follow an "opt-in" regime. Consumers must take action to elect to place, temporarily lift or remove a freeze at any time for any reason. To implement the freeze, the consumer typically must notify the CRA in writing,[cxli] and provide "proper identification".[cxlii] To ensure full protection consumers should place a freeze request with each of the three major CRAs. The CRA typically has short time period to place the freeze,[cxliii] and must send written confirmation of the freeze shortly thereafter.[cxliv] The confirmation must contain a unique personal identification number (PIN) or password that the consumer must use to remove or temporarily lift the freeze.[cxlv] The CRA must also disclose the process for placing and temporarily lifting the freeze.[cxlvi] Many states have a required statutory notice that must be sent to consumers.[cxlvii] The CRAs may advise third parties that a freeze is in effect.[cxlviii]

The freeze remains in effect until the consumer removes it.[cxlix] The consumer may temporarily lift the freeze for a specific party or time period by providing proper identification,[cl] the unique PIN or password, and the proper information regarding the party permitted to receive the report.[cli] The freeze must be lifted promptly, and the CRAs often are authorized to develop phone, fax or electronic procedures.[clii] If the freeze is not lifted, the third party requesting the report may treat a credit application as incomplete.[cliii] The consumer can remove the freeze by providing proper identification and the unique PIN.[cliv] The CRA may remove a freeze that was frozen due to a material misrepresentation of fact by

the consumer, but must provide written notice to the consumer before removing the freeze.[clv]

CRAs may charge a fee for placing, temporarily lifting and removing a fee. Many of the state statutes establish maximum charges for each service.[clvi] The early freeze statutes typically set maximum fees in a range between $10 and $20.[clvii] Victims of identity theft submitting a police report or investigative report usually are not charged a fee to place the freeze.[clviii]

Typical state statutes permit CRAs to issue credit reports to certain parties even while the security freeze is in effect. First, if the consumer has existing financial obligations, accounts, demand deposit accounts or negotiable instruments, a credit report can be issued the creditor that is owed the debt, and their agents and affiliates.[clix] The report may be used only for the purpose of collecting the debt or reviewing the account, which includes account maintenance, monitoring, credit line increases and account upgrades and enhancements.[clx] When the consumer temporarily lifts the freeze for new credit, the CRA can release the report to affiliates and subsidiaries of the prospective credit grantor for use related to extension of credit and "other permissible use".[clxi] Second, reports can be released to government agencies, collection agencies and others acting pursuant to a court order.[clxii] Third, typical state credit freeze statutes provide exceptions that permit use of reports to support variety of uses such as child support, health care fraud, tax collection, permitted pre-

screening under the Fair Credit Reporting Act, and credit monitoring services to which the consumer has subscribed.[clxiii]

The opt-in approach of current legislation is perhaps its weakest feature. Placing a credit freeze requires consumers to take an affirmative preventative action to freeze their credit. Under the current credit system, the default position is that credit reports and information are accessed with minimal consumer control over the report's dissemination. In addition, consumers need to be aware of the freeze and must have accurate information about freeze rights. The limits of the opt-in approach are demonstrated by the limited use of freeze rights. The President's Identity Theft Task Force asked the Federal Trade Commission to review the impact and effectiveness of state credit freeze legislation.[clxiv] As of March 2008, only 125,000 consumers, a mere .07 percent of all consumers with freeze rights guaranteed by state legislation, had used the credit freeze.[clxv] The FTC conducted the review in early 2008 and received many comments regarding disincentives to using freeze rights.[clxvi]

The voluntary opt-in approach relies heavily upon freeze procedures that are convenient, fast and inexpensive. Early credit freeze legislation included features that discouraged consumers from using their freeze rights. Initial freeze procedures required use of mail or certified mail, slow processing times of 3 to 10 days and significant expense of $10 to $20 to place, lift or remove a freeze. Since a freeze request must be sent to all three major CRAs to be effective, these fees are effectively tripled in cost.[clxvii] It was incongruous that

credit could be granted instantly and at low cost by electronic means, but theft prevention measures by consumers required slow, cumbersome and expensive means.

Consumers Union and AARP each supplied the FTC with surveys regarding the barriers to consumer use of the credit freeze. The AARP study noted difficulty in placing the freeze, inability to quickly lift the freeze and cost as significant disincentives to use of the freeze.[clxviii] The Consumers Union survey noted that consumer demand for credit freezes was strong.[clxix] In fact, CRAs had begun marketing "commercially developed freeze options" ("CDFOs") featuring instant credit freezes that are bundled with credit monitoring and other for-profit services to meet this demand.[clxx] Consumers Union recommended that the affordability, accessibility and convenience of credit freeze procedures be improved by implementing a single resource for placing, lifting and removing credit freeze rather than the current duty to separately notify all three major CRAs.[clxxi] The survey also noted that consumers need consistent information about credit freeze rights, especially when CDFOs are bundled with credit monitoring and other services. Consumers Union recommended a public awareness campaign to improve consumer education about credit freeze rights.[clxxii]

States have acted to remove the disincentives to using credit freeze rights in response to continuing identity theft losses and consumer demand. As noted above, most states allow all consumers to place a freeze, not just identity theft victims. States are reducing freeze costs by lowering the maximum fees that CRAs can charge. Indiana requires CRAs to place, lift and remove freezes without charge,[clxxiii] Montana, Georgia and Nebraska require a

maximum charge of $3.[clxxiv] States also are increasing the convenience of the credit freeze by requiring CRAs to temporarily lift a freeze within in 15 minutes.[clxxv]

Given the very low awareness of the credit freeze,[clxxvi] and the tiny percentage taking advantage of their freeze rights,[clxxvii] one might conclude that the credit freeze statutes are had very little impact. However, these statutes have established very important principles that lay the groundwork for greater consumer control over credit than ever before. First, for the first time all consumers have the ability to control access to their credit accounts. CRAs now have a duty to create a consumer-managed account for each credit file upon request. Since California's law took effect in 2003, CRAs have built the technical infrastructure and systems to handle individual consumer management of credit accounts. Second, these consumers are now identified by a unique PIN number that functions as the password to control their credit information. This PIN is not currently in possession of identity thieves nor can it be obtained through data aggregation and mining techniques from other public information. Third, these statutes have demonstrated the ability of states to take the lead in developing innovative solutions to the problems of identity theft rather than awaiting delayed and weak federal solutions.

With this important foundation in place, states should continue to incrementally expand consumer power over their credit accounts. To overcome the weaknesses of an opt-in system, states should do more than merely remove disincentives to use of the credit freeze. Instead states should give consumers the tools to manage access to their credit

accounts and the incentives to do so carefully. One possibility is to require CRAs to allow each consumer to create a PIN-Protected Consumer Managed Report (herein referred to as a "PPCMR") with the CRAs even without immediately placing a freeze, i.e. while permitting open access to the credit account. Consumers could then exercise their freeze rights by placing or lifting a freeze from time to time as needed.

States also should act to create attractive incentives for consumers to create a PPCMR. For example, states could make some discretionary state services available only to those with a PPCMR. For example, the convenience of paying state fees online, reserving a camping spot in a state park online, or receiving electronic payments from the state could be available made only to those with a PPCMR. Private financial entities such as banks also could create incentives to establish a PPCMR. Soon establishing a PPCMR would become a commonplace and ordinary feature of modern financial life, like having an ATM card, direct deposit of wages, or having repeating payments automatically deducted from a bank account.

The next step would be to use the PPCMR to offer enhanced security features created and managed by consumers without cost. The credit freeze has only two positions - frozen and thawed. Currently, without a freeze in place, credit is always thawed and access to the credit account relies on pitifully weak security - matching of extended name fields such as the SSN, date of birth and address. By placing a freeze, the consumer uses the unique PIN as an additional security password in addition to the extended fields. Once a PPCMR exists, consumers could customize the degree of security, in addition to the PIN,

that they find suitable. They could by specify the number and kinds of knowledge fields required to function as sufficient passwords to release the credit information.[clxxviii]

After creating a PPCMR, cautious consumers could, for example, require that a large number of matching knowledge fields, in addition to their PIN, must be submitted to function as a password. The consumers should choose unique knowledge fields not available to identity thieves, such as: names of pets, childhood nicknames, youngest sibling's birthday, etc.[clxxix] They could also require photo ID of a particular type as an additional safeguard, such as a passport, employer ID badge, etc. Cautious consumers could change the questions frequently. Less cautious consumers could require only one knowledge field in addition to the PIN from the CRA. In this sense, the credit account is constantly "frozen" by the multiple passwords, but available to be thawed instantly by the correct owner of the accounts who possesses the unique knowledge to match all of the chosen passwords.

To create incentives for strong security, legislation could limit liability for new account fraud based on the degree of security consumers maintain on their PPCMR. For example, if a consumer meets robust security standards - $50 maximum liability, similar to credit card accounts. If the consumer establishes only moderate security - $1000 maximum liability; if the consumer chooses weak security or an open credit account - $5,000 maximum liability. Incentives also could be created for the CRAs. Once a PPCMR were created, the CRAs liability could be limited only to those instances in which they release credit information in violation of the consumer's security instructions.

Some commentators have suggested that access to credit accounts should be restricted at all times unless a consumer chooses to authorize a release. Chris Jay Hoofnagle argued for this "opt-out" approach.[clxxx] The significant advantage of Hoofnagle's proposal is that it forces consumers to make conscious decisions about access to their credit report information. Consumers will be forced to establish a direct relationship with CRAs by creating an PIN identified account allowing management their credit information. The significant disadvantage is that a sudden migration to frozen credit will cause significant disruption for CRAs and consumers. CRAs will face substantial costs from enrolling the 99% of consumers not currently using their freeze rights. In addition, thousands of consumers will not prepare properly for the shift and will suddenly be unable to access their credit. The situation would be likely be similar the conversion from analog to digital television. Despite a long phase-in period and a major public awareness campaign, the conversion still had to be delayed by Congressional action.[clxxxi]

The opt-in regime of the current freeze legislation, coupled with improved incentives for consumers, lenders and CRAs, will provide for a more orderly transition toward a system of greater consumer control. As more consumers establish PPCMR's costs shift to the CRAs. The major costs will arise from properly identifying the consumers to establish the unique PIN and establish a PPCMR. After this initial expense, costs to maintain the accounts should be low. Even though the CRAs have nearly 200 million customers, the security passwords involve only small amounts of data. By comparison, FaceBook recently

topped 200 million subscribers.[clxxxii] Yet FaceBook is able to manage users that post large volumes of high capacity files such as video and photos. Further, the costs that arise can be limited and spread. As Prof. Sovern points out, the CRAs are in best position to efficiently reach risk neutrality, and they can spread costs to borrowers and lenders through fees charged for their services.[clxxxiii]

Some have suggested that a federal credit freeze law would be preferable to state laws because it could provide uniform procedures.[clxxxiv] Two bills were introduced in Congress in 2007 and both were referred to committee without further action.[clxxxv] While Congress has delayed, the states pioneered the freeze law and have continuously improved them. States have proven themselves as successful innovators in response to identity theft concerns. Consumer organizations have opposed creation of a federal credit freeze law for two reasons. First, a federal law that preempts state law would prevent state legislatures from continuing to innovate to protect consumer from identity fraud. Second, federal laws often are weaker than the state laws that respond quickly and strongly to consumer concerns.[clxxxvi]

CONCLUSION

Laws aimed at preventing information theft have not reduced either the incidence or cost of identify fraud. Strong laws are needed to prevent the economic losses from identity

theft. Current identity authentication systems are vulnerable and processes for granting credit create unnecessary risks that are preventable. While legislation requiring credit reporting agencies, lenders and merchants to bear the risks of their credit granting procedures, these laws are unlikely to be enacted in the immediate future. However, state laws permitting consumers to place a freeze on their credit reports are an important first step in granting consumers control over access to the credit reports. States should continue to innovate to make use of the freeze convenient and inexpensive, and should create incentives for using the freeze. In addition, consumer power over access to their credit accounts should be expanded to allow them to customize the security regarding the safety of their credit information.

[i] Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1423 (2001).

[ii] Holly K. Towle, *Identity Theft: Myths, Methods, And New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 238 (2004), (citing Stephen F. Miller, *Someone Out There is Using Your Name: A Basic Primer on Federal Identity Theft Law*, FED. LAW., Jan. 11, 2003, at 11).

[iii] FEDERAL TRADE COMMISSION, *2006 Identity Theft Survey Report* 4-5 (Nov. 27, 2007), at http://www.ftc.gov/opa/2007/11/idtheft.shtm ; (last visited Oct. 18, 2008). [hereinafter, ["*FTC 2007 Survey*"].

[iv] *FTC 2007 Survey*, *supra* note 3, at 3.

[v] FEDERAL TRADE COMMISSION, *Identity Theft Survey Report* 4-5 (Sept. 2003), at http://www.ftc.gov/os/2003/09/synovatereport.pdf. (last visited, October 18, 2008), [hereinafter, "*FTC 2003 Survey*"].

[vi] Gary R. Gordon and Norman A. Willox, Jr.; Utica College Economic Crime Institute, June 2006, *The Ongoing Critical Threats Created by Identity Fraud: An Action Plan*" http://www.utica.edu/academic/institutes/ecii/publications/papers.cfm? action=submit (last visited October 18, 2008); Gary R. Gordon & Norman A. Willox, Jr., Economic Crime Institute of Utica College & LexisNexis, *Identity Fraud: A Critical National and Global Threat*, at 4 (Oct. 28, 2003) http://www.utica.edu/academic/institutes/ecii/publications/papers.cfm? action=submit (last visited October 18, 2008). [hereinafter, Gordon and Willox *2003].*

[vii] Benjamin Sutherland, *The Rise of Black Market Data*, Newsweek, December 15, 2008, *available at* http://www.newsweek.com/id/173398 (last visited April 7, 2009). *See also,* Brian Krebs, *Glut of Stolen Banking Data Trims Profits for Thieves*, WASH. POST, (April 15, 2009), available at *http://voices.washingtonpost.com/securityfix/2009/04/glut_of_stolen_banking_data_tr.html.*

[viii] *FTC 2003 Survey*, *supra* note 5, at 4-5.

[ix] CAL. CIVIL CODE §1785.11.2

[x] *See*, *Consumers Union's Guide to Security Freeze Protection*, *available at* http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited October 18, 2008).

[xi] *FTC 2003 Survey*, *supra* note 5, at 7.

[xii] *FTC 2003 Survey*, *supra* note 5, at 45-48, 7.

[xiii] *FTC 2003 Survey*, *supra* note 5, at 38-44, 7.

[xiv] *FTC 2003 Survey*, *supra* note 5, at 45-48, 7. These frauds took victims an average of 60 hours to resolve, compared with an average of 15 hours for misuse of existing accounts.

[xv] Avivah Litan, *Underreporting of Identity Theft Rewards The Thieves,* M-20-3244 Gartner Inc., (July 2003), *available at* http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp (Last visited October 18, 2008).

[xvi] Harris Interactive, *Identity Theft New Survey and Trend Report,* 5, (August 2003). Available at www.bbbonline.org/IDtheft/IDTheftSrvyAug03.pdf (Last visited October 18, 2008).

[xvii] *Id.*

[xviii] Hurley, J. and Veytsel, A., *Identity Theft: A $2 Trillion Criminal Industry in 2005*, Aberdeen Group, (2003), *available at* http://www.aberdeen.com/summary /report/perspective/05030013.asp.

[xix] Javelin Strategy and Research, *2005 Identity Fraud Survey Report,* 3 (2005), *available at* http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html. (Last visited July 19, 2005).

[xx] *Id.* at 5.

[xxi] Identity Theft Resource Center, *Identity Theft: The Aftermath*, 11 (Summer 2003), p. 27, *available at* http://www.idtheftcenter.org/artman2/publish/lib_survey/Press_Release_-_The_Aftermath_2003_Study.shtml. (last accessed October 18, 2008). [hereinafter, "*ITRC Study*"]

[xxii] *ITRC Study*, *supra* note 21, at 24.

[xxiii] *ITRC Study*, *supra* note 21, at 23.

[xxiv] *FTC 2007 Survey*, *supra* note 3, at 50-51.

[xxv] FEDERAL TRADE COMMISSION, *Consumer Sentinel Network Databook, January – December 2008*, 12, (February, 2009), http://www.ftc.gov/sentinel/reports.shtml

[xxvi] *Id.* at 5.

[xxvii] Jon Swartz and Byron Acohido, *FTC Report: Identity Theft Fell; Results Disputed, USA Today,* November 27, 2007, http://www.usatoday.com/money/industries/technology/2007-11-27-id-theft_N.htm

[xxviii] *FTC 2007 Survey*, *supra* note 3, at 3, 9; *FTC 2003 Survey*, *supra* note 5 at 7.

[xxix] *FTC 2007 Survey*, *supra* note 3, at 9.

[xxx] Javelin Stategy and Research, *2007 Identity Fraud Survey Report,* p.1 (February 2007). Available at http://www.javelinstrategy.com/idf2007.

[xxxi] Javelin Stategy and Research, *2009 Identity Fraud Survey Report,* p.1 (February 2009). Available at http://www.javelinstrategy.com/research/2.

[xxxii] Press Release, Gartner, Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003 (March 6, 2007), http://www.gartner.com/it/page.jsp?id=501912.

[xxxiii] *Id.*

[xxxiv] Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 90 (2001), [hereinafter, LoPucki, *Human Identification*].

[xxxv] Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (2008).

[xxxvi] "Means of identification" includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any: name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; unique electronic identification number, address, or routing code; or telecommunication identifying information or access device. 18 U.S.C. §1028 (d)(7). (2008).

[xxxvii] *Id.* at § §1028 (a)(1-8).

[xxxviii] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1246 (2003) [hereinafter, Solove, *Vulnerability*].

[xxxix] Holly K. Towle, *Identity Theft: Myths, Methods, And New Law,* 30 RUTGERS COMPUTER & TECH. L.J. 237, 238 (2004).

[xl] Erin M. Shoudt, *Identity Theft: Victims Cry Out for Reform*, 52 AM. U. L. REV. 339, 369 (2002).

[xli] Identity Theft and Assumption Deterrence Act of 1998, Pub. Law. No.105-318, § 5, 112 Stat. 3010 (Oct. 30, 1998).

[xlii] Jerilyn Stanley, *Identity Theft: Supporting Victims in Recovering From the Crime of the Information Age,* 32 MCGEORGE L. REV. 566, 567 (2001).

[xliii] Solove, *Vulnerability, supra* note 38, at 1247.

[xliv] *See,* National Conference of State Legislatures, *"Identity Theft Statutes and Criminal Penalties"*, http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm.

[xlv] The President's Identity Theft Task Force, *"Combating Identity Theft: A Strategic Plan",* Volume II, Part H, p. 45, (April 11, 2007). The President's Identity Theft Force was created by Exec. Order. No. 13402, 71 Fed. Reg. 27945, (May 10, 2006).

[xlvi] Identity Theft Penalty Enhancement Act, 18 U.S.C. § 1028A (2008).

[xlvii] Internet False Identification Prevention Act of 2000, 18 U.S.C. § 1001 (2008).

[xlviii] The Secure Authorization Feature and Identification Defense Act, Pub. L. No. 108-21, Title VI, § 607(a), 117 Stat. 689 (April 30, 2003), (also known as the "SAFE ID Act".)

[xlix] Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 1320d *et.seq* (2008).

[l] Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801-09 (2003). The FTC has promulgated Standards for Safeguarding Customer Information to govern other institutions outside the scope of the GLBA, such as mortgage lenders, investment advisers, tax preparers and debt collectors. 16 C.F.R. Part 314 (2002). The Securities and Exchange Commission has enacted Regulation S-P to implement GLBA privacy principles for securities brokers and dealers, investment companies and investment advisers. 17 C.F.R. Part 248 (2000).

[li] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952, (Dec. 4, 2003). The FTC and several federal agencies regulating financial institutions have issued joint rules to reduce identity theft known as the "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003". 72 Fed. Reg. 63718 (Nov. 9, 2007). These rules became effective November 1, 2008, but the FTC delayed enforcement until May 1, 2009.

[lii] Fair Credit Reporting Act, 18 U.S.C. § 1681-1681X (2008).

[liii] Fair and Accurate Credit Transactions Act of 2003, codified as 15 U.S.C. § 1681c-1. (2008)

[liv] For an extensive discussion of the provisions of the FACT Act, *see* Holly K. Towle, *Identity Theft: Myths, Methods, And New Law,* 30 RUTGERS COMPUTER & TECH. L.J. 237, 269-301 (2004).

[lv] Exec. Order. No. 13402, 71 Fed. Reg. 27945, (May 10, 2006).

[lvi] LoPucki, *Human Identification, supra* note 34 at 91.

[lvii] *FTC 2007 Survey*, *supra* note 3, at 50-51.

[lviii] Avivah Litan, *Underreporting of Identity Theft Rewards the Thieves*, Gartner, (July 7, 2003); *see,* Robert Lemos, "*Analyst: Crime Pays For Identity Thieves"*, http://news.cnet.com/2100-1009_3-5050295.html (July 21, 2003) (Oct. 18, 2008). *See, e.g.,* Bob Sullivan, "*ID Theft Victims Get Little Help"* MSNBC, (Feb. 13, 2003), *available at* http://www.msnbc.msn.com/id/3078497/. Last visited Oct. 19, 2008).

[lix] Press Release, U.S. Department of Justice, Fact Sheet: The Work of The President's Identity Theft Task Force, (Sept. 19, 2006), http://www.usdoj.gov/opa/pr/2006/September/06_ag_636.html (last visited Oct. 19, 2008). Some U.S. Attorneys have established economic loss thresholds before charging a case. *See,* The President's Identity Theft Task Force, *"Combating Identity Theft: A Strategic Plan",* Part D, p. 62, (April 11, 2007). *But see, id.* at Volume II, Part J, p. 50-54.

[lx] United States General Accounting Office, Identity Fraud: Prevalence and Cost Appear to Be Growing, GAO 02-363, 10 (March 2002).

[lxi] *Id.*

[lxii] Will Thomas DeVries, *Annual Review of Law and Technology: III. Cyber Law: A. Privacy: Protecting Privacy in the Digital Age,* 18 BERKELEY TECH. L. J. *283 , 292 (2003)*; *see also,* Jerry Berman & Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: A Work in Progress*, 23 NOVA L. REV. 549, 554-56 (1999).

[lxiii] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution,* MINN. L. REV. 1137, 1139 (2002).

[lxiv] *Id.* at 1178.

[lxv] *Id.* at 1153.

[lxvi] ChoicePoint Web site, *available at* http://www.choicepoint.com/authentication/common/pdfs/CPAS_Brochure.pdf (last visited Oct. 19, 2008).

[lxvii] Jean Sahadi, *Your Identity . . . For Sale,* CNN/Money, May 9, 2005, http://money.cnn.com/2005/05/09/pf/security_info_profit/. (last visited Oct.19, 2008)

[lxviii] Andrew J. McClurg, *A Thousand Words Are Worth A Picture: A Privacy Tort Response To Consumer Data Profiling*, 98 NW.U.L.REV. 63, 67-68 (2003).

[lxix] *Id.* at 72.

[lxx] *See*, Scott Zambo, *Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime*, 33 N.E. J. ON CRIM. & CIV. CON. 551, (2007).

[lxxi] Privacy Rights Clearinghouse, *A Chronology of Data Breaches,* http://www.privacyrights.org/ar/ChronDataBreaches.htm#9. (last visited Oct. 19, 2008).

[lxxii] Verizon Business, *2009 Data Breach Investigations Report,* available at http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

[lxxiii] Privacy Rights Clearinghouse, *A Chronology of Data Breaches,* http://www.privacyrights.org/ar/ChronDataBreaches.htm#9. (last visited April. 19, 2009).

[lxxiv] DeVries, *supra* note 62, at 307.

[lxxv] LoPucki, *Human Identification, supra* note 34, at 94.

[lxxvi] Solove*, Vulnerability, supra* note 38, *at* 1251.

[lxxvii] Lynn LoPucki, *Did Privacy Cause Identity Theft?,* 54 HASTINGS L.J. 1277,1289 (2003), [hereinafter, LoPucki, *Privacy*].

[lxxviii] *Solove, Vulnerability, supra* note 38, at 1252.

[lxxix] LoPucki, *Privacy, supra* note 77 at 1280.

[lxxx] *Solove, Vulnerability, supra* note 38, at 1253.

[lxxxi] Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies,* 2004 Stan. Tech. L. Rev. 2 (2004).

[lxxxii] *Solove, Vulnerability, supra* note 38, at 1254.

[lxxxiii] *Id.*

[lxxxiv] *See,* United States General Accounting Office, *Counterfeit Identification Raises Homeland Security Concerns*, GAO 04-133T, (Oct. 1, 2003).

[lxxxv] *See,* United States General Accounting Office, *Social Security Numbers: Securing the Integrity of the SSN*, GAO 03-941T, (Oct. 1, 2003); United States General Accounting Office, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain,* GAO 4-12, (Oct. 1, 2003);

[lxxxvi] *See,* United States General Accounting Office, *Counterfeit Identification Raises Homeland Security Concerns*, GAO 04-133T, (October 1, 2003).

[lxxxvii] *See*, Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, INFO. TECH. & PEOPLE, Dec. 1994, at 6, 8.

[lxxxviii] LoPucki, *Privacy, supra* note 77 at 1283.

[lxxxix] Gordon & Willox, *2003, supra* note 6 at 18-19.

[xc] The Social Security Number Confidentiality Act of 2000, 31 U.S.C. § 3327 (2000) prohibited display of the SSN on checks and Treasury drafts.

[xci] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 11 Stat. 3638 (Dec. 17, 2004).

[xcii] REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231 (2005).

[xciii] Social Security Administration, *Improved Agency Coordination Needed for Social Security Card Enhancement Efforts,* 23-28, Government Accounting Office, GAO-06-303 (March 2006)

[xciv] Gordon & Willox, *2003, supra* note 6 at 19.

[xcv] Gordon & Willox, *2003, supra* note 6, at 13-19.

[xcvi] Markle Foundation Task Force*, Creating A Trusted Information Network For Homeland Security*, Appendix A, (Dec. 2003).

[xcvii] This information is available on the CRAs' corporate web sites. For TransUnion, *see* http://www.transunion.com/content/page.jsp?id=/transunion/general/data/about/CapabilitiesMarkets.xml; for Experian *see* http://www.experian.com/corporate/factsheet.html; for Equifax, see,

[xcviii] *See,* LoPucki, *Human Identification, supra* note 34, at 100.

[xcix] *Id.* at 104.

[c] *Id.*

[ci] *See* Sections III.A and III. B, *supra.*

[cii] There are 2,376,206 persons in the United States with the surname "Smith". Johnson, Williams, Brown, Jones, Miller and Davis all top one million surnames. U.S. Census Bureau, "*Frequently Occuring Surnames From Census 2000"*, http://www.census.gov/genealogy/www/freqnames2k.html (Last visited Oct. 24, 2008).

[ciii] One report suggests that one quarter of credit reports contain serious errors. National Association of State *PIRGs, Mistakes Do Happen: A Look at Errors in Consumer Credit Reports,* June 2004, http://static.uspirg.org/reports/MistakesDoHappen2004.pdf (last visited, October 24, 2008); *see also,* Consumer Federation of America, *"Credit Score Accuracy and Implications for Consumers"* Dec. 17, 2002, *http://www.ncrainc.org/documents/CFA%20NCRA%20Credit%20Score%20Report.pdf* (Last visited Oct. 24, 2008); *See also,* Robert B. Avery, Raphael W. Bostic, Paul S. Calem, and Glenn B. Canner, *An Overview of Consumer Data and Credit Reporting*, Federal Reserve Bulletin, vol. 89, at 47-73 (Feb. 2003) (2003 Board staff study); Robert B. Avery, Paul S. Calem, Glenn B. Canner, and Shannon C. Mok, *Credit Report*

Accuracy and Access to Credit, Federal Reserve Bulletin, vol. 90, at 297-322 (Summer 2004) (2004 Board staff study). http://www.federalreserve.gov/pubs/bulletin/2004/summer04_credit.pdf

[civ] LoPucki, *Privacy, supra* note 77, at 1280.

[cv] *See, Identity Theft: Hearing Before the S. Comm. on Commerce,* 109th Cong. (June 16, 2005), (Statement of Gail Hillenbrand, Senior Attorney of Consumers Union and Susanna Montezemolo, Policy Analyst for Consumers Union, *Identity for Sale? Protecting Consumers from Identity Theft*), *available at* http://www.consumersunion.org, PDF file 616-privacy.pdf.

[cvi] United States Census Bureau, Geographical Mobility: 2006 to 2007, http://www.census.gov/population/www/socdemo/migrate/cps2007.html

[cvii] United States Census Bureau, 2009 Statistical Abstract, Marriages and Divorces, http://www.census.gov/compendia/statab/2009edition.html. There were 2,160,000 marriages in 2006. *Use and Misuse of Social Security Numbers: Hearing Before the Subcommittee on Social Security of the H. Comm. on Ways and Means*, 108th Cong. Serial 108-35 (July 10, 2003) (Statement of Stuart K. Pratt, Consumer Data Industry Association); http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=1440. There are approximately 1.2 million divorces annually and 6 million vacation homes or second homes.

[cviii] *See,* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors*, in Chander, Radin, Gelman, *Securing Privacy In the Internet Age,* at 212, 215 (Stanford University Press 2007). Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650162.

[cix] LoPucki, *Human Identification, supra* note 34 at 102.

[cx] Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 367 (2003).

[cxi] U.S. Census Bureau, "*Advance Monthly Sales for Retail and Food Services, December 2008",* 2, http://www.census.gov/marts/www/download/html/adv0812.html. Total retail sales in 2008 were $4.47 trillion dollars. $50 billion of annual identity theft losses is just 1.1% of retail sales. *See also,* United States General Accounting Office, *Identity Fraud: Prevalence and Cost Appear to Be Growing*, GAO 02-363, 43 (March 2002). In 2000, total fraud losses to Visa and MasterCard, were less than one-tenth of one percent of total sales, and those attributed to identity theft were only 11 percent of the total.

[cxii] Sovern, *supra* note 110, at 375.

[cxiii] For example, Experian's Credit Manager service costs. $11.95 per month.

[cxiv] FTC Survey, *supra* note 3, at 7.

[cxv] Sovern *supra* note 110 at 368.

[cxvi] FTC Survey, *supra* note 3, at 7.

[cxvii] *FTC 2007 Survey*, *supra* note 3, at 32-42; *FTC 2003 Survey*, *supra* note 5, at 38-48;

[cxviii] Holly K. Towle, *Identity Theft: Myths, Methods, And New Law,* 30 RUTGERS COMPUTER & TECH. L.J. 237, 269-301 (2004).

[cxix] For example, CRAs and merchants should not be responsible for new account fraud committed by relatives and other insiders who obtain personal identifying information from the victim.

[cxx] Sovern, *supra* note 110 at 385.

[cxxi] The Consumer Data Industry Association claims that one billion credit reports are issued each year in the United States. Consumer Data Industry Association, *available at* http://www.cdiaonline.org/about/index.cfm?unItemNumber=515//

[cxxii] Sovern, *supra* note 110*,* at 383.

[cxxiii] Stats 2001 Ch. 720, codified as CAL. CIVIL CODE §1785.11.2 to §1785.11.6. This article will cite the California statute as an example of typical credit freeze legislation that has been enacted in the various states.

[cxxiv] *See,* Consumers Union, *Consumers Union Guide to Security Freeze Protection*, available at http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (Last visited April 7, 2009.)

[cxxv] *Id.*

[cxxvi] Brian Krebs, *TransUnion to Offer Credit Freeze In All U.S. States*, WASH. POST (Sept.19, 2007), http://voices.washingtonpost.com/securityfix/2007/09/transunion_to_offers_credit_fr.html , *see also*, Press Release, *TransUnion First to Announce File Freeze Option in all 50 States, D.C.* available at http://newsroom.transunion.com/index.php?s=43&item=432. Experian and also offer credit freezes shortly thereafter.

[cxxvii] 15 U.S.C. § 1681c-1.

[cxxviii] *Id. See* discussion of the FACT Act in the text at Section II, *supra.*

[cxxix] *See*, *e.g.* CAL. CIVIL CODE §1785.11.2 (a).

[cxxx] FTC Survey, *supra* note 3 at 21.

[cxxxi] *Id.*

[cxxxii] ITRC Study, *supra* note 21 at 17.

[cxxxiii] Javelin Stategy and Research, *2005 Identity Fraud Survey Report,* 3, 8 (2005). http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html. (Last visited July 19, 2005).

[cxxxiv] Washington at first limited the credit freeze to identity theft victims. *See*, 2005 Wash. Sess. Laws Ch. 342, §1. Later this requirement was removed and all consumers can place a freeze. 2007 Wash. Sess. Laws Ch. 499, §1. Texas and Vermont are examples of other states expanding the credit freeze remedy to all consumers.

[cxxxv] ARK. CODE ANN. § 4-112-101 (2007).

[cxxxvi] KAN. STAT. ANN. § 50-723 (2006).

[cxxxvii] MISS. CODE ANN. § 74-24-201 (2007).

[cxxxviii] S.D. CODIFIED LAWS § 54-15-3 (West 2007).

[cxxxix] *See, e.g.,* S. D. CODIFIED LAWS § 54-15-3 (West 2007), KAN. STAT. ANN. § 50-723 (2006).

[cxl] This article will provide examples of the meaningful differences in the other states in the footnotes.

[cxli] *See*, *e.g.* CAL. CIVIL CODE §1785.11.2 (a).

[cxlii] This is defined in CAL. CIVIL CODE §1785.15 (c) as "information generally deemed sufficient to identify a person".

[cxliii] *See*, CAL. CIVIL CODE§1785.11.2 (b) requires three days.

[cxliv] *See*, CAL. CIVIL CODE §1785.11.2 (c) requires ten days.

[cxlv] *Id.*

[cxlvi] *See*, *e.g.* CAL. CIVIL CODE §1785.11.2 (i).

[cxlvii] *See, e.g.* ALASKA STAT. § 45.48.170 (2009); Arkansas, ARK. CODE ANN. § 4-112-111 (2008); Delaware, DEL. CODE ANN. tit 6, § 2203(c) (2009); District of Columbia, D.C.

CODE § 28-3863 (2009); Florida, FLA. STAT. § 501.005 (17) (2009); Georgia, GA. CODE ANN. § 10-1-915 (2009); Missouri, MO. REV. STAT. § 407.1382 (10) (2009); Montana, MONT. CODE ANN., § 30-14-1733 (2007), New Hampshire, N.H. REV. STAT. ANN. 359-B:23 (2009), New Jersey, N.J. STAT. ANN. § 56:11-46 (i) (West 2009), New Mexico, N.M. STAT. § 56-3A-4 (2008); New York , N.Y. GEN. BUS. LAW § 380-t (q) (Consol. 2009); North Carolina, N.C. GEN. STAT. § 75-63 (p) (2009); North Dakota, N.D. CENT. CODE, § 51-33-12 (2009); Ohio, OHIO REV. CODE ANN. 1349.52 (f) (West 2009); Oklahoma, OKLA. STAT. tit. 24 § 158 (2008); Rhode Island, R.I. GEN. LAWS § 6-48-6 (2009), Vermont, VT. STAT. ANN. tit. 9 § 2480b (c) (2009); Virginia, VA. CODE. ANN. § 2480b (P) (2009); West Virginia, W. VA. CODE § 46A-6L-103 (2009).

[cxlviii] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (a).

[cxlix] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (j), CAL. CIVIL CODE §1785.11.2 (g)(1).

[cl] *See, e.g.* CAL. CIVIL CODE §1785.15 (c).

[cli] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (d).

[clii] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (f).

[cliii] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (h).

[cliv] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (j).

[clv] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (g)(2).

[clvi] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (m).

[clvii] For information regarding current fees in each state, *see,* Consumers Union, *Consumers Union Guide to Security Freeze Protection*, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited April 7, 2009).

[clviii] *Id.*

[clix] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (l)(1).

[clx] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (l)(1).

[clxi] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (l)(2).

[clxii] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (l)(3).

[clxiii] *See, e.g.* CAL. CIVIL CODE §1785.11.2 (l)(3) - (9).

[clxiv] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan,* p. 52, (April 2007) http://www.idtheft.gov/about.html, (last visited April 8, 2009).

[clxv] Eric J. Ellman, *Public Comment of the Consumer Data Industry Association to the Federal Trade Commission Concerning Credit Report Freezes - Comment, Project No. P075420,* March 3, 2008, at p. 1. 125,000 consumers had requested freezes out of 170 million consumers in state with freeze legislation. Available at http://www.ftc.gov/os/comments/creditreportfreezes/index.shtm (Last accessed on April 8, 2009).

[clxvi] Press Release, *"FTC Staff Seeks Comments on Credit Freezes: Impact and Effectiveness",* Federal Trade Commission, January 10, 2008. http://www.ftc.gov/opa/2008/01/freeze.shtm. All public comments received by the FTC and related documents are available at http://www.ftc.gov/os/comments/creditreportfreezes/index.shtm (Last accessed on April 8, 2009).

[clxvii] Jeannine Kenney and Gail Hildebrand, Public Comment of Consumers Union, *"Credit Report Freezes - Comment Project No. P075420,"* p. 5, February 25, 2008. Available at http://www.ftc.gov/os/comments/creditreportfreezes/index.shtm (Last accessed on April 8, 2009).

[clxviii] Daniel Certner, Public Comment of AARP, "*Credit Report Freezes - Comment, Project No. P075420,*" February 25, 2008. Available at http://www.ftc.gov/os/comments/creditreportfreezes/index.shtm (Last accessed on April 8, 2009).

[clxix] Kenney and Hildebrand, *supra* note 167 at 4.

[clxx] *See, e.g.* TransUnion's TrueCredit product allows credit freezing electronically with a single click. http://www.truecredit.com. *See also,* Equifax's Credit Report Control Product, http://www.equifax.com/credit-report-lock/.

[clxxi] Kenney and Hildebrand, *supra* note 167 at 5-9.

[clxxii] Kenney and Hildebrand, *supra* note 167 at 2.

[clxxiii] IND. CODE § 24-5-24-14 (2009).

[clxxiv] Montana, MONT. CODE ANN., § 30-14-1735 (1) (2007); Georgia, GA. CODE ANN. § 10-1-914 (p) (2009); Nebraska, 2009 NEB. LAWS 177.

[clxxv] Alaska, ALASKA STAT. 45.48.130; Arizona, ARIZ. REV. STAT. ANN. § 44-1698 (G), (2008); Arkansas, ARK. CODE ANN. §4-112-104 (b); Delaware, DEL. CODE ANN. tit 6, § 2203 (b)(5) (2009); District of Columbia, D.C. CODE § 28-3862 (e) (2009); Georgia, GA. CODE ANN. § 10-1-914 (f) (2009); Idaho, IDAHO CODE ANN. § 28-52-104 (3) (2008); Indiana, IND. CODE § 24-5-24-7 (d) (2009); Maryland, MD. CODE ANN. COM. LAW. § 14-1212.1(e) (West 2008); Minnesota, MINN. STAT. § 13C.016, Subd. 4 (c) (2008); Missouri, MO. REV. STAT. § 407.1382 (7) (2009); Montana, MONT. CODE ANN., § 30-14-1729 (2)(2007); Nebraska, NEB. REV. STAT. § 8-2606 (3), (2009); New Jersey, N.J. STAT. ANN. § 56:11-46 (f) (West 2009); New Mexico, N.M. STAT. § 56-3A-3 (2008); New York, N.Y. GEN. BUS. LAW § 380-t (e)(2), (Consol. 2009); North Dakota, N.D. CENT. CODE, § 51-33-04 (3), (2009); OHIO REV. CODE ANN. 1349.52 (E), (West 2009); South Carolina, S.C. CODE ANN. §37-20-160 (G) (2008); Tennesee, TENN. CODE ANN. § 47-18-2108 (f), (2009); Virginia, VA. CODE ANN. § 59.1-444.2 (E), (2009); Washington, WASH. REV. CODE Wash. § 19.182.170 (6), (2009); West Virginia, W. VA. CODE § 46A-6L-102 (g), (2008); Wyoming, WYO. STAT. ANN., § 40-12-504 (c), (2008).

[clxxvi] Jennifer H. Sauer and Neal Walters, *Security Freeze Legislation: Awareness and Incidence of Placement Among Consumers 18+ in Seven States* (November 2008). This survey conducted by AARP was included in AARP's Public Comment to the FTC. *See,* Certner, *supra* note 168, at Appendix B.

[clxxvii] *See,* Ellman, *supra* note 165.

[clxxviii] Hoofnagle*, supra* note 108 at 215. Hoofnagle proposed the idea customer customization of credit access, but by selectively freezing and thawing the credit report from time to time.

[clxxix] For other example of good security questions *see, http://www.goodsecurityquestions.com/examples.htm*

[clxxx] Hoofnagle, *supra* note 108 at 215.

[clxxxi] *See,* DTV Delay Act, Pub. L. No.111-4, 123 Stat. 112 (2009).

[clxxxii] Barbara, Ortutay, *Fast-Growing Facebook's User Base Hits 200 Million*, Associated Press, April 8, 2009; http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040802764.html (Last accessed on April 12, 2009).

[clxxxiii] Sovern, *supra* note 110, at 382.

[clxxxiv] Kristan T. Cheng, *Identity Theft and the Case for a National Credit Report Freeze Law,* 12 N.C. BANKING INST. 239 (2008).

[clxxxv] The Consumer Identity Protection and Security Act, S. 806, 110th Cong. (2007); Identity Theft Protection Act, H.R. 3316, 110th Cong. (2007).

[clxxxvi] *See, e.g.* Can Spam Law, 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) citation. Several commentators found the federal law to be weaker than state initiatives. See, e.g., Thomas K. Ledbetter, *Comment, Stopping Unsolicited Commercial E-Mail: Why the CAN-SPAM Act Is Not the Solution to Stop Spam*, 34 SW. U. L. REV. 107 (2004); Sameh I. Mobarek, Student Article, *The CAN-SPAM Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to it*, 16 LOY. CONSUMER L. REV. 247 (2004); Lily Zhang, Note, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301 (2005).